

TABLE OF CONTENTS

CORE: INDIGO PILL

[LIBERTARIA IN CYBERSPACE](#) by Timothy C. May, 1992

[MY WET AND WILD BITCOIN WEEKEND ON RICHARD BRANSON'S ISLAND REFUGE](#) by Hannes Grassegger, Motherboard, 08.03.2016

[WHEN THE BLOCKCHAIN SKEPTIC WALKED INTO THE LIONS' DEN](#) by Erin Griffith, Wired, 05.2018

CORE: FLURO PILL

[STARTING AN OVERDUE CONVERSATION ABOUT MONEY](#) by Nathaniel Popper, New York Times, 03.2014

[THE MARKET FOR CRYPTOCURRENCIES](#) by Lawrence H. White, PDF, 2015

[WHAT DOES \\$100 ETHER MEAN?](#) by Vinay Gupta, May 5, 2017
Ethereum milestone recap

[IF, WHEN AND HOW BLOCKCHAIN TECHNOLOGIES CAN PROVIDE CIVIC CHANGE](#) by P2P Foundation - 06.01.2019

CORE: IRON PILL

[BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM](#) by Satoshi Nakamoto, 01.11.2008

[THE CRYPTO-CURRENCY BITCOIN AND ITS MYSTERIOUS INVENTOR](#) by Joshua Davis, New Yorker, 10.2011

[BEYOND ENDLESS WINTER: AN INTERVIEW WITH NICK SRNICEK](#) by Golrokh Nafisi, 20.02.2018

CORE: MAGENTA PILL

[INTO THE BITCOIN MINES](#) by Nathaniel Popper, 12.2013

[IN CHINA'S HINTERLANDS, WORKERS MINE BITCOIN FOR A DIGITAL FORTUNE](#) by Cao Li and Giulia Marchi, 09.2017

[WHAT TO EXPECT IN 2019 AND BEYOND, ACCORDING TO 14 CRYPTO LUMINARIES](#) by Mark Yarm, 26.12.2018

CORE: GREEN PILL

[THE CRYPTO-ANARCHIST MANIFESTO](#) by Timothy C. May, 1988 / 1992

[BITCOIN, THE END OF THE TABOO ON MONEY](#) by Denis Jaromil Roio, 6 April 2013, version 1.0

[VITALIK BUTERIN ON THE HARD LESSONS OF ETHEREUM'S FIRST FIVE YEARS](#) by Brian Patrick Eha, 11.12.2018

CORE: CARMINE PILL

[THE GREAT CHAIN OF BEING SURE ABOUT THINGS](#) by The Economist, 10.2015

[IF YOU DON'T HAVE BREAD, EAT ART!: CONTEMPORARY ART AND DERIVATIVE FASCISMS](#) by Hito Steyerl, 10.2016

[RAVE CULTURE IS MAKING ITS MOVE ONTO THE BLOCKCHAIN](#) by Ben Vickers and Hans-Ulrich Obrist, 10.01.2018

[BOOK - ARTISTS RETHINKING THE BLOCKCHAIN](#)

Read: A Quasi Proto Preface by Nathan Jones & Sam Skinner, 2017
Introduction by Ruth Catlow, 2017

Name of Core

INDIGO PILL

Political Breakdown

LIBERTARIANS, ANARCHO-CAPITALISTS, PLATFORM
CAPITALISTS

Common Beliefs

WE NEED THE FREEDOM TO CREATE PLATFORMS THAT
FACILITATE EXCHANGE AND SOCIAL ACTIVITY. SHARING
ECONOMY, NEW ECONOMY. THE FREEDOM TO CREATE
MARKET OPPORTUNITIES.

Social Constructs

SHARING ECONOMY, POWER OF NETWORK, SURVIVAL OF
THE FITTEST


Coders

JIMMY SONG, BITCOIN SIGN GUY, VINAY GUPTA, JOHN
MCAFEE

Coin

BITCOIN, LITECOIN

LIBERTARIA IN CYBERSPACE

 activism.net/cypherpunk/libertaria.html

To: Extropians@gnu.ai.mit.edu
 From: tcmay@netcom.com (Timothy C. May)
 Subject: Libertaria in Cyberspace
 Date: Tue, 1 Sep 92 11:42:12 PDT

CYBERSPACE MORE HOSPITABLE TO IDEAS OF LIBERTY AND CRYPTO ANARCHY

Here are a few points about why "cyberspace," or a computer-mediated network, is more hospitable than physical locations for the kind of "crypto anarchy" libertarian system I've been describing.

Several folks have commented recently about ocean-going libertarian havens, supertankers used as data havens, and so forth. In the 1970s, especially, there were several unsuccessful attempts to acquire islands in the Pacific for the site of what some called "Libertaria." (Some keywords: Vanuatu, Minerva, Mike Oliver, Tonga)

Obtaining an entire island is problematic. Getting the consent of the residents is one issue (familiar to those on the this list who weathered the Hurrican Andrew diversion debate). Being _allowed_ to operate by the leading world powers is another....the U.S. has enforced trade embargoes and blockades against many nations in the past several decades, including Cuba, North Korea, Libya, Iran, Iraq, and others. Further, the U.S. has invaded some countries---Panama- is a good example---whose government it disliked. How long would a supertanker "data haven" or libertarian regime last in such an environment? (Stephenson's fascinating *Snow Crash* didn't address the issue of why the "Raft" wasn't simply sunk by the remaining military forces.)

I should note that the recent splintering of countries may provide opportunities for libertarian (or PPL, if your prefer to

think of it in this way) regions. Some have speculated that Russia itself is a candidate, given that it has little vested in the previous system and may be willing to abandon statism. If several dozen new countries are formed, some opportunities exist..

The basic problem is that *physical space* is too small, too exposed to the view of others. "Libertaria" in the form of, say, an island, is too exposed to the retaliation of world powers. (I won't go into the "private nukes" strategy, which I need to think about further.)

A floating private nation (or whatever it's called) is too vulnerable to a single well-placed torpedo. Even if it serves as a kind of Swiss bank, and thus gets some of the same protection Switzerland got (to wit, many leaders kept their loot there), it is too vulnerable to a single attacker or invader. Piracy will be just one of the problems.

Finally, how many of us want to move to a South Pacific island? Or a North Sea oil rig? Or even to Russia?

Cyberspace looks more promising. There is more "space" in cyberspace, thus allowing more security and more colonizable space. And this space is coterminous with our physical space, accessible with proper terminals from any place in the world (though there may be attempts in physical space to block access, to restrict access to necessary cryptographic methods, etc.).

I won't go into the various cryptographic methods here (see my earlier posting on the "Dining Cryptographers" protocol and various other postings on public key systems, digital mixes, electronic cash, etc.). Interested readers have many sources. (I have just read a superb survey of these new techniques, the 1992 Ph.D. thesis of Jurgen Bos, "Practical Privacy," which deals with these various protocols in a nice little book.)

Alice and Bob, our favorite cryptographic stand-ins, can communicate and transact business without ever meeting or

even knowing who the other is. This can be extended to create virtual communities subject only to rules they themselves reach agreement on, much like this very Extropians list. Private law is the only law, as there is no appeal to some higher authority like the Pope or police. (This is why I said in several of my potings on the Hurricane Andrew debate that I am sympathetic to the PPL view.)

And this is the most compelling advantage of "Crypto Libertaria": an arbitrarily large number of separate "nations" can simultaneously exist. This allows for rapid experimentation, self-selection, and evolution. If folks get tired of some virtual community, they can leave. The cryptographic aspects mean their membership in some community is unknown to others (vis-a-vis the physical or outside world, i.e., their "true names") and physical coercion is reduced.

Communalists are free to create a communal environment, Creative Anachronists are free to create their own idea of a space, and so on. I'm not even getting into the virtual reality-photorealistic images-Jaron Lanier sort of thing, as even current text-based systems are demonstrably enough to allow the kind of virtual communities I'm describing here (and described in Vinge's "True Names," in Gibson's *Neuromancer* , in Sterling's *Islands in the Net* , and in Stephenson's *Snow Crash* ...though all of them missed out on some of the most exciting aspects...perhaps my novel will hit the mark?).

But will the government allow these sorts of things? Won't they just torpedo it, just as they'd torpedo an offshore oorig data haven?

The key is that distributed systems have no nexus which can be knocked out. Neither Usenet norFidoNet can be disabled by any single government, as they are worldwide. Shutting them down would mean banning computer-to-computer communication. And despite the talk of mandatory "trap

doors" in encryption systems, encryption is fundamentally easy to do and hard to detect. (For those who doubt this, let me describe a simple system I posted to sci.crypt several years ago. An ordinary digital audio tape (DAT) carries more than a gigabyte of data. This means that the least significant bit (LSB) of an audio DAT recording carries about 8 megabytes of data! So Alice is stopped by the Data Police. They ask if she's carrying illegal data. She smiles innocently and say "No. I know you'll search me." They find her Sony DATman and ask about her collection of tapes and live recordings. Alice is carrying 80 MB of data---about 3 entire days worth of Usenet feeds!---on each and every tape. The data are stored in the LSBs, completely indistinguishable from microphone and quantization noise...unless you know the key. Similar methods allow data to be undetectably packed into LSBs of the PICT and GIF pictures now flooding the Net, into sampled sounds, and even into messages like this...the "whitespace" on the right margin of this message carries a hidden message readable only to a few chosen Extropians.)

I've already described using religions and role-playing games as a kind of legal cover for the development and deployment of these techniques. If a church decides to offer "digital confessionals" for its far-flung members, by what argument will the U.S. government justify insisting that encryption not be used? (I should note that psychiatrists and similar professionals have a responsibility to their clients and to their licensing agencies to ensure the privacy of patient records. Friends of mine are using encryption to protect patient records. This is just one little example of how encryption is getting woven into the fabric of our electronic society. There are many other examples.)

In future discussions, I hope we can hit on some of the many approaches to deploying these methods. I've spent several years thinking about this, but I've surely missed some good ideas. The "crypto anarchy game" being planned is an

attempt to get some of the best hackers in the Bay Area thinking along these lines and thinking of new wrinkles. Several have already offered to help further.

Some have commented that this list is not an appropriate place to discuss these ideas. I think it is. We are not discussing anything that is actually illegal, even under the broad powers of RICO (Racketeer-Influenced and Corrupt Organizations Act, used to go after "conspiracies" of porn dealers and gun dealers, amongst others). What we are discussing are long-range implications of these ideas.

In conclusion, it will be easier to form certain types of libertarian societies in cyberspace than in the real world of nations and physical locations. The electronic world is by no means complete, as we will still live much of our lives in the physical world. But economic activity is sharply increasing in the Net domain and these "crypto anarchy" ideas will further erode the power of physical states to tax and coerce residents.

Libertaria will thrive in cyberspace.

- [Tim May](#)

MY WET AND WILD BITCOIN WEEKEND ON RICHARD BRANSON'S ISLAND REFUGE

motherboard.vice.com/en_us/article/vv7vyy/bitcoin-blockchain-summit-with-richard-branson-on-necker-island

March 8, 2016



AT AN EXCLUSIVE SUMMIT ON NECKER ISLAND, MEN IN FLIP FLOPS PLOTTED HOW TO OVERTURN THE GLOBAL ECONOMY.

BY [HANNES GRASSEGGER](#)

Hannes Grassegger of [Das Magazin](#) reports from the Blockchain Summit on Necker Island and discovers how the global economy is being overturned by men in flip flops.

A young woman waved from a red pier. The breeze pressed her short jumpsuit against her body. She waved with her right hand, while her left held her sunhat in place. The

captain brought the speedboat about, the motor sputtered, and I jumped off.

"Welcome to Necker," the woman breathed, "I'm Kezzia." She turned, "Come with me."

The air was that perfect temperature, somewhere in the low 80s, where you stop sensing your body and feel as though you are melting into the world. The crystal clear water of the Caribbean was just a few refreshing degrees cooler. The invitation said "Smart Casual"—so I wore a white dress shirt with my swim trunks.

After a 36-hour journey, I had finally reached my destination: an island that for ten years has been the permanent residence of British billionaire Sir Richard Branson. Kezzia led me to a golf cart parked in the sand. I couldn't help thinking of [a video I had seen](#) in which one of Necker Island's accountants cheerfully recounted serving as a human platter in a naked sushi dinner after finishing her office work. In one interview, Branson laughingly told of a new housekeeper on the island who wanted to institute a rule barring romantic relationships between employees and visitors. "It lasted exactly two days," he said.

On Necker, there is no line between business and private life, at least for employees. For moments when Branson himself does not wish to be disturbed, he purchased the neighboring Mosquito Island. Only Larry Page, Branson's kite-surfing buddy and CEO of Google, was recently allowed to buy himself a piece of land there.

The occasion of my trip was a gathering of two dozen of the entrepreneurs and radical anarcho-capitalists who make up the upper echelons of the bitcoin digital currency movement. The event took birth at a private evening on Necker Island, when the organizers of a kite surf event called MaiTai had asked Branson over a drink if he would be up for bringing together all the leading minds in bitcoin—on his island. "Sure," he said. What exactly this was all about was unclear

to me, but it seemed they were getting together to plan a coup. "We look forward to welcoming you to paradise," the invitation to the Blockchain Summit proclaimed.

Only a select few dozen people received an invitation to the Necker Island summit. Originally, the group included a single woman. Following some concerned remarks on the internet, the organizers invited some more female guests. All had to undertake a strenuous journey, as the island lies on the easternmost edge of the British Virgin Islands, two hours east of Jamaica by plane. The entry fee alone was several thousand dollars per day.

I had already met a few of the participants on the way here. Standing at a kiosk on the beach waiting for a ferry, wearing jeans and a green t-shirt, was Michael Zeldin, 64, a prominent anti-money-laundering expert from the United States, familiar from his many appearances on CNN. Previously a US delegate to the G7, he is now "Special Counsel" to a law firm that represents 17 of the 20 largest US banks.



On the way to paradise.
Photo: Hannes Grassegger

Next to him, dressed in swim trunks and holding a Carib beer, was Brock Pierce. Pierce, who claims to have invented the term "user-generated content," rose from child star to

millionaire tycoon of the old New Economy by age 17. While living in Spain, he built up an online-gaming empire by mining and selling virtual currencies and weapons in computer games, thereby becoming one of the most important early digital currency entrepreneurs. He told me over a drink that, as founder and managing partner of his own venture capital firm, he is currently an investor in 34 different companies.

Pierce, Zeldin, and I had received invitations to the Blockchain Summit, which was meant to bring together "the world's greatest minds in digital innovation" to "define the future." Essentially, what seemed to be happening was that a great deal of money and power were being gathered in the middle of the Caribbean, on a billionaire's private island, for the purpose of plotting. The meeting would culminate in the second night's "Blockchain Summit Final Dinner," a networking event with a "cocktail reception and lemur feeding."

The golf cart trundled just a few meters over a narrow, stone-lined sand track and stopped in front of a two-story wooden house. "The others are already up at lunch," Kezzia said. "I suggest you get a drink, look around a bit, and then come join us."

"Do I need money?" I asked.

She shook her head, laughing, and flitted away.



A bar-hopping lemur.
Photo: Hannes Grassegger

From the second story I heard the murmur of guests at lunch. The ground floor was a kind of tropical pub, open on all sides. A large flatscreen played a tennis match. Reggae bubbled out from hidden speakers. On the central bar, a brown creature with a dog-like face and the body of a monkey suckled someone's left-behind drink. Presumably this was one of the lemurs that Branson had brought over from Madagascar to save from extinction. He has introduced hundreds of species to the island in order to protect them: a "Greatest Hits" of nature. The lemur stared at me for a moment, then turned back to its drink.

Branson evidently had two things on his mind when establishing his island: sex and drinks. His villa was built in Bali, then disassembled, shipped, and erected on Necker's highest point. A wooden hot tub is enthroned on the roof, behind which waves the flag of the British Virgin Islands, the Union Jack on a blue background with the motto, *Vigilate* : "Be vigilant." From here one can see the entire island: the beach house, the tennis court, the two ponds, a handful of scattered love nests, and, in the distance, a few other islands. Next to the house is a shimmering green infinity pool that looks out on an endless Caribbean horizon.

Necker was also once the occasional refuge of Princess Diana. A handwritten letter to Branson testifies to her love of the place. Branson has occasionally used the island to stage ambitious meetings, such as when he brought together politicians and entrepreneurs, like Tony Blair and Larry Page, to save the world from climate change. As part of a proviso by the local government, Branson was required to build a resort here shortly after he bought it, in 1979 at the age of 28. For \$65,000 a day, you can [rent out the island for yourself and up to 29 of your friends](#) . Below, I saw the solar panels that provide the island's electricity. On a hidden pier, workers are unloading one of the boats that run constantly, supplying the island with everything it needs, including sunscreen and an energy drink called "Pussy."



The infinity pool.
Photo: Hannes Grassegger

We live in an age obsessed with progress, comparable to the end of the 19th century, when new technologies such as the railroad and the telephone were changing everything and generating previously undreamt-of riches. Our age, like that one, has seen an explosion in the number of the super-rich. Today, the Rockefellers are Zuckerberg, Page, Gates, and, well, Branson. There are currently around 1,800 billionaires, as measured in dollars. In the past few years,

their fortunes have increased so massively that they have begun wondering what to do with all the money. At the same time, there is a valley near San Francisco full of technology entrepreneurs who need money—lots of money—for their business ventures.

The goal of these entrepreneurs is to rebuild existing industries with new technology, monopolize the market, and watch the profits roll in. They call this "disruption"—as Airbnb has done in the hotel industry, or Uber in the realm of taxis. The larger the target industry, the better. Google has built a whole "vertical," X, [for testing so-called "moonshots,"](#) ideas so megalomaniacal that anyone would consider them impossible—anyone who did not have a few billion to spare on their realization, that is.

Winter is coming to the Valley soon, and it might be the first since the bubble burst first in 2001. This bubble bursting might not be as tough as the last one, most people in the tech industry hope, but who could say for sure.

Nevertheless, when people congregated on the island, there was a feeling that new territories were needed for chasing unicorns—the startups that remake entire industries with multi-billion valuations and big payoffs for venture capitalists. It is just such a project that Richard Branson has in mind. With a net worth of \$4.9 billion, he's invested millions each in [over a dozen startups around the globe](#) , including \$30 million in [Blockchain](#) , a popular bitcoin wallet and blockchain explorer service.

In his opening speech, Branson invited the guests to rate their business plans in terms of "Scale of Effect on Society." This was accompanied by a musical interlude by star cellist Zoë Keating, who spent the rest of her stay on Necker Island excitedly posting snapshots of Branson's giant tortoises on Instagram.

From the rooftop hot tub, I walked past a few terraces to reach a hall with a ceiling high enough to accommodate full-

size palm trees. A disco ball hung from the ceiling. A few books with titles like *An Optimist's Tour of the Future* or *An Experiment in Industrial Democracy* lay strewn across the landscape of cozy couches.

"Imagine experiencing the birth of the internet. That's about how big this is."

On the other side of the bar, several rows of wicker chairs were set up facing a flatscreen emblazoned with the words: "Blockchain Summit – The Vision." It was clear to me that this was a gathering of people whose time is short and expensive. Such people do not meet just for fun, but perhaps also for fun.

Nor does Branson's choice of residence seem accidental. Branson officially relocated to Necker in 2006 for health reasons, [he has said](#) . But the British Virgin Islands—or BVI, for short—of which Necker is one, are the most popular offshore tax haven in the world. By developing a complicated network of BVI companies, Branson [pays few taxes](#) in his native land. Many English children have heard of Necker Island. It is a dream island that represents the idea that an individual can beat the state.

To moderate the summit, the organizers booked one of the most renowned writers on finance technology, Wall Street Journal columnist Michael J. Casey, who last year published *The Age of Crypto-Currency* , a book on digital currencies like bitcoin and its underlying programming principle, the "blockchain."

The blockchain, Casey explains in the book, is a register, a vast bank-book, a digital ledger, that lists every individual transfer of bitcoin. In contrast to our current money system, in which every bank maintains its own centralized register to verify whether the correct quantities of money are being moved, the blockchain decentralizes the verification, thereby creating a "shared common ledger" stored on every

connected computer. Thus, the blockchain allows every bitcoin user to take on the functions of a bank.

But this is just incidental. The blockchain not only makes digital currency impossible to duplicate: In principle, Casey prophesied, the technology could even replace companies, law firms, and agencies whose main job is to manage assets. Lately, the Bitcoin community has been torn asunder by a debate over the future of the blockchain, and [whether it can continue to grow as quickly and cheaply under its current design](#) . But this was not a topic of discussion at the conference: the weather was more blue-sky.



Zipline time.
Photo: Hannes Grassegger

Under a sun canopy on the beach, I encountered a bunch of men in their 30s. All are in shorts, rather pasty, with the beginnings of a paunch. A bearded giant by the name of Oliver Luckett played rap on the kind of small, tube-shaped boombox often used by teenagers in parks. He told how he recently bought a \$10,000 Rolls Royce on Craigslist, only to torch it with flamethrowers for the rapper's video. It went viral, since all the video's participants already had so many followers on the web. "A bargain, right?" he asked. The others nodded. (Luckett's company, the Audience, also ran Obama's social media campaign for a time. Before that, he

worked for Disney. In the digital empire, he is a Minister of Propaganda.)

Over on a sandbar, I saw a catamaran with a dozen people next to it. Perhaps Branson is there. "Do you want to try something?" one of the beach beaus asked. He led me over to a shack filled with surfboards, sails, and snorkels. On the wall hung a photo of Branson, grinning broadly for the camera, flying over the water as the wind blows his hair. He is on a surfboard, holding a kite-sail in front of him while a nude model hangs on him like a backpack.

A Dutchman in his 50s, who introduces himself as Marc, wanted to try paddleboarding, so I decided to join him. Marc invests in startups. He flew in from Vancouver. "Why did you come?" I asked him. The trainer positions the board on some calm water for us.

"Bitcoin is gradually turning into a serious thing," Marc said as he tried to stand on the wobbly board. "Look at who's here—a president of Samsung, a chief strategy officer of Ernst & Young. Did you hear that Obama's favorite economist, Larry Summers, has gotten involved with a bitcoin bank? And the founder of Visa?"

In the tropical pub, I ran into Michael J. Casey. He looked like one of those classic American war reporters on TV with their oversize microphones, only that he is Australian. We ordered Painkillers, an excellent coconut-based cocktail, and started chatting.

"Since the crisis in 2008," Casey said, "the financial system has been completely broken. They've tried to camouflage the fact by printing more dollars, but money is just a product, and now there's a surplus of it. Look what's happening in Switzerland. Negative interest rates. You're actually paying to give someone money. Of course, people are looking to other assets, houses or whatever. But what are they supposed to use for currency?" Casey shook his head.

"The fundamental problem of the financial crisis was that everything was too interconnected,"he continued.

"Centralization. Insanely enough, it's gotten even worse. Meanwhile, the entire international economy depends on two central banks. Do you call that stable? Bitcoin is the alternative to this broken money system."

As the evening cocktail reception approached, I walked back from the tropical pub to Branson's villa with Luckett and an Australian man. The Australian took us to his room, which costs just over \$2,000 per night. It's a good price—typically, one must [rent the entire island](#) . For this budget rate, the Australian had to share the room with the elderly futurist Marshall Thurber. Out on the balcony, Casey filmed the sunset.

"It's such a thrilling time," he said. "Imagine experiencing the birth of the internet. That's about how big this is."



Capturing the sunset.
Photos: Hannes Grassegger

The first guests had arrived the day before, but no one was really clear on the specifics of the program. Back at the big hall, Casey plopped onto a sofa next to a plump bald man in a wine-red polo shirt. He was telling the story of how he wrote the constitution of Peru. This was Hernando de Soto. An advisor to governments, de Soto may be Latin America's

most renowned stronghold of market capitalism, which he sees as a tool against any evil available, most recently terrorism.

When de Soto has a question about Russia, as Casey explains it, "Hernando" just calls Putin—and he picks up. Bill Clinton [once called de Soto the "greatest living economist."](#) To ensure that Hernando could get to the meeting on time, the premier of the Virgin Islands personally faxed him a visa. De Soto has frighteningly strong, hairy arms, which he moves like a crab's pincers. That morning, the Peruvian had primed the participants for their mission: to bring capitalism to life. For true capitalism does not yet exist.

Poverty, according to the theory that brought de Soto international fame, is not exploitation, but exclusion. In other words, people are unable to participate in capitalism because they have nothing to bargain with. Slum residents, for example, build huts but cannot own them, as there is no place and no law that will register them. If they had some kind of official paper, a certified claim to the property, a title, the hut would be worth something. They could sell it, or take on debt to start a business. To raise people out of poverty, therefore, their valuables must somehow be linked to them as individuals. They must have property rights.

In most countries, this is next to impossible. De Soto opened a folder of papers: the three dozen applications necessary to register a company in Peru. A "physical blockchain," he said, that takes hundreds of days to process. If such situations were remedied, world poverty would end, and true capitalism would blossom. The participants were rapt.

Next to de Soto sat Brian Forde, a quiet man who until recently was Obama's technology advisor. Now he is leading the Digital Currency Initiative at the Media Lab of the Massachusetts Institute of Technology, as well as traveling around the world convincing governments and companies to give the blockchain a try.

We were greeted at the dinner party by hundreds of screeching flamingos. A fire was burning, chefs stood at the buffet, and a long, white table was waiting. Other than the employees, almost no one followed the dress code, "Evening in White." Most wore shorts. Suits are the mantel of civilization, too confining. Suddenly, a shark fin appeared in the sea behind the buffet. One of the guests giggled and tossed a chicken drumstick into the water. "Save Water, Drink Champagne," his shirt read.



Flamingos at dinner.
Photo: Hannes Grassegger

I sat across from Paul Brody, a slim executive from San Francisco with short, greying hair. Cheerfully, he spoke in a nasal voice of being wiped off the tennis court by Branson at seven in the morning. "Impressive for 65!" he said.

Brody had been trying out all of the island's personal trainers. A little morning weightlifting, "all-inclusive." I asked how much he paid to come here. "Hmm," he calculated, "the company paid. My rate, which would be \$36,000 for three days, plus the flight, plus accommodation here on the island, 8,000 ... the participation fee. About \$50,000."

"No government in the world would be able to control bitcoin anymore"

Brody is a minor star in Silicon Valley. His husband negotiated Facebook's purchase of Instagram. Brody himself had 6,000 people working under him at IBM, where his focus was the Internet of Things. Now he is the American "Strategy Leader" for Ernst & Young. Somehow we get onto the subject of cycling. "I love it!" he said. "I used to ride a lot until I was hit by a car. I swore to myself that I wouldn't get on a bike again until there are only self-driving cars." Our tablemate nodded enthusiastically: "People are too fallible. We have to take them out of the equation."

Next to Brody sat Jeff Garzik, one of bitcoin's longtime developers. At the moment, he is looking for investors to help him put mini-satellites into orbit for a special bitcoin network. "No government in the world would be able to control bitcoin anymore," he said.

Later, I ran into a group of people lounging on a sofa, passing around an e-cigarette filled with liquid marijuana. One of them, part of Branson's service team, told me that it takes 120 people to keep the island running every day, or about three staff members per guest. He said he earned \$1,200 a month—Brody's hourly rate.

*

Around nine o'clock the next morning, there was a breakfast buffet: bacon, eggs, tomatoes, croissants, and kale juice to detox; fair-trade granola bars and champagne bottles with a golden label that read, "Sir Richard Branson's Private Island." Over at the muesli bowl, I found myself suddenly face-to-face with Branson himself.

"Hi!" he said, with a friendly smile. Tan and wearing a grey t-shirt and swim trunks, he has a surfer's lion-gold, almost neon-ish mane, which goes well with his large mouth and huge teeth bordered by a darker goatee. He grabbed a glass of fruit juice and walked away with his muesli. I followed him to a veranda with a long wooden table, plenty big enough for the thirty people who are staying in Branson's villa.

The blockchain would, in essence, allow capitalism to more fully move into the realm of the internet.

The life of a billionaire, I had begun to understand, is like a reality TV competition. De Soto, Forde, Casey, and Lockett sat around Branson, all of them trying to sell him on their projects and plans in as few sentences as possible. This is an "elevator pitch": the 90 seconds one has to try to convince the investor of a lifetime to join in a business venture. Branson, with an estimated worth of five billion dollars and a reputation for wild business ideas, is an amazing opportunity. An elevator manufacturer once suggested to Branson that he install one here on the island expressly for elevator pitches.

Branson listened calmly, eating his muesli and sipping coffee. Now and then, he asked a question in his gentle voice. His pronounced stutter is well under control. When he tried to go back to the buffet, he couldn't make it more than a few meters without being detained, to listen to a new idea or to pose for a photo that will immediately be posted online, thereby increasing the market value of the person posing with him.



Lunch with Richard.
Photo: Hannes Grassegger

At around ten, we arrived at the main event. The 35 attendees, who include seven women, gather around the flatscreen in the big hall. Some of them have prepared short presentations. Brody, the star executive, explains that in the near future practically everything will be online.

"Every toaster will have a chip like this one here," he said, holding up his iPhone. "This chip has more processing power than the first iPhone," he added enthusiastically. "This device could connect to the net. And what happens to things when they go online? We record their usage, start measuring their capacity, and try to increase it. Like fitness, thanks to Fitbit wristbands that count our steps. Like apartments, that we sublet on Airbnb when we're away. Like cars, that you can rent when they're not being used."

"Unused potential is everywhere," Brody continued. If there were a method for indexing this potential and trading with it, the market would be "tremendous, unbelievable." The blockchain, he said, is precisely the tool to manage an "internet of value," in which "everything" would be tradeable. De Soto beamed.

The blockchain would, in essence, allow capitalism to more fully move into the realm of the internet. This has always failed in the past, because in digital environments, everything is so easy to copy. Therefore nothing is scarce, which is why digital content, like music, images, and text, is almost always free, or extremely protected. The blockchain's comprehensive ability to allocate each piece of code within its system could completely eliminate the possibility of copying a song, for example, because who has which digital copy when would be traceable. A digital magazine based on the blockchain system would have unique copies, just like a printed magazine. It could be bought and sold like a physical object.

Next, a long-haired computer scientist named Patrick Deegan demonstrated one of the idea's applications. He's

used blockchain to create digital passports that allow people to register their possessions. Deegan talks about "smart contracts": digital agreements that execute themselves automatically, like leased cars that will not start if the installment has not been paid. Administrative staff would be unnecessary. Deegan is optimistic. The blockchain, it seems, could automate bureaucracy. It could replace millions of employees. A moonshot. Most recently, he said, the world's most powerful banks have formed a [consortium named R3](#) to employ such ideas.

All of this dramatically serves the common good, most of the speakers say during their presentations. One speaker invoked the visionary architect Buckminster Fuller, a kind of Abraham in the epic of Silicon Valley. He handed out Fuller's bible, *Spaceship Earth*, and told how "Bucky" passed on his mission in his last days: "On personal integrity hangs humanity's fate." He then presented a rating system for humans in which people are continually evaluated. Like the taxi service Uber, where customers rate drivers and drivers rate customers, but for all of life, visible to everyone.

The problem for the guests, it seems, is that the business case for Buckys vision is not obvious. The reactions in the audience were mixed. Friendly applause.

To conclude, Lockett—the Rolls Royce burner—demonstrated that the development of the internet and the blockchain are not only spiritually correct, but deeply natural. Nature too is organized in networks. As proof, he showed pictures of networks of mushrooms next to visualizations of social media networks. The applause was frenetic. During a short pause, the participants gathered on the giant chess terrace for a 3D group picture. As the picture-snapping drone approached from the blue skies, everyone raised their arms in a group cheer.



Preparing for a drone selfie.
Photo by Hannes Grassegger

At lunch, served in the lower pool, the mood was euphoric. As I sank into the water, a girl launched a little boat laden with drinks in my direction. "Sake cocktail?" Next came a flower-bedecked kayak filled with sushi. A French star-chef served cuisine in his swim trunks. From the palm-leaf-covered pool bar I hear electro-pop duo Ratatat's "Cream on Chrome."

"When everything goes through the blockchain ... I could fire half my team. Lawyers, notaries, bankers—they just do what the blockchain does automatically."

Over coconut water at the bar, I talked to an investment banker with gelled blond hair. He was high.

"Fantastic, man!" he said. "My business is number one at getting money out of China. It's complicated as hell, nothing but regulations, transparency, and limits. Huge monitoring costs ... I think efficiency is going to increase tremendously."

"How?" I asked.

"When everything goes through the blockchain ... I could fire half my team," he beams. "Lawyers, notaries, bankers—they just do what the blockchain does automatically." Then a woman in a tight black dress with a huge floppy hat stole his attention. The party guests have arrived.

The fresh fish was excellent, and must have been flown in from far away, as a strange virus had made the local fish inedible. A dark-haired man in his mid-thirties paddled near me. He trades in bitcoin and commutes between London and France. His eyes gleamed.

"Huge sectors of government do nothing but manage assets and execute contracts," the man said. "Not just the central banks, but the passport agencies, registration offices, land registries for real estate. All of that will be unnecessary." As a senior venture capitalist sunk into the water next to us, still holding his Blackberry, the man whispered conspiratorially, "C'est une revolution. "

We climbed out of the pool, and a thin young Arab man stood before me. "Salaam," he said with a smile.

"He's from the Emirates," my new friend explained as we walk toward the beach. "He could be the first big blockchain investor from there. He might be richer than Branson. In any case, Branson forbid him from bringing his bodyguards to the island."

On the beach, I grabbed a snorkel. I swam along the ocean floor, passing a ball-shaped creature. It was half a meter wide and pulsing. Strange, large fish were everywhere.

*

Around seven, I met Tina Hui, who runs a social media site about bitcoin. She posts updates constantly, even while doing her makeup.

"I can't ever look bad," she said, "I'm always online." Tina was one of the few women added to the guest list after the organizers were criticized for inviting only men. The others included an aerospace engineer who works for Branson's spaceship company, a famous attorney, and Elizabeth Rossiello, the CEO of Nairobi-based BitPesa, which provides [transfer between bitcoin and local currencies in Africa](#) .

This is great for the currency's reputation, the thinking goes, as bitcoin will never be adopted by the masses as long as it is seen as money for internet gangsters. To the same end, that morning an inconspicuous gentleman with an extreme comb-over and an apricot linen shirt—previously employed

by the Department of Justice—had suggested cooperation with "state agencies." A strategic cease-fire, so to speak.



By the beach.
Photo: Hannes Grassegger

We made it to the tropical pub just in time. The chef had prepared a Moroccan-style meal, perhaps in honor of the event's special Middle Eastern guest. The table is U-shaped. There were now some seventy guests on the island. I spotted Brock Pierce, Michael Zeldin, and several ladies in dresses. Torches were stuck in the sand. Rosé from New Zealand was poured. Across from me sat Ted Rogers, who looks like the captain of a rowing team. Rogers is president of the bitcoin vault Xapo, which Larry Summers joined after ending his candidacy for president of the Federal Reserve.

Bitcoin entrepreneurs have to get out of the pirates' islands, Rogers said, and into "clean" countries. Xapo has one of its legal headquarters in Argentina, another one in Switzerland. "Switzerland could become the home of bitcoin," he suggested. He finds the culture of privacy and the hands-off government optimal. "And the legislators are reasonable, too. You can talk to them." He had just explained that there is an important community of bitcoin supporters in the Swiss town of Zug when Branson appeared.

Zug, a small town of 30,000 inhabitants, was once Switzerland's capital of offshore banking. Thanks to its free-market reputation, it has recently become one of the world's leading hubs for the cryptocurrency folks. Nevertheless it's so boring that Xapo actually resettled half an hour north, in Zürich, Switzerland's busiest town. In January Xapo's CEO Wences Casares joined Paypal's board.

There are two kinds of billionaire. One makes money off the system. Branson makes money off its destruction.

Cello music wafted over the tennis court and the guests reclined on pillows arranged in a semi-circle, while Branson sat enthroned on a sofa with the sheikh to his left. The cellist Zoë Keating left the stage. De Soto stands. His act is next. And for a brief moment, Branson was alone.

"Sir," I said. He bows. "You signed the Sex Pistols."

He nodded, baring his teeth to smile. At the Queen's Silver Jubilee in 1977, Branson chartered a boat on the Thames, on which the punk band famously mocked the monarch. The police got involved, of course, and the media was there, filming everything. The scandal put the Sex Pistols' single on the charts and made Branson a lot of money. There are two kinds of billionaire. One makes money off the system. Branson makes money off its destruction.

"Is it still all about the same thing as back then?" I asked. "Against the state, against banks?"

"Sure, man. You got it," Sir Richard grinned. He raised his hand for a high five.

"Capital!" cried de Soto. He made a fist, scanning the crowd. "The word comes from Caesar's head on Roman coins. From caput —head." His voice was strong, and even the cellist was listening. "This head is the power." De Soto raised his fist. "And this head is you."

Branson looked like a boy seeing his model airplane lift off the ground for the first time. De Soto pointed to his

audience, and said: "You're part of the creation of a new capital."

"Yes!" Branson said from his divan. "Yes!" and he began to clap. The others joined him and the applause nearly filled the island.

The closing beach party was a flop.

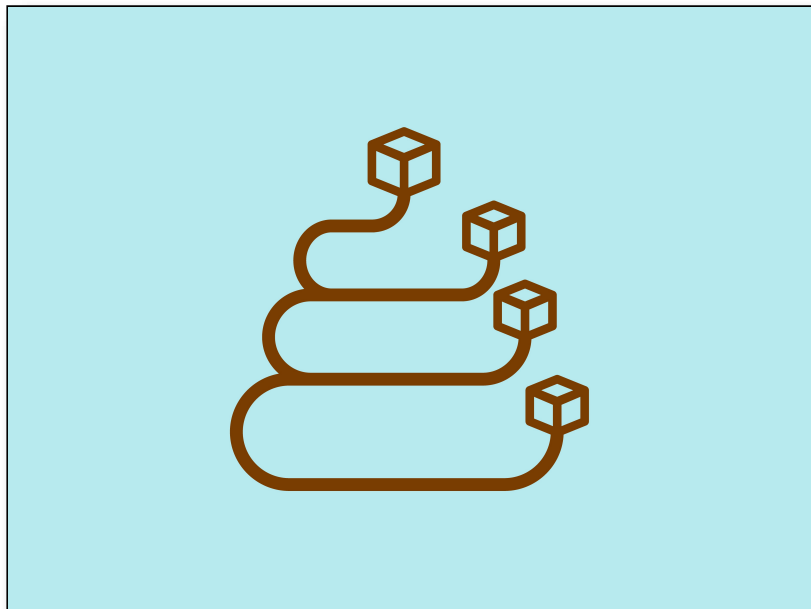
*

Hannes Grassegger is an economist based in the financial capital of Zürich, Switzerland, who skipped investment banking to become the leading German reporter on digital life (Digitales Leben, as they call it). He is the author of [Das Kapital bin Ich \(I am Capital\)](#) , a pamphlet on how to screw the NSA plus all other secret services and make a dime from it, too. Follow him on Twitter [@HNSGR](#). This article first appeared in German in [Das Magazin](#) .

WHEN THE BLOCKCHAIN SKEPTIC WALKED INTO THE LIONS' DEN

■ [wired.com/story/when-the-blockchain-skeptic-walked-into-the-lions-den/](https://www.wired.com/story/when-the-blockchain-skeptic-walked-into-the-lions-den/)

ERIN GRIFFITH



HOTLITTLEPOTATO

It takeschutzpah to walk on stage in front of thousands and declare that most of the people in the room are totally full of shit. That's how Jimmy Song, a venture partner at Blockchain Capital, entered Monday at Consensus, the biggest [cryptocurrency](#) conference of the year, at New York's Hilton Hotel. That he did so sporting a black cowboy hat and boots was merely a bonus.

Song, an investor and [bitcoin](#) enthusiast, declared he hadn't seen anything of interest at the conference's three floors of packed displays, breakouts, and roundtables. An endless string of sponsor logos floated by on a 40-foot screen behind him. But Song said most of the problems being tackled by those companies don't need [blockchain](#) technology.

"Blockchain is not going to solve all your problems for you," he declared. "You're a hammer-thrower just looking for nails." When you have technology in search of a use, he said, "you end up with crap that we see out there in the enterprise today."

Indeed, as the crypto craze has gathered hype over the past year, mercenaries have rushed in, leveraging enthusiasm around the technology to raise money, artificially boost their stock prices, and ride a cycle of good press. But the cracks are starting to show: Some businesses that experimented with blockchain technology have [decided](#) they can achieve the same results with less cumbersome and less expensive tech tools.

In that way, Song pierced a hole in the near-religious zeal of crypto enthusiasts, who tend to sort the world into two categories: [HODLers](#) (true believers) and no-coiners (haters). That an insider would deride a large swath of the industry hints at its precariousness. Bitcoin, and other digital currencies with no underlying value, are worth something because people say they're worth something. But what if all of this—physically embodied by an elaborate, corporate-sponsored business carnival—is just an expensive, inefficient solution in search of a problem? Song was the first presenter I saw at the conference to forcefully challenge the industry belief that decentralized networks can solve just about any problem.

LEARN MORE

THE WIRED GUIDE TO [THE BLOCKCHAIN](#)

Song hammered the point with gusto while his co-panelist, Ethereum cofounder Joseph Lubin, responded with measured counterarguments. Not all blockchains have to be

expensive, Lubin said. Tech advancements will permit bigger projects. But Song was determined to suck all the hot air out of the room, at one point imitating Oprah giving away cars, shouting, "You get a blockchain! You get a blockchain!"

Song's issue is that most enterprise-software companies offering blockchain solutions don't benefit from decentralization. Blockchain technology is supposed to eliminate the need for a trusted third party to verify things like transactions and contracts. But most of the use cases available today still need some sort of third-party involvement, be it a bank, lawyer, or regulatory body.

In one example—global trade—Song argued that existing standards organizations can handle the problems blockchain purports to solve. Even if today's systems are broken, he doesn't see how blockchain can fix them. "Blockchain is not this magical thing where you sprinkle blockchain dust over a problem," he said.

When Song declared that most projects being built today will not exist in five years, Lubin offered to bet "any amount of bitcoin" that he's wrong. Someone in the back of the ballroom shouted, "One million!" (Lubin's crypto holdings are [estimated](#) to be worth \$1 billion to \$5 billion.) The speakers agreed to decide on terms after the panel.

Song ended by saying he looked forward to meeting everyone in the room who was laughing at his views. The session's moderator responded that he could expect plenty of feedback; while they were onstage, her phone "was literally melting" from all the tweets.

Afterward, Song told WIRED he'd gotten mostly positive feedback, though plenty of people tried to convince him he was wrong. "There can be a feeling of, if you don't drink the Kool-Aid, you're stupid," he said.

Name of Core

FLURO PILL

Political Breakdown

CENTRIST-LEFT, LEFT, CIVIC CHANGE NETWORKS

Common Beliefs

A NEW CHIMERA ECONOMY MUST BE BIRTHED ON BOTH A
SOCIAL AND EMOTIONAL LEVEL FOR US TO THRIVE

Social Constructs

UNIVERSAL BASIC INCOME, DECENTRALIZED NETWORKS FOR
GOOD, PARTICIPATORY GOVERNANCE, ECONOMIC JUSTICE,
TECHNOLOGY FOR PEACE

Coders

VINAY GUPTA, ELISABETH STARK, P2P FOUNDATION, YANIS
VAROUFAKIS, DIEM25

Coin

ETHEREUM, MONERO, DFINITY

STARTING AN OVERDUE CONVERSATION ABOUT MONEY

dealbook.nytimes.com/2014/03/31/starting-a-overdue-conversation-about-money

DealB%k WITH FOUNDER
ANDREW ROSS SORKIN

BY NATHANIEL POPPER
MARCH 31, 2014 5:48 PM



JENNIFER DANIEL

THERE is no end to the disagreements about the importance and usefulness of the upstart virtual currency Bitcoin.

There is, though, no disagreement that Bitcoin's rise to a billion-dollar market has helped fuel a wide-ranging conversation on Wall Street and in Silicon Valley — and many places in between — about the nature of money and how it might be evolving.

There have been few big changes in the infrastructure of the world's payment networks in decades. The basic elements of the credit card system have been around since the 1960s, and the mechanisms for bank transfers have been pretty much the same since the 1970s. Cash looks little different from the way it did in the 18th century.

Bitcoin is but an example of several recent technologies that are seeking to upend the way banks, regulators, merchants and consumers think about dealing in money. Creators of mobile wallets and digital tokens, such as Venmo and Square, are trying to provide faster, more seamless ways of paying bills. But few of these other new technologies are trying to change as many elements of the financial system as Bitcoin.

"The awareness of how we spend our money, and how it flows through the pipes, has totally been elevated as a result of Bitcoin," said Mark Williams, a professor at [Boston University](#) who has been one of the harshest critics of the virtual currency system.



WITNESSES In January, venture capitalists and Bitcoin investors testified at a New York State hearing in Manhattan: left to right, Barry Silbert of SecondMarket and Bitcoin Investment Trust; Jeremy Liew of Lightspeed Venture Partners; Fred Wilson of Union Square Ventures; and Cameron and Tyler Winklevoss.

LUCAS JACKSON/REUTERS

Perhaps the biggest challenge that virtual currencies present to the existing financial system is the speed and ease with which they can move across boundaries of all sorts.

Benjamin M. Lawskey, New York State's top financial regulator, who is scrutinizing the virtual currency sector, has complained in recent appearances about the time it takes for his bank to move money from his own account to pay off a credit card issued by the same bank. In the Bitcoin universe, by contrast, most transactions are confirmed and completed within 10 minutes.

The current financial plumbing is a particular concern for people in countries with less-developed financial institutions, and for immigrants trying to send money over international borders. While [Western Union](#) can charge a 10 percent fee to move money to Mexico or China, Bitcoin users can make transfers free if they know what they are doing.

"There is something very powerful there in terms of allowing these kinds of international transactions with a lot less frictions and lot less cost," Mr. Lawskey said in a recent interview.



WITNESSES Benjamin Lawskey, superintendent of financial services, also spoke.

LUCAS JACKSON/REUTERS

Frustration with fees of all sorts has helped drive the interest in virtual currencies. Credit cards, for instance, generally charge merchants 2 to 3 percent of every purchase.

Because Bitcoin is run by a decentralized network of computers, rather than a central company, there is essentially no charge to move money from one wallet to another. Start-ups like BitPay that handle the process for merchants currently charge around 1 percent. A [Goldman Sachs](#) analyst estimated in a March report that retailers could save \$155 billion a year if they all moved to accepting only Bitcoin at current rates.

Credit card fees are a particular problem for companies looking to collect small online payments for goods and services that cost less than a dollar — the penny candy purchases of the Internet world. A number of video game companies, including [Zynga](#) and Big Fish, have recently decided to take virtual currencies because tiny payments can be made without most of the money going to fees.

Even with these advantages, though, virtual currencies have real obstacles to overcome before they become as commonplace as cash. The most frequently discussed shortcoming is their price volatility. If the price of a Bitcoin could fall 10 or even 20 percent in a day — as it has many times — why would a merchant want to take the risk of accepting it?

What's more, the lower costs of Bitcoin transactions are at least partly a result of the fact that Bitcoin companies face fewer regulations. That is changing as regulators like Mr. Laws look at creating rules for the industry. He held a hearing in January and is accepting applications for licenses from Bitcoin exchanges. If government authorities do create more rules for these companies, the costs may rise. And if regulators do not move in, the Bitcoin network could remain vulnerable to the hackers and fraudsters who have scared so many consumers away.

But while certain types of security flaws have been a major drawback of Bitcoin, the security of the Bitcoin network has also been a major selling point. Recent revelations about the [National Security Agency](#) 's classified collection of digital data — and the theft of credit card numbers from retailers like [Target](#) — have given ammunition to privacy advocates who think that virtual currencies can provide a more secure and private way to move money.

Bitcoin transactions are recorded on a common ledger, which makes all transfers traceable. But people who want to keep their Bitcoin spending private are usually able to keep their virtual currency addresses secret.

Beyond the practical concerns that Bitcoin is taking on, the virtual currency is helping to fuel broad debates about the way the world's central banks currently create and manage money.

Many Bitcoin advocates are fierce critics of the [Federal Reserve](#) 's efforts to help the economic recovery by injecting new money into the financial system, in what is known as [quantitative easing](#)

The anonymous creator of Bitcoin determined in the software that was released in 2009 that no more than 21 million coins would ever be created, hoping to stave off the inflation that has been a regular feature of the dollar.

Fears that the Fed's recent policies would fuel inflation have not been borne out. In fact, many economists think the bigger threat to the economy is deflation.

This has not cooled the ardor of Bitcoin aficionados, who are convinced that the world needs to move away from centralized control of the monetary system. For those who are not fans, the presence of Bitcoin has, if nothing else, held a flashlight to the financial plumbing that used to be all but invisible.

THE MARKET FOR CRYPTOCURRENCIES

Lawrence H. White

Cryptocurrencies like Bitcoin are transferable digital assets, secured by cryptography. To date, all of them have been created by private individuals, organizations, or firms. Unlike bank account balances, they are not anyone's liability. They are not redeemable for any government fiat money such as Federal Reserve Notes or for any commodity money such as silver or gold coins. The cryptocurrency market is thus a market of *competing private irredeemable* monies (or would-be monies). Friedrich A. Hayek (1978a) and other economists over the last 40 years could only imagine how market competition among issuers of private irredeemable monies would work. Today we have an actual market to study. In what follows I will discuss the main economic features of the market. I also discuss whether the market is purely a bubble.

As an introduction to the topic, I offer the following comic verse about the contrast between Bitcoin and the physical gold coins of the past:

In the past, money's value was judged with our teeth;
We *bit* coins to confirm they were real.
Now a Bitcoin's just data, no gold underneath.
That's okay if it buys you a meal.¹

Cato Journal, Vol. 35, No. 2 (Spring/Summer 2015). Copyright © Cato Institute. All rights reserved.

Lawrence H. White is Professor of Economics at George Mason University, a Senior Fellow with the F. A. Hayek Program for Advanced Study in Philosophy, Politics and Economics at GMU's Mercatus Center, and a Senior Fellow at the Cato Institute's Center for Financial and Monetary Alternatives. He thanks Patrick Newman for research assistance and participants at Cato's 32nd Annual Monetary Conference for comments.

¹The fourth line is mine. It refers to the news that Washington, D.C. now has a food truck that accepts Bitcoin payments. The first three lines are by Gary Crockett (2014). His original fourth line was: "Bitten bits don't make much of a meal."

The Size and Composition of the Cryptocurrency Market

Bitcoin rightly gets the lion's share of media attention, but it is not alone in the market for cryptocurrencies. The authoritative website CoinMarketCap.com tracks the U.S. dollar price and total "market cap" (price per unit multiplied by number of units outstanding) for each of more than 500 traded cryptocurrencies. Bitcoin is the largest by far. On a recent day (March 9, 2015), the site showed Bitcoin trading at \$291 per unit, with a market cap of \$4.05 billion. The second and third largest cryptocurrencies, Ripple and Litecoin, had market caps respectively 8.5 percent and 1.8 percent as large. The entire set of non-Bitcoin cryptocurrencies (known as "altcoins") had a market cap of roughly \$619 million, or 15 percent of Bitcoin's. Stated differently, Bitcoin had roughly 87 percent of the market, altcoins 13 percent. In percentage terms, altcoins do a higher share of Bitcoin's business than Bitcoin does of the Federal Reserve Note's business (currently \$1.35 trillion in circulation). In trading volume the percentage share of altcoins (led by Litecoin and Ripple) has been similar.

The cryptocurrency market has grown about fourfold in market cap over the last 22 months, with altcoins growing faster than Bitcoin. This is seen by comparing recent data to the oldest snapshot of the CoinMarketCap site available via the Internet Archive "Wayback Machine," which reports data for May 9, 2013. On that date, Bitcoin had a price of \$112 per unit, and a market cap of \$1.2 billion. The two largest altcoins at that time, Litecoin and Peercoin (aka PPCoin), had market caps respectively 4.7 percent and 0.4 percent as large. Only 13 altcoins were listed. Jointly their market cap was about 6 percent of Bitcoin's, giving Bitcoin 95 percent of the market. Since then, the market share of altcoins has doubled, and their market cap has grown ninefold. Trading volumes then were not reported.

At \$4.05 billion, the market cap of Bitcoin, as of March 2015, was slightly smaller than the dollar value of the September 2014 monetary bases of the Lithuanian litas (\$5.8 billion) and the Guatemalan quetzal (\$5.5 billion), but larger than those of the Costa Rican colon (\$3.3 billion) and the Serbia dinar (\$3.3 billion).² The August 2014 figures from the Central Bank of the Bahamas do not provide the

²All figures to follow come from official central bank websites, converted to U.S. dollars using the xe.com rates for September 30, 2014.

monetary base, but count Bahamian dollar currency in circulation at \$210 million, less than two-thirds of Ripple's recent market cap of around \$344 million.

Medium of Exchange, Store of Value, and Medium of Remittance Functions

The retail use of Bitcoin as a medium of exchange for goods and services is small to date, but is growing. In December 2014, Microsoft began accepting bitcoin payments “to buy content such as games and videos on Xbox game consoles, add apps and services to Windows phones or to buy Microsoft software” (BBC 2014). In doing so it joined prominent online retailers Overstock, Dell, Expedia, TigerDirect, and Newegg, and the payment processors Paypal and Square. The list grows weekly. Payments processing firms Bitpay, Coinbase, Coinkite, and others are enabling (and recruiting) brick-and-mortar retail shops to accept Bitcoin from any consumer whose smartphone “Bitcoin wallet” application can display a QR code. On its website Bitpay claims a clientele of “44,000 businesses and organizations”; Coinbase claims 37,000. These processors offer to purchase the consumer's bitcoin as it is spent, paying the equivalent (minus a fee) in dollars or other preferred currency to the merchant. The merchant avoids all exchange rate risk of holding bitcoin. For the retailer on the front end of the transaction, “accepting bitcoin” via these services actually means receiving dollars (or euros, etc.), just like accepting a credit card or debit card does. Bitpay and Coinbase thereby remove the barrier against transacting in cryptocurrency posed by the incumbency advantage of the established domestic currency unit (Luther and White 2014), just as Visa and Mastercard enable merchants to accept credit and debit cards from a customers whose accounts are denominated in a foreign currency.

A potentially vast market for bitcoin and altcoin use is international remittances. For example, workers abroad send an estimated \$25 billion per year to the Philippines, where remittances contribute a remarkable 10 percent of national income. The established remittance services Western Union and MoneyGram commonly charge more than 10 percent in fees. Bitcoin remitters, by contrast, are charging only 1 percent. As the CEO of a recently launched bitcoin remittance service remarked to a reporter: “We thought: with

Bitcoin we can do it cheaper.” A Filipino working in Singapore or Hong Kong (say) doesn’t need to have online access or a Bitcoin wallet. The worker can purchase bitcoins at a BTM (bitcoin teller machine), bring the QR code printout to the local “reittance” provider’s office, and the service delivers Philippine pesos as a direct deposit into a designated recipient’s account at a participating bank back home or (for an addition fee but still much less than the legacy firms) as cash (Ferraz 2014, Buenaventura 2014).

Market Competition

The market for cryptocurrencies has always been characterized by free entry. A new development in the past two years is competition from profit-seeking enterprises. Free entry is exhibited by the remarkable growth in the number of altcoins, from the 13 listed in May 2013 to the 500+ listed in March 2015. Profit-seeking by new entrants is especially conspicuous in systems like Ripple (2nd behind Bitcoin in market cap as of March 9, 2015), BitShares (4th), Nxt (6th), and MaidSafeCoin (8th). In each of these systems a substantial share of “pre-mined” coins was initially held by their developer-entrepreneurs. The entrepreneurs hope to profit by raising the coin’s market price through efforts to promote wider use of the coin and its associated proprietary payment network or trading platform, such that they can eventually realize a market value for their coin holdings greater than their expenditures on development and promotion.

Bitcoin, by contrast, was launched by a pseudonymous programmer (or set of programmers) apparently as a public-spirited experiment. Revenue from producing (“mining”) new coins, the reward for validating peer-to-peer transfers, is open to anyone with the computing power to participate successfully. While Federal Reserve Bank of Chicago economist François Velde (2013) is thus right to contrast the nonprofit Bitcoin system to the profit-seeking firms that Hayek (1978a) foresaw, the contrast does not apply to the new enterprises that are launching altcoins for profit.³ In these new altcoin enterprises

³Velde also writes that Bitcoin does not “truly embody what Hayek and others in the ‘Austrian School of Economics’ proposed.” But I would distinguish Hayek’s *proposal*—to allow free choice and private competition in currency—from his *prediction* about what type of money would then dominate the field.

we see a working embodiment of competitive issue of irredeemable money by profit-seeking private firms. It is no longer correct—if it ever was—to say that Bitcoin is not “operating in a competitive environment.” Bitcoin competes with altcoins in the same way that the giant nonprofit YMCA competes with smaller nonprofit and for-profit health clubs, or a large nonprofit hospital competes with smaller nonprofit and for-profit immediate-care clinics.

The Novel Implementation of Quantity Commitments

We should not be too surprised that the features of competing irredeemable privately issued currencies are different from what Hayek (and other economists) imagined, for two reasons. First, market competition is a discovery procedure as Hayek (1978b) elsewhere emphasized, in which successful entrepreneurs discover profit in overlooked or unforeseen ways of producing products and reconfiguring product features. Secondly and more specifically, Hayek imagined that the issuer of a successful irredeemable private currency issuer would retain discretion to vary its quantity. The issuer would promise (but not make any contractual commitment) to maintain a stable purchasing power per unit.⁴ A naked promise of that sort unfortunately appears to be time-inconsistent (Taub 1985; White 1989: 382–83; White 1999: ch. 12). An issuer whose promise was believed could reap a large one-time payoff by spending a massive batch of new money into circulation until the public caught on. The one-time profit would exceed the normal rate of return from staying in business. By assumption, there would be no legal recourse against the decline of the money’s value. Aware of the problem, the public would not believe the promise to begin with, giving the money zero value in equilibrium.

The traditional solution to the problem of giving a privately issued money a reliably positive value is a redemption contract, an enforceable money-back guarantee or *price commitment* (White 1989). Under the gold standard, a banknote was worth \$20 when the bank of issue was bound to pay a \$20 gold coin for it. Today a

⁴Benjamin Klein (1974), in a more formal model, supposed perfect competition among issuers on “rental price”—that is, the risk-adjusted rate of return to holding money—in an environment of perfect foresight or the equivalent (see White 1999: ch. 12).

bank deposit is worth \$100 when the bank is bound to pay \$100 in Federal Reserve Notes for it. A suitable medium of redemption has a value that is known and independent of actions by any particular bank of issue.

Ronald Coase (1972) identified an alternative solution to the problem—how an issuer is to bind himself not to run down the price of the thing issued—in the context of a monopolist selling a durable good priced above marginal cost. To get customers to pay \$200 for an art print when the marginal cost of producing a duplicate copy is \$1, the artist must convince them that she will not run off and sell lower-priced duplicates in the future. To commit herself, the artist produces the print in a numbered edition with a stated maximum (“this print is #45/200”), providing an enforceable *quantity commitment* that she will issue no more than a fixed number of prints. Despite discussing this solution years ago (White 1989), I did not foresee that a quantity commitment could be used in practice to launch a successful irredeemable private currency.⁵

It is this second solution that Bitcoin has creatively introduced to the field of private currency. The implementation uses an entirely new technology: the limit on the number of Bitcoin units in the market is not guaranteed by a contractual promise that can (with some probability) be enforced on an issuing firm, but rather by a limit having been *programmed* into the Bitcoin system’s observable source code and being continuously verifiable through a public ledger (the “block chain”) that is shared among all “miners” who participate in bitcoin transactions processing.⁶ Altcoins employ the same basic idea of a programmed quantity commitment verified through a public ledger, though sometimes implemented in a different way.

Altcoin Innovations

In order to compete with the market leader Bitcoin, the developers of altcoins have understandably emulated its best features (decentralized peer-to-peer exchange, quantity commitment embedded in

⁵I believed that redeemable claims to a commodity money would be preferred over any IOU-nothing as a medium of exchange. And perhaps they would be even today, if not for government suppression of the former. For recent examples of suppression, see Dowd (2014: 1–37) and White (2014b).

⁶On the mechanics of the Bitcoin system see King, Williams, and Yanofsky (2013), Velde (2013), and Dowd and Hutchinson (2015).

an open source code, and shared public ledger), while introducing various general improvements and customizations. Most of the emphasis has been on improving speed, robustness, and privacy. A few altcoins aim to serve niche constituencies.⁷

The first generation of altcoins are nonprofit projects like Bitcoin, but tweak the Bitcoin code. Litecoin was introduced in October 2011 to provide faster transaction confirmation times (2.5 minutes versus 10 minutes). Peercoin, launched in August 2012, increases the speed even more by using a newer protocol (“proof of stake” rather than Bitcoin’s “proof of work”) that is less computationally demanding. This protocol also promises to allow participants to share in the rewards from mining without joining mining pools or buying the expensive specialized equipment that it now takes, as the result of competition, to succeed at Bitcoin mining. Because Peercoin’s protocol, unlike Bitcoin’s, does not promote the merger of miners into ever-larger pools, it is said to be less vulnerable to a possible collusive attack by 51 percent of miners.⁸ Primecoin, a later project from Peercoin’s main developer, implements a newer proof-of-work protocol (finding prime numbers) to reduce confirmation times to 1 minute.

Darkcoin, a nonprofit project launched in April 2014, and recently renamed Dash, has introduced payment confirmation “within seconds.” Dash alters the Bitcoin code to provide greater anonymity to users. Whereas the Bitcoin ledger puts every transaction and transactor address on public view, Dash transactions are “obfuscated.” BlackCoin, supported by an active nonprofit foundation and first listed in February 2014, uses a “proof of stake” protocol for speedy verification. It is connected to a proprietary trading platform, BlackHalo, that promises greater user anonymity than other systems. Blackcoin can now be spent (along with Bitcoin and Litecoin) at participating retail shops using the Coinkite debit card.

⁷While CoinMarketCap.com tracks market caps, the site CoinGecko.com ranks altcoins on a combination of market cap, trading volume, ongoing development activity, and social media buzz. In December 2014 it had Dogecoin at #2 and Darkcoin at #6, each four steps above its market cap ranking, based on their buzz factors. By March 2015 Darkcoin (Dash) had risen to #5 in market cap.

⁸On this problem with the Bitcoin protocol, see Dowd and Hutchinson (2015), who predict that it will bring Bitcoin’s demise. Whether or not they are right about that, many altcoin developers have recognized the problem and have made deliberate design changes to avoid what Dowd and Hutchinson call “inherent tendencies toward centralization, takeover, and collapse.”

Ripple, first traded in August 2013, is a cryptocurrency issued by the for-profit enterprise Ripple Labs. It does not rely on a mining protocol. A fixed stock of Ripples was “premined,” though the developers have not released them all yet. To make the fixity of the Ripple stock credible, the system follows Bitcoin’s lead in having a shared public ledger. The Ripple payment network confirms transactions through a “consensus” protocol that works *much* faster than mining protocols (5 seconds versus 1 to 10 minutes), so has a much better prospect of competing with ordinary credit and debit cards for point-of-sale transactions. The coin is only one part of the parent firm’s efforts, which include building a wholesale remittance system for “real-time, cross-border payments” between banks, cheaper and faster than the legacy Automated Clearing House system (Liu 2014). Stellar is a non-profit project that emulates Ripple.

BitShares also promises greater anonymity and ease of use. Like Ripple, it is part of a larger for-profit enterprise funded by venture capital. In this case the larger project, according to the BitShares Wiki (<http://wiki.bitshares.org/index.php/BitShares>), is an “experiment,” based on “a business model similar to existing banks or brokerages,” to enable the creation and trading of “BitAssets,” digital derivative contracts on “the value of anything from dollars, to gold,” to exchange-traded equities, bonds, and commodities. The project exemplifies what two *Wall Street Journal* writers (Vigna and Case 2014) describe as “so-called Bitcoin 2.0 technologies—those bitcoin-inspired software applications that bypass financial middlemen and allow almost any asset to be digitized and traded over a decentralized computer network.”

The niche-market strategy of CannabisCoin is to offer a payment service for medical marijuana dispensaries and other cannabis retailers whose access to bank accounts and credit cards is currently being blocked by the federal government even where their business has been legalized at the state level. In October 2014, the coin’s promoters were seeking retailers willing to provide a specific type of cannabis to patients at one gram per one CannabisCoin. Whether this will lead to the institution of a new commodity money standard remains to be seen, however, as the number of participating retailers and their supplies were quite limited. The promotional effort appears to have helped the market cap of CannabisCoin to surge ahead of other cannabis-themed

cryptocoins, such as the earlier-launched Potcoin and the more recent MaryJaneCoin.

Auroracoin is an Iceland-only altcoin introduced in February 2014 for the purpose of helping Icelanders evade the country's exchange controls. (The controls, which included a ban on Bitcoin purchases, were imposed during the financial crisis in October 2008 and are still in place.) Scotcoin, launched by an Edinburgh venture capitalist in May 2014, in advance of Scotland's independence referendum, is likewise a nationally specific enterprise. Its backer has expressed the hope (Hern 2014) that "introducing a voluntary cryptocurrency, which may in the future act as a medium of exchange for the Scottish people, can only benefit them should there be major disruption." A recent entry is CzechCrownCoin, launched October 2014, at least half of which is being distributed to Czech citizens. None of these national coins had a March 2015 market cap above \$55,000.

But Aren't They All Just Bubbles?

A quantity commitment solves the problem of making a credible commitment not to overissue. But it has a major shortcoming when applied to currency. Unlike a price commitment, it leaves the market price of the currency to vary with demand. This explains how it is possible for the prices of Bitcoin and other cryptocurrencies to be as volatile as they have recently been (Luther and White 2014). And it explains how it was possible for several altcoins, when enthusiasm for them evaporated, to decline to near-zero market cap.

The collapse of several altcoins is readily evident on CoinMarketCap.com. Three of the earliest thirteen altcoins have declined substantially in market cap. Terracoin, which at its peak had a market cap of \$7.1 million, is now (March 2015) down to around \$23,000, a decline of more than 99 percent. Freicoin, which peaked at \$16.1 million, has fallen to around \$61,000, also a decline of more than 99 percent. The whimsically named BBQCoin, having peaked at \$7 million, now trades around \$21,000, another 99+ percent decline. All three had very sharp run-ups to their peaks in early December 2013, mostly reversed by month's end. Megacoin, first listed in July 2013, experienced the same December 2013 pattern, soaring from \$1.2 million on

November 23, 2013, to a peak of \$47.5 million on December 1, then sliding to around \$328,000 today, a decline of more than 99 percent. Later-peaking examples of altcoins suffering 98 percent or greater peak-to-present declines have included Mooncoin, CryptCoin, Scotcoin, Bitgem, and CrtCoin.

Looking only at the market cap charts, the most remarkable case appears to be Auroracoin, which quickly climbed to chart a recorded market cap of \$953 million, but is valued today at around \$46,000, a drop of more than 99.99 percent. The incredible valuation of nearly \$1 billion was, even at the time, a misstatement. The Auroracoin launch plan (Hern 2014) was to jump-start enthusiasm by giving away about 30 premined coins to every Icelandic citizen, for a total of 10 million units. (Such a giveaway is known, in honor of Milton Friedman's famous thought experiment, as a "helicopter drop" or "airdrop.") Dividing the CoinMarketCap.com peak valuation by the price on that day (March 4, 2014) indicates 10 million units in the market, when the number of coins actually available was one-hundredth of that figure (Torpey 2014), the airdrop having yet to be made. Multiplying the price by the actual number of coins, the true market cap was one-hundredth of the reported value, around \$9.53 million. A drop from \$9.53 million down to the current \$46,000, however, is still a 99+ percent drop.

The repeated experience of crashing altcoins, in which the market valuation of a once-popular cryptocurrency all but evaporates, suggests in retrospect that the prices of *those* coins, at least, were simply bubbles. That is, such a coin's demand was unsupported by any price-independent usefulness that would put a floor under its equilibrium market price. (By contrast, industrial and ornamental uses support gold's market value.) To understand the argument, consider again the example of an artist's print. Some print buyers are presumably not just speculators who will put the print in storage and hope for its price to rise, but art-lovers planning to hang it on the wall and enjoy the real aesthetic pleasure it provides. That enjoyment is independent of its price. An irredeemable currency, by contrast, is presumed in standard monetary theory to be held only in order to be later spent or sold. It provides no service that is independent of its market value. People thus presumably have a positive demand price for any irredeemable currency, giving it a positive market value, only to the extent that they expect it to have a future market value. A market

valuation anchored by *nothing* but expectations of market valuation is the definition of a bubble.⁹

Does this logic show that the prices of all cryptocurrencies are pure bubbles? No. We cannot rule out that the flourishing cryptocurrencies have some fundamental support.

As several economists have proposed, owning Bitcoin (or other cryptocurrency) may provide a kind of real pleasure to at least some of its holders, say anti-statists who like what it stands for,¹⁰ tech enthusiasts who admire its ingenuity, or its own developers who gladly stake some wealth to help their project succeed (Luther 2013, Murphy 2013, Selgin 2014). For such an individual we can determine his affinity-based demand curve for Bitcoin by positing that he wants to own Bitcoin worth not just any old amount, but rather a specific amount of purchasing power, say 100 real U.S. dollars. (A “real dollar” here means the equivalent in purchasing power to the dollar of a specified base year.) We can plot the individual’s demand curve against the real price, i.e. the U.S. dollar price of Bitcoin divided by the dollar price level. The individual’s demand curve will be a rectangular hyperbola, a familiar construct in the basic theory of a fiat money’s value. The market demand curve sums all the individual demand curves. At a given U.S. dollar price level, if ten thousand individuals want to hold an average of \$100 worth of Bitcoin each, just because Bitcoin is cool, then the market cap of Bitcoin must be at least \$1 million.

This account does not explain day-to-day variations in the market price of Bitcoin, but it does potentially explain why the price is above zero. In this way real affinity demand provides an answer to economist-blogger Brad DeLong’s (2013) rhetorical question: “Placing a floor on the value of bitcoins is . . . what, exactly?” Of course, if Bitcoin were to become completely uncool to *everyone*, the floor would vanish.¹¹

⁹The same argument applies to any fiat money, to the extent that its market value exceeds whatever floor value it has due to exclusive tax receivability or other government compulsion. No cryptocurrency has *that* kind of support.

¹⁰A pseudonymous commenter on the reddit CryptoMarket page (Pogeymanz 2014) writes about Darkcoin: “I have some DRK because I like what it stands for.”

¹¹DeLong (2013) also writes: “Placing a ceiling on the value of bitcoins is computer technology and the form of the hash function . . . until the limit of 21 million bitcoins is reached.” Actually, of course, Bitcoin’s source code does not put a ceiling on the market cap or *value* of bitcoins, only a limit on the *quantity*. The conceptual ceiling on *value* is Bitcoin achieving a 100 percent share of the real value of all money balances in the world (Luther and White 2014).

I previously (White 2014a) too hastily rejected this argument as an explanation of how Bitcoin first achieved a positive market price, on the grounds that it “does not deliver what the argument requires, namely, an account of how Bitcoins initially had a positive value *apart from their actual or prospective use as medium of exchange*. The value at every point in this scenario derives entirely from use or prospective use as a medium of exchange (only such use as a dollar competitor is what might [provide aesthetic pleasure], not the existence of untraded digital character strings.” I was mistaken to think that the argument has such a requirement. A positive affinity valuation of a cryptocurrency may well require the *possibility* of its taking off as a nonstate money, but that does not imply a chicken-or-egg problem. Affinity demand and hence market value can be positive before actual medium-of-exchange use begins.

The affinity account has the additional merit of being consistent with the great market cap of Bitcoin, esteemed for being the first mover, the middling market cap of altcoins that embody valuable technical improvements and have active support communities, and the low market cap of me-too altcoins. Five hundred altcoins are not all making a statement or breaking new technical ground. They have positive market caps, but most of them are slight.

A second grounding for fundamental value lies in the real demand for the sorts of payment services offered by a cryptocurrency. Ownership of a particular brand of cryptocurrency units is needed to make use of the brand’s payment system, which may offer advantages over other systems (Tucker 2014).

With regard to the “bubble” element in cryptocurrency valuation, economist-blogger Stephen Williamson (2011) reminds us that official fiat money or a commodity money likewise trades well above its fundamental value. In a case where the surplus of a currency asset’s market value over its fundamental value results from its solving a medium-of-exchange coordination problem, that surplus is a good thing because it represents value-added:

Bubbles can be good things, as any asset which is used widely in exchange will trade at a price higher than its “fundamental,” and the asset’s liquidity premium—the difference between the actual price and the fundamental—is a measure of the asset’s social contribution as a medium of exchange.

I would, however, qualify this claim by saying that the difference is a reliable measure of social contribution only insofar as it arises through voluntary trade rather than legal compulsion, and only after we subtract the costs of generating and maintaining the asset in question. It is from by adding such value that Ripple's entrepreneurs hope to profit. Unlike an official fiat currency, no part of Ripple's valuation is based on legal compulsion.

Is There a Problem of Monopoly? Is There Too Much Competition?

Milton Friedman (1960: 8) wrote of "the technical monopoly character of a pure fiduciary currency which makes essential the setting of some external limit on its amount." By "pure fiduciary currency" he meant an irredeemable or fiat currency. By "technical monopoly character" he meant that open entry into counterfeiting would drive the value of an irredeemable paper currency note down to the cost of paper and ink,¹² and all the way down to zero if ever-higher denominations could be introduced at no higher cost. Therefore, a single authorized issuer was needed to preserve the currency's value. As Benjamin Klein (1974) pointed out, however, Friedman here conflated monopoly with enforcement of trademarks. To ban the selling of knock-off perfume in bottles bearing a counterfeit Chanel trademark does not imply giving Chanel a monopoly except in the sale of Chanel-branded perfume. It does not require any restriction on the production of competing perfumes under different trademarks. Enforcing a ban on the counterfeiting of Federal Reserve Notes, or in other words having the Secret Service protect the Federal Reserve's trademark, does not require giving the Fed a monopoly on currency issue.

The counterfeiting of bitcoins (also known as the problem of "double spending") is prevented not through police work and legal prosecution by any central authority, but quite elegantly by the decentralized verification process that prevents the transfer of any coin of unattested provenance from being accepted onto the public ledger. With such effective *de facto* counterfeiting protection, the quantity of bitcoins remains on its programmed path.

¹²For a real-world example of this happening, see Luther (2012).

Velde (2013) states that Bitcoin has “a status of quasi-monopoly in the realm of digital currencies by virtue of its first-mover advantage.” By “quasi-monopoly status” he may mean only that Bitcoin has a large market share, derived from its being the first mover into (that is, creating) the market. But such a status is distinct from the usual concept of natural monopoly (or quasi-monopoly) status due to economies of scale, which denotes the ability to serve every (or nearly every) part of the market at lower marginal cost than competitors. The main static danger of a monopoly in the usual sense, whether natural or state-granted, is that the monopolist firm may restrict output to raise price above marginal cost, thwarting efficiency by sacrificing potential gains from trade. Because the quantity of bitcoin is predetermined by a program and not manipulable by a discretionary issuer, it poses no danger of any such monopolistic output restriction.

Competition from new entrants surrounds Bitcoin. The new entrants have the advantage of being able to introduce altcoins with improved features while the Bitcoin code was written five-plus years ago. The Bitcoin community can at most agree to patch the code, not to fundamentally revise it. Bitcoin does have the largest established network, but a dominant proprietary network does not imply monopoly pricing (in this context, transaction fees above marginal cost) when the market is contestable. Ripple, Litecoin, BitShares, and others entrants are vigorously contesting the market. The cryptocurrency market exhibits Schumpeterian competition from new business models rather than only static price competition.

DeLong (2013) raises an issue that is the opposite of monopolistic restriction. He worries that competition from more and more altcoins may expand the total quantity of cryptocurrencies without limit, and thereby—unless Bitcoin “can somehow successfully differentiate itself from the latecomers”—drive the market value of Bitcoin and all other cryptocurrencies to zero. He writes: “the money supply of BitCoin-like things is infinite because the cost of production of them is infinitesimal.” To consider this possibility let us suppose, for the sake of argument, that the cost of introducing a me-too altcoin is indeed infinitesimal. The economic implication is that in a fully arbitrated equilibrium the

marginal altcoin will have an infinitesimal real value (which is an approximate description of the marginal altcoins we do in fact observe). But this is not to say that the value of bitcoins (or of established altcoins) will tend toward zero. Infinitesimally valued altcoins do not eat into Bitcoin's market share in real terms. Only valued altcoins can do that, as they have since May 2013 (reducing Bitcoin's share to 87 percent from 95 percent as noted; but at the same time Bitcoin's market cap in U.S. dollars grew more than three-fold).

In the foreign exchange market for government fiat monies with flexible exchange rates, hyper-expansion in the nominal supply of dollar-like things, say Zimbabwe dollars or Venezuelan bolivars, does not drag down the purchasing power of the U.S. dollar. Likewise, in the existing altcoin market with its completely flexible exchange rates, cheap altcoins simply have low exchange value against Bitcoin and do not drag down Bitcoin's real market value.

Cryptocurrency and Fiat Currency: Comparisons and Contrasts

DeLong likens Bitcoin to government fiat money in the following way: "Bitcoin is like fiat money, and unlike 18th and 19th century Yap stone money, in that its cost of production is zero." In fact, although Bitcoin is similar to a government fiat money (and unlike gold) on the demand side, in that nothing supports its price if transaction and other money-related demand for it goes to zero, it is absolutely *unlike* a government fiat money on the supply side. It does not have an indefinitely expandable supply but the opposite. Just as monopolistic under-supply is ruled out (see above), so too is hyper-expansion. Bitcoin has a verifiably programmed commitment to a pre-specified quantity path.¹³ In light of that commitment, the

¹³Blogger Charlie Stross (2014) colorfully comments that Bitcoin "wears a gimp suit and a ball gag, padlocked into permanent deflation and with the rate of issue of new 'notes' governed by the law of algorithmic complexity." That padlocked "gimp suit and ball gag" is Bitcoin's binding quantity commitment. It is a feature, not a bug.

cost of production beyond the scheduled quantity is extremely high, not zero.¹⁴

Noting that “improvements, bug fixes, and repairs” to the Bitcoin code have been “carried out by the community of bitcoin users, dominated by a small set of programmers,” Velde (2013) downplays the prospects for Bitcoin to rival the fiat U.S. dollar:

Although some of the enthusiasm for bitcoin is driven by a distrust of state-issued currency, it is hard to imagine a world where the main currency is based on an extremely complex code understood by only a few, and controlled by even fewer, without accountability, arbitration, or recourse.

Substitute the phrase “bureaucratic agency” for the word “code” in this statement, however, and the hard-to-imagine world becomes a fair description of our current world of Federal Reserve currency. This fact completely overturns Velde’s argument. If the prospects for Bitcoin against the dollar depended only on the public’s choice between trusting an open source code with a public ledger and trusting a byzantine central bank, the prospects would look extremely good.

Bitcoin as a Vehicle Currency and Unit of Account

Finally, Bitcoin has an interesting role that is often overlooked or denied. A recent paper by a team of Bank of England economists (Ali et al. 2014), for example, declares that cryptocurrencies “are not typically used as media of exchange” and “there is little evidence of digital currencies being used as units of account.” In fact Bitcoin is the vehicle currency (commonly accepted medium of exchange), and consequently is the unit of account, in most altcoin markets. With a few exceptions (Litecoin against U.S. dollar, Chinese yuan, and euro; Chinese exchanges where altcoins trade against yuan; Peercoin

¹⁴In light of its programmed production limit, Selgin (2013) calls Bitcoin a “synthetic commodity money.” He helpfully likens Bitcoin’s quantity commitment to the quantity commitment of an artist who publicly destroys the engraved plates from which a known number of lithographic prints have been made.

against dollar), the vast majority of altcoin exchanges trade and quote prices in bitcoins, not in dollars, euros, or yuan.¹⁵

The altcoin market is structured this way for the same reason that the U.S. dollar is the vehicle currency for foreign exchange transactions (Kreuger 2012). To trade (say) Australian dollars for British pounds, the standard route is AUD for USD, then USD for GBP. Thicker markets enjoy lower bid-ask spreads. The U.S. dollar currency markets are so much larger than others that for most almost all currency pairs that do not include the U.S. dollar (euro-yen is an exception) the sum of bid-ask spreads is less for indirect exchange via the U.S. dollar than for direct exchange. This pattern is self-reinforcing by bringing more volume to the U.S. dollar markets.¹⁶ Most non-USD to non-USD foreign exchange markets are missing.

The Bitcoin-U.S. dollar market has much more volume and thus much lower spreads than any altcoin-U.S. dollar market. To trade U.S. dollars for an altcoin, often the *only* route in practice is to trade U.S. dollars for Bitcoin, and then Bitcoin for the altcoin. Most altcoin-dollar markets are missing because volume would be too low to have attractive bid-ask spreads. With by far the thickest potential markets against any altcoin, even compared to U.S. dollars, Bitcoin is naturally the vehicle currency and thus the unit of account in altcoin markets.

Policy Implications

The market for cryptocurrencies is still evolving, and (to most economists) is full of surprises. Policymakers should therefore be very humble about the prospects for improving economic welfare by restricting the market. Israel Kirzner's (1985) warning about the perils of regulation strongly applies here: Interventions that block or divert the path of entrepreneurial discovery will prevent the realization of potential breakthroughs such that we will never know what we are missing.

¹⁵See <http://www.cryptocoincharts.info/main/priceBoxes>.

¹⁶The positive network effect that makes the U.S. dollar the common medium for inter-currency exchange echoes the self-reinforcing Mengerian process by which a common medium for inter-commodity exchange (money) emerged out of barter.

References

- Ali, R.; Barrdear, J.; Clews, R.; and Southgate, J. (2014) "The Economics of Digital Currencies." Bank of England *Quarterly Bulletin* (Q3): 1–11.
- BBC (2014) "Microsoft to Accept Payments made in Bitcoins" (11 December): www.bbc.com/news/technology-30377654.
- Buenaventura, L. (2014) "The Rise of Rebitance: Reinventing Money Transfers in the Philippines with Bitcoin." *The Next Web* weblog (28 September): <http://thenextweb.com/insider/2014/09/28/rise-rebitance-reinventing-money-transfers-philippines-bitcoin>.
- Coase, R. (1972) "Durability and Monopoly." *Journal of Law and Economics* 25 (April): 143–49.
- Crockett, G. (2014) "Bitcoin Is Seen as an Ephemeral Currency." *Washington Post* Style Invitational Contest, Week 1062: Poems from the headlines (27 April): www.washingtonpost.com/entertainment/style-invitational-week-1069-big-thoughts-little-words-plus-more-from-recent-contests/2014/04/16/f556bf74-c331-11e3-b574-f8748871856a_story.html.
- DeLong, B. (2013) "Watching Bitcoin, Dogecoin, Etc." *Equitable Growth* weblog (28 December): <http://equitablegrowth.org/2013/12/28/watching-bitcoin-dogecoin-etc>.
- Dowd, K. (2014) *New Private Monies: A Bit-Part Player?* London: Institute of Economic Affairs.
- Dowd, K., and Hutchinson, M. (2015) "Bitcoin Will Bite the Dust." *Cato Journal* 35 (2): 357–382.
- Ferraz, E. (2014) "Send Home Your Wages Using Bitcoin and Avoid Hefty Money Transfer Fees? That's Now a Reality." *Tech in Asia* (3 July): www.techinasia.com/send-home-wages-bitcoin-avoid-hefty-money-transfer-fees-reality.
- Friedman, M. (1960) *A Program for Monetary Stability*. New York: Fordham University Press.
- Hayek, F. A. (1978a) *The Denationalisation of Money*, 2nd ed. London: Institute of Economic Affairs.
- (1978b) "Competition as a Discovery Procedure." In Hayek, *New Studies in Philosophy, Politics, Economics, and the History of Ideas*. London: Routledge.
- Hern, A. (2014) "Bitcoin Goes National with Scotcoin and Auroracoin." *The Guardian* (25 March): www.theguardian.com

- /technology/2014/mar/25/bitcoin-goes-national-with-scotcoin-auroracoin.
- King, R. S.; Williams, S.; and Yanofsky, D. (2013) "By Reading This Article, You're Mining Bitcoins." *Quartz* webzine (17 December); <http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins>.
- Kirzner, I. M. (1985) "The Perils of Regulation: A Market-Process Approach." In Kirzner, *Discovery and the Capitalist Process*, 119–49. Chicago: University of Chicago Press.
- Klein, B. (1974) "The Competitive Supply of Money." *Journal of Money, Credit, and Banking* 6 (November): 423–53.
- Krueger, M. (2012) "Money: A Market Microstructure Approach." *Journal of Money, Credit and Banking* 44 (September): 1245–58.
- Liu, A. (2014) "Ripple Labs Signs First Two US Banks." *Rippleblog* weblog (24 September): <https://ripple.com/blog/ripple-labs-signs-first-two-us-banks>.
- Luther, W. J. (2012) "The Monetary Mechanism of Stateless Somalia." Kenyon College Working Paper, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2047494.
- _____ (2013) "Cryptocurrencies, Network Effects, and Switching Costs." Mercatus Center Working Paper No. 13–17, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134.
- Luther, W. J., and White, L. H. (2014) "Can Bitcoin Become a Major Currency?" *Cayman Financial Review* (August): www.compass-cayman.com/cfr/2014/08/08/Can-bitcoin-become-a-major-currency.
- Murphy, R. P. (2013) "The Economics of Bitcoin." *Library of Economics and Liberty* (3 June): www.econlib.org/library/Columns/y2013/Murphybitcoin.html.
- Pogeymanz (2014) Comment in the Thread "Darkcoin Is Going to Be a Behemoth," www.reddit.com/r/CryptoMarkets/comments/20t9nc/darkcoin_is_going_to_be_a_behemoth.
- Selgin, G. (2013) "Synthetic Commodity Money." University of Georgia Working Paper, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.
- _____ (2014) "Mises Was Lukewarm on Free Banking." *Liberty Matters* (January): <http://oll.libertyfund.org/pages/misestmc>.
- Stross, C. (2014) "Schadenfreude." *Charlie's Diary* weblog (25 February): <http://www.antipope.org/charlie/blog-static/2014/02/schadenfreude-1.html>.

- Taub, B. (1985) "Private Fiat Money with Many Suppliers." *Journal of Monetary Economics* 16 (September): 195–208.
- Torpey, K. (2014) "Auroracoin's Market Cap Is Highly Inflated." *Cryptocoins News* (4 March): www.cryptocoinsnews.com/auroracoin-market-cap-highly-inflated.
- Tucker, J. (2014) "What Gave Bitcoin Its Value?" *The Freeman* (27 August): http://fee.org/the_freeman/detail/what-gave-bitcoin-its-value.
- Velde, F. R. (2013) "Bitcoin: A Primer." *Chicago Fed Letter* 317 (December): www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.
- Vigna, P., and Case, M. J. (2014) "BitBeat: Ratings Firm Coinist Tackles Trust Problem with Bitcoin 2.0 Projects." *Wall Street Journal MoneyBeat* weblog (12 August): <http://blogs.wsj.com/moneybeat/2014/08/12/bitbeat-ratings-firm-coinist-tackles-trust-problem-with-bitcoin-2-0-projects>.
- White, L. H. (1989) "What Kinds of Monetary Institutions Would a Free Market Deliver?" *Cato Journal* 9 (Fall): 367–91.
- (1999) *The Theory of Monetary Institutions*. Oxford: Basil Blackwell.
- (2014a) "Ludwig von Mises's The Theory of Money and Credit at 101." *Liberty Matters* (January): <http://oll.libertyfund.org/pages/misestmc>.
- (2014b) "The Troubling Suppression of Competition from Alternative Monies." *Cato Journal* 34 (Spring/Summer): 181–201.
- Williamson, S. (2011) "Bitcoin." *New Monetarist Economics* weblog (24 June): <http://newmonetarism.blogspot.com/2011/06/bitcoin.html>.

WHAT DOES \$100 ETHER MEAN?

medium.com/humanizing-the-singularity/what-does-ether-100-mean-bb58522f781e

VINAY GUPTA

May 5, 2017



◆ Ethereum (ETH)

\$100.98 (25.90%)

0.06350350 BTC (18.68%)

Today, [Ether](#) hit \$100 (may 2017, when this piece was written. update: it's \$300 now, five weeks later. update: it's worth \$132 now, 18 months later. you see how this goes). I'm sure by the time you're reading this it will be in The Guardian and the New York Times as a curiosity piece. Our market cap will approach thirty billion dollars. By all and any standards, this is a success beyond anything dreamt of when the project started, and the money raised will continue to finance

technical innovation for years to come. While the impact and worth of a technology cannot be measured by money alone, on this occasion, celebration is appropriate. We have done well.

For those of you who are new to the Ethereum show, let me explain what has just happened.

Two years ago, I wrote [Programmable Blockchains In Context](#), the Ethereum launch post. It was a huge success, sat on the front page of Hacker News for a day, and really set the conversation and tone around the Ethereum project, without over-promising. I've learned a few things about explaining Ethereum now, and it's not exactly what I would have written with hindsight, but it's close enough that if you want the full depth chapter-and-verse on this new technology, that's where you'd go. If you need more depth, the Ethereum Whitepaper by Vitalik Buterin, our leader, is still an absolute marvel of clarity and deep thinking. But assuming you are a more general reader, let me explain briefly what the technology is, so we can talk meaningfully about what \$100 Ether means.

Ethereum is a programmable blockchain. It was created by a small team built by Vitalik Buterin, who was (at the time the project started) famously young—a CEO of a 20 person team with \$18m of bitcoin in the “bank.” Many members of that team are remarkable in their own right: Joe Lubin who went from Wall St. to found Consensus Systems, a major New York company building out the blockchain future. Dr Gavin Wood, of Parity, a truly remarkable computer scientist. Dr Jutta Steiner, also of Parity. It grew into a large team, made of remarkable people, and I'm just namechecking a few. Over the couple of years the project took, the team grew, fragmented, splintered, reunited, forged ahead. The first year, the year before I joined, is truly the stuff of legends.

Anyway, that's the cultural context. A 20 year old kid and a bunch of funny-looking villains pull together this remarkable piece of technology which, at the time, we thought was going to change the world, and now it has.

So what does it do, this programmable blockchain that's worth ten billion dollars? Well, let me explain. A blockchain is a way of arranging a lot of computers together to do the same thing. It's a bit like Dropbox or Google Docs or any other syncing technology that moves pictures from your phone to your laptop or whatever. The difference is that it's syncing thousand and thousands of computers. If a few machines drop offline or get hacked, the network does not even notice: the consensus of all the machines which have the same data overwhelms the occasional drop outs. The computers form a choir, and they never forget the chorus.

This blockchain has two remarkable features. The first is the way that it pays for all those computers. On the head end of the blockchain there is a sort of roulette wheel. Five times a minute, the wheel gets a spin, and one of the computers which is helping to run the blockchain gets a prize of [5 Ether](#) . This award is noted down in the blockchain, and synced to all of the computers in the system. The lucky winner can transfer this ether to another person (identified by their cryptographic code address) in exchange for, say, goods, services—or cash.

So this hundred dollars per Ether price that you see, that's \$500 every twelve seconds, \$2500 a minute, \$3.6 million dollars per day pouring out of cyberspace into the pockets of those lucky enough to have computers helping to run and sync the blockchain—the computer system which stores their winnings is paying for itself by issuing those winnings. It's a perfect self-generating system, just like Bitcoin was before it. So that's where the money is coming from, should you be too

embarrassed to ask! For historical reasons, they call this process “mining.”

The second property of this programmable blockchain is even more remarkable. Programmability is a funny thing: when a system does a simple job, like Bitcoin (which has more or less the same mining dynamics as I outlined above for Ether) it’s easy to understand, easy to secure. But you add some element of programming to the thing—not just coins are mined and exchanged, but somehow this whole thing is software too? Well, that’s where things get complicated.

Ethereum incorporates Smart Contracts. Smart Contracts are the reason I came back into this kind of work, more than two decades after I’d been exposed to the original ideas on the Cipherpunks mailing list all those years ago. I’d left the field, only dipping back now and again to keep my perspective fresh, but when I heard a smart contract ecosystem was being built, it pulled me back out of my retirement from matters cryptographic. I came running.

A smart contract is a tool for changing the world. We have this mental model of all these computers synced together. Now imagine that rather than syncing a transaction: 5 Ether go to Bob in the reward lottery, or 22 Ether go to Helen from Fred’s account, we do something else. What is this something else? We sync software. I upload a program—needfully small, because it’s going to thousands of other machines—and we secure that syncing process using all the same sync-and-mining approaches taken to cash-only blockchain like Bitcoin’s.

Every machine in the network runs the same small program. It could be something simple, like a loan: I send you some money, and your account automatically pays it back, with interest, a few days later. If you can’t pay, a third party covers

your debts, and it's all locked in at the start—your consent, my consent, and their consent. We all agree to these terms, and it's locked in using the smart contract. We have achieved programmable money. You might say that this doesn't sound very complicated or impressive, but just wait and see where this goes.

What kinds of things can you do with programmable money? Nearly the entire financial system is built from programmable money. They don't call it that, of course, but the loans and bonds and derivatives and futures and mortgages and credit default swaps and all the rest? Although at the very bottom of the stack, right in the guts of the system they might eventually be represented by a paper contract, in fact they're represented as software for almost every step in their evolution. An individual mortgage might be a paper contract between a person and a bank, but a hundred million mortgages in the mortgage system are pure digital: software representing homes, offices, warehouses, cars, land—and more ephemeral items like airline tickets and concert tickets and even the music itself in a digital download. All of this, and more, is just software representing value, programmable money singing its songs of desire and achievement across the wires.

In short, programmable money builds the world. And Ethereum is new programmable money.

Now, as a new system, Ethereum is a little crude. Probably the longest smart contract in current use is about 2000 lines, and that's compared to around 6 million lines of code for the F35 warplane. These are little baby steps: enough to implement a simple bond, but maybe not all the super complicated contingency management that you might get in a real paper bond contract. But in the pure digital world of the blockchain, the vast majority of the things which can go wrong with a bond in the messy real world just can't happen.

So there's a tradeoff—simpler, kind of abstract systems which work inside of this blockchain universe, which lack the sophistication of the main financial system, versus the big old clunky machinery which occasionally runs into crises like not being able to find mortgage paperwork when house repossessions roll around during an economic contraction, because the mortgages were being moved between banks carelessly. It's early days on this new frontier, and we are still in the trial-and-error phase of blockchain developments—we don't know the best way to use the power of these amazing new tools, but the hundreds of prototypes done by big companies and banks make it pretty clear what the general consensus is: this tech is going somewhere.

The last piece of general magic we need to consider is this. Every bank has its own ferociously complex, and incredibly expensive and usually very delicate, computer system for managing all of the bank's assets—the customer accounts (your money!), the bank's assets (your house!) and all of its complex obligations to regulators, to other banks, and so on. The whole bank is in there: the bank is the software, and the software is the bank.

And the financial system is made of tens of thousands of these institutions all networked using crude, old, unreliable computer systems in many cases. Technical processes are slow, as anybody who's ever sent a wire transfer will attest. Systems are inscrutable: when you hit a problem with your bank, it's you who has the problem. Accountability is slow, and often painful to extract.

But the blockchain is different. Every one of those thousands of machines we referred to earlier, running their copy of the blockchain software, is a full peer. Each one carries with it all the transactions in the system, and each node can—as long as the software can carry the tune—run its own code. Systems like Bitcoin or Ethereum have many, many

implementations. As long as they can all smoothly work together (and bugs at this level are, indeed, very rare) the whole thing works like a single machine. That nobody owns.

That nobody owns!

There is no “Bitcoin Corporation” or “Ethereum Incorporated.” There are some charities which help write the software, but the actual networks are not run by anybody, any more than the internet itself is run by somebody. The full peers, the computers which make up the network, are all owned by different people. They interact in pretty much the same way that computers interact when they are passing along email or other messages—a message can flow over dozens or hundreds of other computers before it reaches your mailbox, and those machines can be owned and run by almost anybody. The nature of the internet is that it is a network of networks: nobody owns the entire thing, everybody owns and manages their own piece, from your laptop and your cellphone, through to the local area network that manages your machines at work, up to the big fibre line installations done by AT&T. Nobody owns the internet, and we get along just fine.

So to recap, this crazy little system that was launched only a couple of years ago, that mines its own currency through a strange lottery system, that stores little programs which represent financial instruments or games of chance or skill—or whatever programmers want them to represent—this little system is trading at \$100 per ether, or nearly \$10 billion dollars?

Yes.

Now let’s try to understand why.

Bitcoin is Ethereum's parent. It's a bigger, older, surly beast, much beloved by non-State anarchists and American libertarians. It was built on a promise of issuing a sort of digital gold, a central bank of the internet, a new reserve currency backed by pure mathematics. It was intended to be fully decentralized, with all that tricky "mining" work we talked about before done on everybody's home laptops, scattered all over the world for security.

In practice Bitcoin has fallen a fair bit short of that. The mining thing rapidly centralized in the hands of a relatively small number of miners, and the initial hard line Libertarian position softened as taxes needed to be collected and paid, and the original bold vision came up rather short in contact with cold reality. But this was not to say that Bitcoin was a failure in any way, shape or form: the ideas behind Bitcoin certainly ran into trouble as they encountered regulation, but the actual technology and all-important community adoption soldiered right on. Tonight, while Ether passes the \$100 barrier, Bitcoin hovers around \$1700 for a total of more than four times Ethereum's total market value. Bitcoin is also succeeding. It's being used for buying coffee, buying pot (notoriously, on the dark markets), and making international money transfers for bargain basement prices. It's the face which launched a thousand ships (altcoins), some of which have also recently broken the billion dollar total coin value threshold. Bitcoin enables trade, as simple as that, and understood in these terms is an unmitigated success.

Ethereum never had that kind of clarity of political purpose. The team tended towards a mild left-green bias, that I might unfairly summarize as "radicalized Guardian readers" with, of course, a few outliers. I certainly fit that description. The general bias of the project has always been to get things done, and let the future figure out what the tools are for. We talk about decentralization, perhaps as a proxy for freedom or

at least economic freedom, and we think the ownerless nature of the network is inherently a good breeding ground for democratic ideals. But there probably isn't, and never was, a single coherent political ideology behind Ethereum.

Rather, there's a vision about the future of society and global trade. I'm going to try and articulate that vision for you now.

Right now, when a group of people want to get something done, usually they put somebody in charge. That person is sometimes a leader, and sometimes a facilitator. The facilitators are theoretically neutral parties which are just there to get the job done, on behalf of the people they serve. They should be, ideally, neutral functionaries. The leaders we pay to have informed opinions which are better than our own ideas, but the facilitators we pay to be neutral voices. But in practice these facilitators are often so powerful that they apply pressure to the whole of society, and in fact often step in and usurp the jobs which should be left to leaders: corporate lobbyists pushing agendas on our elected officials, for instance. The result is a world in which nearly any organization which truly enjoys economies of scale—from a national grid through to Wal-Mart—will tend to reconfigure the environment in ways which make it more profitable. We create these giants in the name of efficiently serving our needs, but they wind up ruling over us as if we had elected them with every dollar of our spending.

I believe the Ethereum vision of the future of the human race is different. Rather than constantly being hassled by our intermediaries—from Google through to the Department of Motor Vehicles—the idea is to disintermediate and deal directly with our neighbours and friends and strangers alike, to get the job done ourselves. Some people called this disintermediation—a direct relationship between two people without a middleman. But I think the correct emphasis is not on what we are taking away (the intermediaries) but on what

we are creating: direct communications between people, which are capable of storing and transmitting economic value.

Now that is a bit of a mouthful, so let me break that down to the basics.

We have this programmable blockchain. It's a computer system made up of lots of computers scattered all over the world. Different people own those computers. Different software runs on those computers. But all these people, machines and software collaborate to create a secure system which generates value in the form of digital tokens called Ether. People can transfer value and make simple contracts on this machine made from so many diverse elements.

Some would call this system disintermediated. But I prefer to think of it as direct. Yes, there is an intermediary between you and I if we trade on this system: in fact there are many intermediaries—every miner, every person writing the software, and all the internet providers and so on along the way. But, unlike the banking system, the intermediary in the Ethereum universe has no agenda: it doesn't make policy. It doesn't make rules. It doesn't surprise you with unexpected fees. It doesn't change the rules of the game between you kicking the ball and it arriving in the goal. The intermediary in Ethereum is transparent: it simply serves to carry out your will, your instructions.

And this is the core vision of the Ethereum community: a world in which two people can deal directly with each other, and the systems that support their interaction don't distort the message as they carry out our instructions. You say what you want, and the machines carry your instructions to the person on the other end of the deal. Directness is the real fruit of disintermediation: people dealing as they would face-to-face, but with the benefit of a network.

I went to Norway recently, and I suggested at a [talk I did](#) that we could move Scandinavia very quickly to experiments involving a blockchain for payments, fully supported by their government, on the basis that taxation could be built directly into the platforms they might use (it's unlikely, today, the Norwegian government could collect taxes in Ether not Kroner!). In a system like this, the social contract of the country would be represented directly in the medium-of-exchange: a 15% cut to run a welfare state and provide world class healthcare to everybody is as natural to that environment as a fully-transparent end-to-end system with zero taxes feels to Libertarians. The precise configuration of your payment systems implements your social values, and this is an enormous lesson for all of us: there is no neutral medium, only one that shares your values, which you then perceive as neutral.

So here we are, at (or perhaps just slightly under) \$100 USD per Ether. I promised you I would tell you what it means.

It means that enough people are rallying around this vision of the future, and putting their money on the line for it, that the core development teams and entrepreneurs building that future will be funded more-or-less indefinitely. It means that there's a massive wave of product innovation as people try to figure out how to get the millions of Ethereum users to spend their money on our products, and that evolutionary process builds further into the potential that the Ethereum system has to satisfy real human needs and desires. The system is learning to take care of us. Without arbitrary interference by middlemen, it may be quite a rapid adaptation.

On a personal note, I pushed very deep into the theory around Ethereum and Direct Trade (Decentralization) since Ethereum launched. I came back with three fundamental results.

1. The [Dubai Blockchain Strategy](#) which set one of the most innovative nation states in the world on a new track relative to this technology, which was then backed up in Dubai by a second piece of work (in collaboration with Consensys),
2. The [Internet of Agreements](#) , which I'll discuss more below, which pulls together many of the loose threads in the Decentralization discussion into an easier-to-express whole.
3. The Harvard Business Review pieces, which expand in many directions, including [Globalization 2.0](#) (blockchains to protect world trade during deglobalization) and a rather wonderful (unpublished!) piece on Leapfrogging to blockchains in the developing world.

No ICO, and no blockchain startup (per se) for me. Why not?

I decided, on close examination, that the weakest link in the ecosystem was the willingness of broader society and mass culture to pull us into the mainstream. While I could be deep in the tent doing financial architecture or designing business models for new ICO projects, where I wanted to be was on the periphery, perceived as being “in the real world,” building on ramps for blockchain projects to break out of the microculture they currently exist in, and get all the way into the mainstream. I've supported quite a few projects from mostly behind the scenes, though.

I've also built up a very, very solid stack of theory which is being packaged as concepts like the Internet of Agreements. I hope this framing of our work will stick to the mainstream and make it far, far easier for us to build this future together with the main productive forces in society (rather than being set up in false opposition to them—the worst mistake that Bitcoin made!)

I phrase it like this:

- In the beginning there was the Internet of Ideas, back before...
- Online credit card processing gives birth to Amazon and the Internet of Shopping
- Blockchains bring the rest of our financial instruments online beside the credit card, giving rise to the Internet of Agreements. The internet finally gets a native representation for deals that is better than emailing PDFs back and forwards.

The Internet of Agreements is a pretty simple concept: two (or more) people negotiate a business deal. There's a computer in the room, a bit like Amazon's Alexa, to take notes. When it's pretty sure a deal has been done, it displays the terms to the participants to fine tune, and if they agree, a smart contract is prepared which reflects those terms. Of course that's an AI problem, and a hard one. This part is a little futuristic. But I want to look forwards about 10 years, and in that time frame, all this seems possible. And of course, on the back end, robots and self-driving cars and automated warehouses and factories do the majority of the work. I think this kind of relationship between us and our machines is more-or-less inevitable. I think of this as a picture of what it will all turn into when it grows up, much like Ted Nelson's concept of Hypertext guided internet development for many, many years. To me, the Internet of Agreements is a simple image of where we are going, and is a vision we can all get behind. Almost nobody disagrees with the Internet of Agreements as a goal, and it seems to meet the inevitable curve of both technology and society.

The Internet of Agreements gave me what I was looking for: a largely technologically-neutral and politically-agnostic goal state. It's naive to say that politics don't matter—they do, they're vital. But at a 10 year horizon it's so difficult to imagine how things will be, and debates of today will be

seem long-settled by then. Important technical hurdles remain, including Proof of Stake and the entire Scaled Blockchain debate. I don't know, and I don't want to second guess, exactly which technological solutions will work out best: Ethereum must speed up, but I don't want to specify exactly how I see that happening, because I am unsure. I wanted something that I could drive towards that was simple enough it could be explained casually, broad enough that most of our emerging technologies in trade facilitation could fit in somewhere, and far enough away that nobody was going to argue too much about the precise details. In short, I wanted a vision. Not a road map of the next two or three years, looking at lightning networks and snarks, but out 10 years, out when all is said and done.

I think Ether at \$100 means that so many people believe in the world they think Ethereum will create, that it is becoming inevitable. I suspect that the full implementation of that vision will be a lot more humane and user-friendly than most of what people are thinking about right now, and I suspect that a settlement of the issues around nation state law and smart contracts will be settled by automated compliance checking (i.e. smart contract testing by regulatory oracles) rather than by wholesale end-runs around democratic sovereignty in favor of libertarian ideals. I don't know that for a fact, but that guess is also built into the Internet of Agreements model of the world.

Regardless of how the technological details are worked out, I am more convinced than ever that the smart contract ecosystem is here to stay, because people want it, they need it, and it solves problems they face regularly. It may well be used by ordinary people 50 times a day without ever realizing they have touched it. The coffee is hot and waiting for you when you arrive in the coffee shop, your lunch has a picture of the person who caught the tuna with a fishing line printed

on the side, the solar panels are gleaming in the sun, and the computers are matching the supply to demand at the right price. That's the vision of the smart contract world: stuff just works, because the computers just work. And that's what we are building now.

So right now I'm at the next frontier. I'm building a new set of concepts, called Humanizing the Singularity, to help us navigate these tricky waters. That's similar to the work I did on explaining Ethereum and teaching people ways to explain it. The Internet of Agreements and Globalization 2.0 explain the blockchain and associated futures in a simple, easy to deal with package. Later this year, Autumn, we will have a big Internet of Agreements conference to push the field further, really pushing on bridge building between blockchain and AI, and blockchain and advanced logistics solutions. Shortly after that there'll be a paper or two on AR/VR, and an attempt to make sense of that field in a way that lets people get to grips with it faster. Then in 2018 there will be the long-time-coming strategy on AI. The blockchain weaves through all of these areas, like the internet itself, giving persistence to virtual property, flagging ownership of drones or robots, and giving AI problem solving a way to interact with the real world.

Now, a final word on the ICO situation.

I've always tried, often unsuccessfully, to be a voice of conscience in the Ethereum community. Right now I see a lot of very good ideas attracting huge amounts of funding very fast, and that's great. And if that was all that was happening, that would be great. But the more of a mess people are making with legal shoddiness, technical ineptitude or carelessness, and improper handling of investor interests or identities, the worse the mess is going to be if it all has to be untangled. If this ecosystem is to stabilize, it will be because people ran a tight ship, did exactly what they promised to do, got the details right, dealt sensibly with regulation where

applicable, and gave good value for hard-earned cash. I want to sound that note of caution now: I was right to feel uneasy about the original DAO, and did not speak out loudly enough. Self-governing is good, but it must be maintained at the highest standards of ethical integrity to hold up in the long run.

Much as I'd like to raise \$100m in 24 minutes in an ICO to re-invest in building out the core technologies to connect Ethereum to everything else, I just can't see a way of doing it that gives us the flexibility down the line to make the decisions we need to. So I've started a very conventional venture capital firm to build these technologies, and others. I hope to see you further down the line! (Late 2018 update: [Mattereum.com](https://mattereum.com), "perhaps the world's weirdest and most daring start up" —TechCrunch)

Take care, enjoy your profits, and good night.

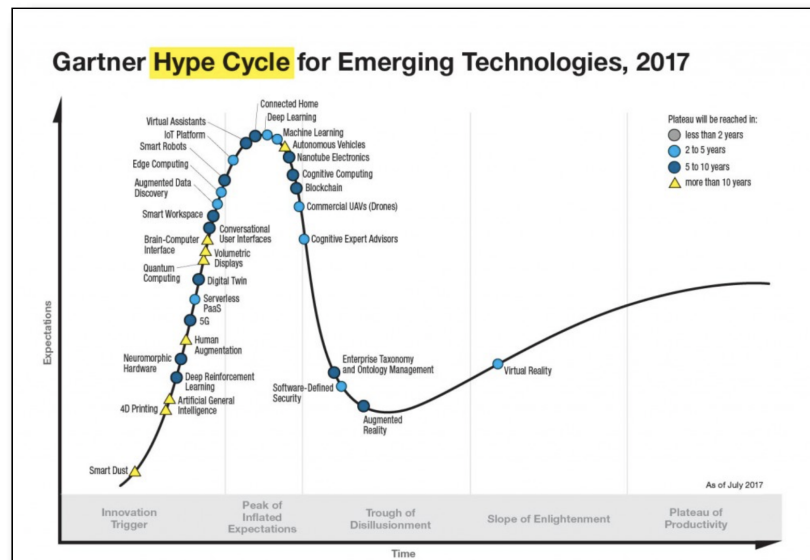
IF, WHEN AND HOW BLOCKCHAIN TECHNOLOGIES CAN PROVIDE CIVIC CHANGE

blog.p2pfoundation.net/if-when-and-how-blockchain-technologies-can-provide-civic-change/2019/01/06

GOVLAB

January 6, 2019

Stefaan G. Verhulst and Andrew Young: The hype surrounding the potential of blockchain technologies– the distributed ledger technology (DLT) undergirding cryptocurrencies like Bitcoin – to transform the way industries and sectors operate and exchange records is reaching a fever pitch.



Source: [Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017](#)

Governments and civil society have now also joined the quest and are actively exploring the potential of DLTs to create transformative social change. Experiments are underway to leverage blockchain technologies to address major societal challenges – from [homelessness](#) in New York

City to the [Rohyingya crisis](#) in Myanmar to [government corruption](#) around the world. At the same time, a [growing backlash](#) to the newest ‘shiny object’ in the technology for good space is gaining ground.

At this year’s [The Impacts of Civic Technology Conference \(TICTeC\)](#) , organized by [mySociety](#) in Lisbon, the GovLab’s Stefaan Verhulst and Andrew Young joined the [Engine Room](#) ’s [Nicole Anand](#) , the [Natural Resource Governance Institute](#) ’s [Anders Pedersen](#) , and [ITS-Rio](#) ’s [Marco Konopacki](#) to consider whether or not Blockchain can truly deliver on its promise for creating civic change.

For the GovLab’s contribution to the panel, we shared early findings from our [Blockchange: Blockchain for Social Change](#) initiative. Blockchange, funded by the Rockefeller Foundation, seeks to develop a deeper understanding of the promise and practice of DLTs in addressing public problems – with a particular focus on the lack, the role and the establishment of trusted identities – through a set of detailed case-studies. Such insights may help us develop operational guidelines on when blockchain technology may be appropriate and what design principles should guide the future use of DLTs for good.

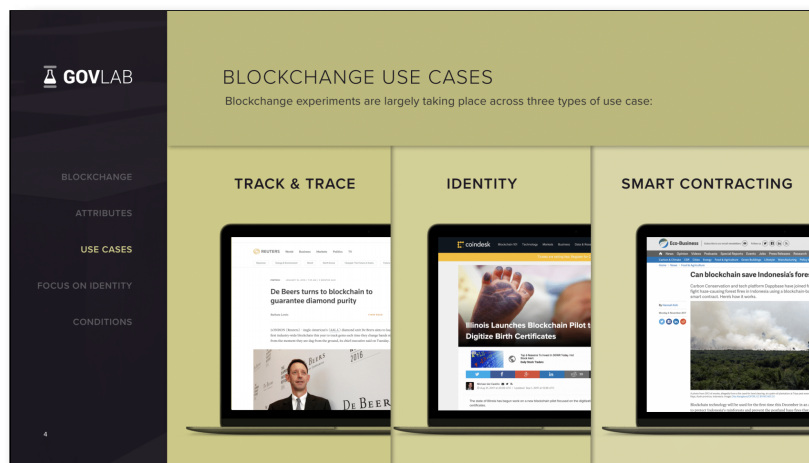
Our presentation covered four key areas (Full presentation [here](#)):

1. *The evolving package of attributes present in Blockchain technologies* : on-going experimentation, development and investment has lead to the realization that there is no one blockchain technology. Rather there are several variations of attributes that provide for different technological scenarios. Some of these attributes remain foundational — such as immutability, (guaranteed) integrity, and distributed resilience – while others have evolved as optional including disintermediation,

transparency, and accessibility. By focusing on the attributes we can transcend the noise that is emerging from having too many well funded start-ups that seek to pitch their package of attributes as the solution;

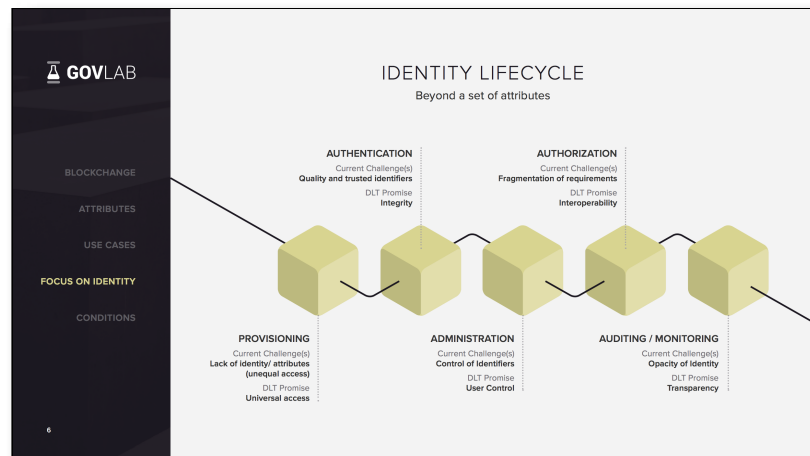
2. The three varieties of Blockchain for social change use cases: Most of the pilots and use cases where DLTs are being used to improve society and people's lives can be categorized along three varieties of applications:
 1. Track and Trace applications. For instance:
 1. [Versiart](#) creates verifiable, digital certificates for art and collectibles which helps buyers ensure each piece's provenance.
 2. [Grassroots Cooperative](#) along with Heifer USA created a blockchain-powered app that allows every package of chicken marketed and sold by Grassroots to be traced on the Ethereum blockchain.
 3. [Everledger](#) works with stakeholders across the diamond supply chain to track diamonds from mine to store.
 4. [Ripe](#) is working with [Sweetgreen](#) to use blockchain and IoT sensors to track crop growth, yielding higher-quality produce and providing better information for farmers, food distributors, restaurants, and consumers.
 2. Smart Contracting applications. For instance:
 1. In Indonesia, [Carbon Conservation](#) and Dappbase have created smart contracts that will distribute rewards to villages that can prove the successful reduction of incidences of forest fires.
 2. [Alice](#) has built Ethereum-based smart contracts for a donation project that supports 15 homeless people in London. The smart contracts ensure donations are released only when pre-determined project goals are met.

3. **Bext360** utilizes smart contracts to pay coffee farmers fairly and immediately based on a price determined through weighing and analyzing beans by the Bext360 machine at the source.
3. Identity applications. For instance:
 1. The State of Illinois is working with **Evernym** to digitize birth certificates, thus giving individuals a digital identity from birth.
 2. **BanQu** creates an economic passport for previously unbanked populations by using blockchain to record economic and financial transactions, purchase goods, and prove their existence in global supply chains.
 3. In 2015, **AID:Tech** piloted a project working with Syrian refugees in Lebanon to distribute over 500 donor aid cards that were tied to non-forgable identities.
 4. **uPort** provides digital identities for residents of Zug, Switzerland to use for governmental services.



1. *The promise of trusted Identity*: the potential to establish a trusted identity turns out to be foundational for using blockchain technologies for social change. At the same time identity emerges from a process (involving, for instance, provisioning, authentication, administration, authorization and auditing) and it is key to assess at what stage of the ID lifecycle DLTs provide an advantage vis-a-

vis other ID technologies; and how the maturity of the blockchain technology toward addressing the ID challenge.



1. Finally, we seek to translate current findings into

- Operational conditions that can enable the public and civic sector at-large to determine when “to blockchain” including:
 - The need for a clear problem definition (as opposed to certain situations where DLT solutions are in search of a problem);
 - The presence of information asymmetries and high transaction costs incentivize change. (“The Market of Lemons” problem);
 - The availability of (high quality) digital records;
 - The lack of availability of credible and alternative disclosure technologies;
 - Deficiency (or efficiency) of (trusted) intermediaries in the space.
- Design principles that can increase the likelihood of societal benefit when using Blockchain for identity projects (see picture) .



In the coming months, we will continue to share our findings from the Blockchange project in a number of forms – including a series of case studies, additional presentations and infographics, and an operational field guide for designing and implementing Blockchain projects to address challenges across the identity lifecycle.

The GovLab, in collaboration with the , is also delighted to announce a new initiative aimed at taking stock of the promise, practice and challenge of the use of Blockchain in the extractives sector. The project is focused in particular on DLTs as they relate to beneficial ownership, licensing and contracting transparency, and commodity trading transparency. This fall, we will share a collection of Blockchain for extractives case studies, as well as a report summarizing if, when, and how Blockchain can provide value across the extractives decision chain.

Name of Core

IRON PILL

Political Breakdown

ANARCHO-SOCIALIST, MARXIST, CRYPTO-SCEPTICS

Common Beliefs

DE-ACCELERATION AS CODE, TO GO FASTER YOU MUST
SLOW DOWN, TECHNOLOGY HELPS (IF IT'S GOOD)

Social Constructs

CRITICAL THINKING, ANTI-CAPITALISM, AUTONOMOUS
LIVING, CARER, NEO-LUDDITE, EXTROPIANISM

Coders

NICK SZABO, RICK FALKVINGE, CIXIN LIU, NICK SRNICEK

Coin

BITCOIN, MONERO, ETHEREUM, FAIR COIN

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

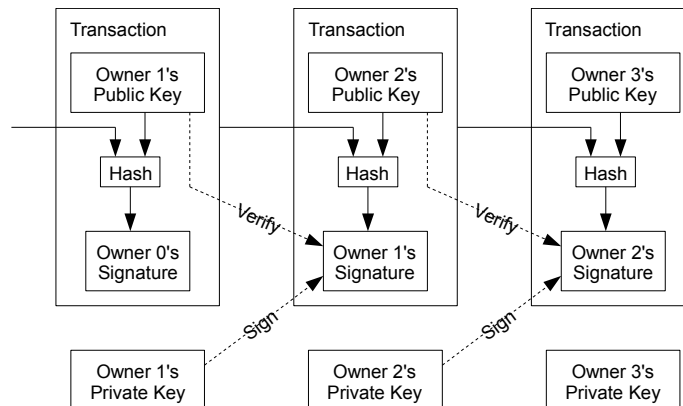
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

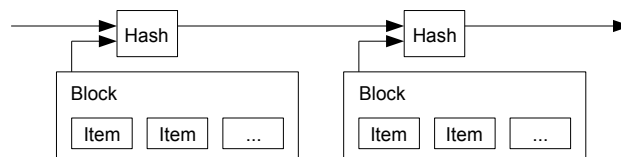


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

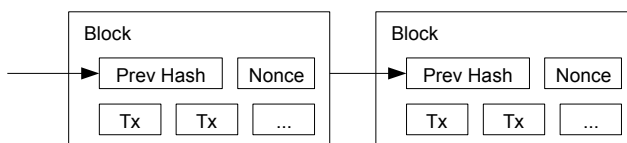
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 5) Nodes accept the block only if all transactions in it are valid and not already spent.
- 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

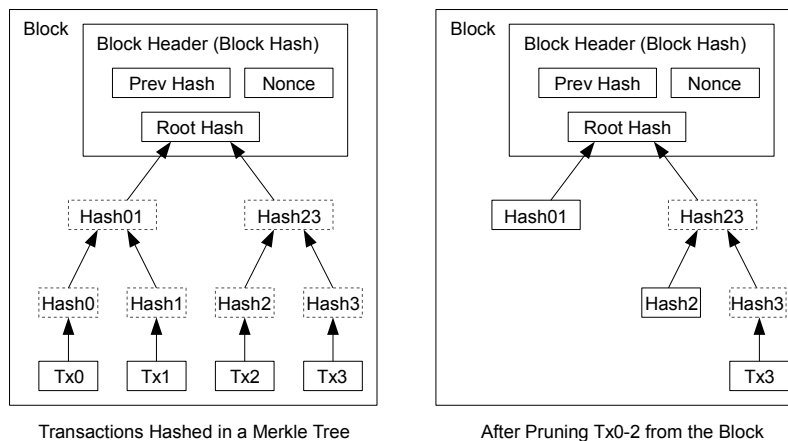
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

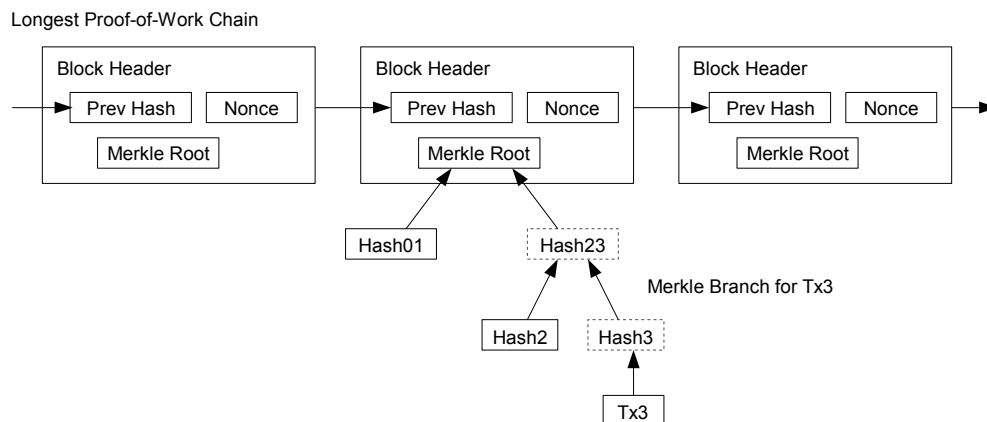
Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, $80 \text{ bytes} * 6 * 24 * 365 = 4.2\text{MB}$ per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

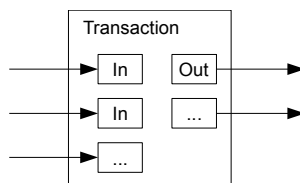
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

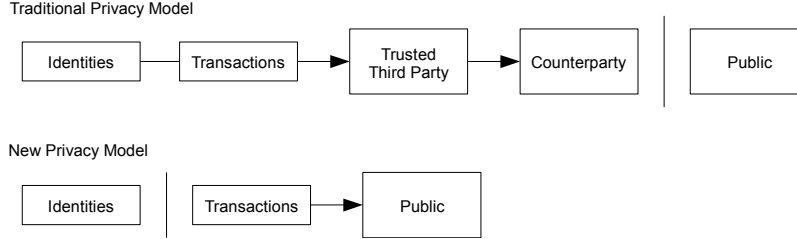
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
 q = probability the attacker finds the next block
 q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012
```

```
q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10  z=5
q=0.15  z=8
q=0.20  z=11
q=0.25  z=15
q=0.30  z=24
q=0.35  z=41
q=0.40  z=89
q=0.45  z=340
```


12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

- [1] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
- [2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.
- [3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.
- [4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.
- [5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.
- [6] A. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
- [7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.
- [8] W. Feller, "An introduction to probability theory and its applications," 1957.

THE CRYPTO-CURRENCY BITCOIN AND ITS MYSTERIOUS INVENTOR

 newyorker.com/magazine/2011/10/10/the-crypto-currency

BY JOSHUA DAVIS



It's not clear if bitcoin is legal, but there is no company in control and no one to arrest.

ILLUSTRATION BY GRAFILU

There are lots of ways to make money: You can earn it, find it, counterfeit it, steal it. Or, if you're Satoshi Nakamoto, a preternaturally talented computer coder, you can invent it. That's what he did on the evening of January 3, 2009, when he pressed a button on his keyboard and created a new currency called bitcoin. It was all bit and no coin. There was

no paper, copper, or silver—just thirty-one thousand lines of code and an announcement on the Internet.

Nakamoto, who claimed to be a thirty-six-year-old Japanese man, said he had spent more than a year writing the software, driven in part by anger over the recent financial crisis. He wanted to create a currency that was impervious to unpredictable monetary policies as well as to the predations of bankers and politicians. Nakamoto's invention was controlled entirely by software, which would release a total of twenty-one million bitcoins, almost all of them over the next twenty years. Every ten minutes or so, coins would be distributed through a process that resembled a lottery. Miners—people seeking the coins—would play the lottery again and again; the fastest computer would win the most money.

Interest in Nakamoto's invention built steadily. More and more people dedicated their computers to the lottery, and forty-four exchanges popped up, allowing anyone with bitcoins to trade them for official currencies like dollars or euros. Creative computer engineers could mine for bitcoins; anyone could buy them. At first, a single bitcoin was valued at less than a penny. But merchants gradually began to accept bitcoins, and at the end of 2010 their value began to appreciate rapidly. By June of 2011, a bitcoin was worth more than twenty-nine dollars. Market gyrations followed, and by September the exchange rate had fallen to five dollars. Still, with more than seven million bitcoins in circulation, Nakamoto had created thirty-five million dollars of value.

And yet Nakamoto himself was a cipher. Before the début of bitcoin, there was no record of any coder with that name. He used an e-mail address and a Web site that were untraceable. In 2009 and 2010, he wrote hundreds of posts in flawless English, and though he invited other software developers to help him improve the code, and corresponded

with them, he never revealed a personal detail. Then, in April, 2011, he sent a note to a developer saying that he had “moved on to other things.” He has not been heard from since.

When Nakamoto disappeared, hundreds of people posted theories about his identity and whereabouts. Some wanted to know if he could be trusted. Might he have created the currency in order to hoard coins and cash out? “We can effectively think of ‘Satoshi Nakamoto’ as being on top of a Ponzi scheme,” George Ou, a blogger and technology commentator, wrote.

It appeared, though, that Nakamoto was motivated by politics, not crime. He had introduced the currency just a few months after the collapse of the global banking sector, and published a five-hundred-word essay about traditional fiat, or government-backed, currencies. “The root problem with conventional currency is all the trust that’s required to make it work,” he wrote. “The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.”

Banks, however, do much more than lend money to overzealous homebuyers. They also, for example, monitor payments so that no one can spend the same dollar twice. Cash is immune to this problem: you can’t give two people the same bill. But with digital currency there is the danger that someone can spend the same money any number of times.

Nakamoto solved this problem using innovative cryptography. The bitcoin software encrypts each transaction—the sender and the receiver are identified only by a string of numbers—but a public record of every coin’s movement is published across the entire network. Buyers and sellers remain anonymous, but everyone can see that a coin has

moved from A to B, and Nakamoto's code can prevent A from spending the coin a second time.

Nakamoto's software would allow people to send money directly to each other, without an intermediary, and no outside party could create more bitcoins. Central banks and governments played no role. If Nakamoto ran the world, he would have just fired Ben Bernanke, closed the European Central Bank, and shut down Western Union. "Everything is based on crypto proof instead of trust," Nakamoto wrote in his 2009 essay.

Bitcoin, however, was doomed if the code was unreliable. Earlier this year, Dan Kaminsky, a leading Internet-security researcher, investigated the currency and was sure he would find major weaknesses. Kaminsky is famous among hackers for discovering, in 2008, a fundamental flaw in the Internet which would have allowed a skilled coder to take over any Web site or even to shut down the Internet. Kaminsky alerted the Department of Homeland Security and executives at Microsoft and Cisco to the problem and worked with them to patch it. He is one of the most adept practitioners of "penetration testing," the art of compromising the security of computer systems at the behest of owners who want to know their vulnerabilities. Bitcoin, he felt, was an easy target.

"When I first looked at the code, I was sure I was going to be able to break it," Kaminsky said, noting that the programming style was dense and inscrutable. "The way the whole thing was formatted was insane. Only the most paranoid, painstaking coder in the world could avoid making mistakes."

Kaminsky lives in Seattle, but, while visiting family in San Francisco in July, he retreated to the basement of his mother's house to work on his bitcoin attacks. In a windowless room jammed with computers, Kaminsky paced around talking to himself, trying to build a mental picture of

the bitcoin network. He quickly identified nine ways to compromise the system and scoured Nakamoto's code for an insertion point for his first attack. But when he found the right spot, there was a message waiting for him. "Attack Removed," it said. The same thing happened over and over, infuriating Kaminsky. "I came up with beautiful bugs," he said. "But every time I went after the code there was a line that addressed the problem."

He was like a burglar who was certain that he could break into a bank by digging a tunnel, drilling through a wall, or climbing down a vent, and on each attempt he discovered a freshly poured cement barrier with a sign telling him to go home. "I've never seen anything like it," Kaminsky said, still in awe.

Kaminsky ticked off the skills Nakamoto would need to pull it off. "He's a world-class programmer, with a deep understanding of the C++ programming language," he said. "He understands economics, cryptography, and peer-to-peer networking."

"Either there's a team of people who worked on this," Kaminsky said, "or this guy is a genius."

Kaminsky wasn't alone in this assessment. Soon after creating the currency, Nakamoto posted a nine-page technical paper describing how bitcoin would function. That document included three references to the work of Stuart Haber, a researcher at H.P. Labs, in Princeton. Haber is a director of the International Association for Cryptologic Research and knew all about bitcoin. "Whoever did this had a deep understanding of cryptography," Haber said when I called. "They've read the academic papers, they have a keen intelligence, and they're combining the concepts in a genuinely new way."

Haber noted that the community of cryptographers is very small: about three hundred people a year attend the most important conference, the annual gathering in Santa

Barbara. In all likelihood, Nakamoto belonged to this insular world. If I wanted to find him, the Crypto 2011 conference would be the place to start.

“Here we go, team!” a cheerleader shouted before two burly guys heaved her into the air.

It was a foggy Monday morning in mid-August, and dozens of college cheerleaders had gathered on the athletic fields of the University of California at Santa Barbara for a three-day training camp. Their hollering could be heard on the steps of a nearby lecture hall, where a group of bleary-eyed cryptographers, dressed in shorts and rumpled T-shirts, muttered about symmetric-key ciphers over steaming cups of coffee.

This was Crypto 2011, and the list of attendees included representatives from the National Security Agency, the U.S. military, and an assortment of foreign governments.

Cryptographers are little known outside this hermetic community, but our digital safety depends on them. They write the algorithms that conceal bank files, military plans, and your e-mail.

I approached Phillip Rogaway, the conference’s program chair. He is a friendly, diminutive man who is a professor of cryptography at the University of California at Davis and who has also taught at Chiang Mai University, in Thailand. He bowed when he shook my hand, and I explained that I was trying to learn more about what it would take to create bitcoin. “The people who know how to do that are here,” Rogaway said. “It’s likely I either know the person or know their work.” He offered to introduce me to some of the attendees.

Nakamoto had good reason to hide: people who experiment with currency tend to end up in trouble. In 1998, a Hawaiian resident named Bernard von NotHaus began fabricating silver and gold coins that he dubbed Liberty Dollars. Nine years later, the U.S. government charged NotHaus with

“conspiracy against the United States.” He was found guilty and is awaiting sentencing. “It is a violation of federal law for individuals . . . to create private coin or currency systems to compete with the official coinage and currency of the United States,” the F.B.I. announced at the end of the trial.

Online currencies aren’t exempt. In 2007, the federal government filed charges against e-Gold, a company that sold a digital currency redeemable for gold. The government argued that the project enabled money laundering and child pornography, since users did not have to provide thorough identification. The company’s owners were found guilty of operating an unlicensed money-transmitting business and the C.E.O. was sentenced to months of house arrest. The company was effectively shut down.

Nakamoto seemed to be doing the same things as these other currency developers who ran afoul of authorities. He was competing with the dollar and he insured the anonymity of users, which made bitcoin attractive for criminals. This winter, a Web site was launched called Silk Road, which allowed users to buy and sell heroin, LSD, and marijuana as long as they paid in bitcoin.

Still, Lewis Solomon, a professor emeritus at George Washington University Law School, who has written about alternative currencies, argues that creating bitcoin might be legal. “Bitcoin is in a gray area, in part because we don’t know whether it should be treated as a currency, a commodity like gold, or possibly even a security,” he says.

Gray areas, however, are dangerous, which may be why Nakamoto constructed bitcoin in secret. It may also explain why he built the code with the same peer-to-peer technology that facilitates the exchange of pirated movies and music: users connect with each other instead of with a central server. There is no company in control, no office to raid, and nobody to arrest.

Today, bitcoins can be used online to purchase beef jerky and socks made from alpaca wool. Some computer retailers accept them, and you can use them to buy falafel from a restaurant in Hell's Kitchen. In late August, I learned that bitcoins could also get me a room at a Howard Johnson hotel in Fullerton, California, ten minutes from Disneyland. I booked a reservation for my four-year-old daughter and me and received an e-mail from the hotel requesting a payment of 10.305 bitcoins.

By this time, it would have been pointless for me to play the bitcoin lottery, which is set up so that the difficulty of winning increases the more people play it. When bitcoin launched, my laptop would have had a reasonable chance of winning from time to time. Now, however, the computing power dedicated to playing the bitcoin lottery exceeds that of the world's most powerful supercomputer. So I set up an account with Mt. Gox, the leading bitcoin exchange, and transferred a hundred and twenty dollars. A few days later, I bought 10.305 bitcoins with the press of a button and just as easily sent them to the Howard Johnson.

It was a simple transaction that masked a complex calculus. In 1971, Richard Nixon announced that U.S. dollars could no longer be redeemed for gold. Ever since, the value of the dollar has been based on our faith in it. We trust that dollars will be valuable tomorrow, so we accept payment in dollars today. Bitcoin is similar: you have to trust that the system won't get hacked, and that Nakamoto won't suddenly emerge to somehow plunder it all. Once you believe in it, the actual cost of a bitcoin—five dollars or thirty?—depends on factors such as how many merchants are using it, how many might use it in the future, and whether or not governments ban it.

My daughter and I arrived at the Howard Johnson on a hot Friday afternoon and were met in the lobby by Jefferson Kim, the hotel's cherubic twenty-eight-year-old general

manager. “You’re the first person who’s ever paid in bitcoin,” he said, shaking my hand enthusiastically.

Kim explained that he had started mining bitcoins two months earlier. He liked that the currency was governed by a set of logical rules, rather than the mysterious machinations of the Federal Reserve. A dollar today, he pointed out, buys you what a nickel bought a century ago, largely because so much money has been printed. And, he asked, why trust a currency backed by a government that is fourteen trillion dollars in debt?

Kim had also figured that bitcoin mining would be a way to make up the twelve hundred dollars he’d spent on a high-performance gaming computer. So far, he’d made only four hundred dollars, but it was fun to be a pioneer. He wanted bitcoin to succeed, and in order for that to happen businesses needed to start accepting it.



“We never talk anymore.”

The truth is that most people don’t spend the bitcoins they buy; they hoard them, hoping that they will appreciate. Businesses are afraid to accept them, because they’re new and weird—and because the value can fluctuate wildly. (Kim

immediately exchanged the bitcoins I sent him for dollars to avoid just that risk.) Still, the currency is young and has several attributes that appeal to merchants. Robert Schwarz, the owner of a computer-repair business in Klamath Falls, Oregon, began selling computers for bitcoin to sidestep steep credit-card fees, which he estimates cost him three per cent on every transaction. “One bank called me saying they had the lowest fees,” Schwarz said. “I said, ‘No, you don’t. Bitcoin does.’ ” Because bitcoin transfers can’t be reversed, merchants also don’t have to deal with credit-card charge-backs from dissatisfied customers. Like cash, it’s gone once you part with it.

At the Howard Johnson, Kim led us to the check-in counter. The lobby featured imitation-crystal chandeliers, ornately framed oil paintings of Venice, and, inexplicably, a pair of faux elephant tusks painted gold. Kim explained that he hadn’t told his mother, who owned the place, that her hotel was accepting bitcoins: “It would be too hard to explain what a bitcoin is.” He said he had activated the tracking program on his mother’s Droid, and she was currently about six miles away. Today, at least, there was no danger of her finding out about her hotel’s financial innovation. The receptionist handed me a room card, and Kim shook my hand. “So just enjoy your stay,” he said.

Nakamoto’s extensive online postings have some distinctive characteristics. First of all, there is the flawless English. Over the course of two years, he dashed off about eighty thousand words—the approximate length of a novel—and made only a few typos. He covered topics ranging from the theories of the Austrian economist Ludwig von Mises to the history of commodity markets. Perhaps most interestingly, when he created the first fifty bitcoins, now known as the “genesis block,” he permanently embedded a brief line of text into the data: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”

This is a reference to a *Times* of London article that indicated that the British government had failed to stimulate the economy. Nakamoto appeared to be saying that it was time to try something new. The text, hidden amid a jumble of code, was a sort of digital battle cry. It also indicated that Nakamoto read a British newspaper. He used British spelling (“favour,” “colour,” “grey,” “modernised”) and at one point described something as being “bloody hard.” An apartment was a “flat,” math was “maths,” and his comments tended to appear after normal business hours ended in the United Kingdom. In an initial post announcing bitcoin, he employed American-style spelling. But after that a British style appeared to flow naturally.

I had this in mind when I started to attend the lectures at the Crypto 2011 conference, including ones with titles such as “Leftover Hash Lemma, Revisited” and “Time-Lock Puzzles in the Random Oracle Model.” In the back of a darkened auditorium, I stared at the attendee list. A Frenchman onstage was talking about testing the security of encryption systems. The most effective method, he said, is to attack the system and see if it fails. I ran my finger past dozens of names and addresses, circling residents of the United Kingdom and Ireland. There were nine.

I soon discovered that six were from the University of Bristol, and they were all together at one of the conference’s cocktail parties. They were happy to chat but entirely dismissive of bitcoin, and none had worked with peer-to-peer technology. “It’s not at all interesting to us,” one of them said. The two other cryptographers from Britain had no history with large software projects. Then I started looking into a man named Michael Clear.

Clear was a young graduate student in cryptography at Trinity College in Dublin. Many of the other research students at Trinity posted profile pictures and phone numbers, but Clear’s page just had an e-mail address. A

Web search turned up three interesting details. In 2008, Clear was named the top computer-science undergraduate at Trinity. The next year, he was hired by Allied Irish Banks to improve its currency-trading software, and he co-authored an academic paper on peer-to-peer technology. The paper employed British spelling. Clear was well versed in economics, cryptography, and peer-to-peer networks.

I e-mailed him, and we agreed to meet the next morning on the steps outside the lecture hall. Shortly after the appointed time, a long-haired, square-jawed young man in a beige sweater walked up to me, looking like an early-Zeppelin Robert Plant. With a pronounced brogue, he introduced himself. “I like to keep a low profile,” he said. “I’m curious to know how you found me.”

I told him I had read about his work for Allied Irish, as well as his paper on peer-to-peer technology, and was interested because I was researching bitcoin. I said that his work gave him a unique insight into the subject. He was wearing rectangular Armani glasses and squinted so much I couldn’t see his eyes.

“My area of focus right now is fully homomorphic encryption,” he said. “I haven’t been following bitcoin lately.”

He responded calmly to my questions. He was twenty-three years old and studied theoretical cryptography by himself in Dublin—there weren’t any other cryptographers at Trinity. But he had been programming computers since he was ten and he could code in a variety of languages, including C++, the language of bitcoin. Given that he was working in the banking industry during tumultuous times, I asked how he felt about the ongoing economic crisis. “It could have been averted,” he said flatly.

He didn’t want to say whether or not the new currency could prevent future banking crises. “It needs to prove itself,” he said. “But it’s an intriguing idea.”

I told him I had been looking for Nakamoto and thought that he might be here at the Crypto 2011 conference. He said nothing. Finally, I asked, “Are you Satoshi?”

He laughed, but didn’t respond. There was an awkward silence.

“If you’d like, I’d be happy to review the design for you,” he offered instead. “I could let you know what I think.”

“Sure,” I said hesitantly. “Do you need me to send you a link to the code?”

“I think I can find it,” he said.

Soon after I met Clear, I travelled to Glasgow, Kentucky, to see what bitcoin mining looked like. As I drove into the town of fourteen thousand, I passed shuttered factories and a central square lined with empty storefronts. On Howdy 106.5, a local radio station, a man tried to sell his bed, his television, and his basset hound—all for a hundred and ten dollars.

I had come to visit Kevin Groce, a forty-two-year-old bitcoin miner. His uncles had a garbage-hauling business and had let him set up his operation at their facility. The dirt parking lot was jammed with garbage trucks, which reeked in the summer sun.

“I like to call it the new moonshining,” Groce said, in a smooth Kentucky drawl, as he led me into a darkened room. One wall was lined with four-foot-tall homemade computers with blinking green and red lights. The processors inside were working so hard that their temperature had risen to a hundred and seventy degrees, and heat radiated into the room. Each system was a jumble of wires and hacked-together parts, with a fan from Walmart duct-taped to the top. Groce had built them three months earlier, for four thousand dollars. Ever since, they had generated a steady flow of bitcoins, which Groce exchanged for dollars,

averaging about a thousand per month so far. He figured his investment was going to pay off.

Groce was wiry, with wisps of gray in his hair, and he split his time between working on his dad's farm, repairing laptops at a local computer store, and mining bitcoin.

Groce's father didn't understand Kevin's enthusiasm for the new currency and expected him to take over the farm. "If it's not attached to a cow, my dad doesn't think much of it," Groce said.

Groce was engaged to be married, and planned to use some of his bitcoin earnings to pay for a wedding in Las Vegas later in the year. He had tried to explain to his fiancée how they could afford it, but she doubted the financial prudence of filling a room with bitcoin-mining rigs. "She gets to cussing every time we talk about it," Groce confided. Still, he was proud of the powerful computing center he had constructed. The machines ran non-stop, and he could control them remotely from his iPhone. The arrangement allowed him to cut tobacco with his father and monitor his bitcoin operation at the same time.

Nakamoto knew that competition for bitcoins would eventually lead people to build these kinds of powerful computing clusters. Rather than let that effort go to waste, he designed software that uses the processing power of the lottery players to confirm and verify transactions. As people like Groce try to win bitcoins, their computers are harnessed to analyze transactions and insure that no one spends money twice. In other words, Groce's backwoods operation functioned as a kind of bank.

Groce, however, didn't look like a guy Wells Fargo would hire. He liked to stay up late at the garbage-hauling center and thrash through Black Sabbath tunes on his guitar. He gave all his computers pet names, like Topper and the Dazzler, and, between guitar solos, tended to them as if they

were prize animals. “I grew up milking cows,” Groce said. “Now I’m just milking these things.”

A week after the Crypto 2011 conference, I received an e-mail from Clear. He said that he would send me his thoughts on bitcoin in a day. He added, “I also think I can identify Satoshi.”

The next morning, Clear sent a lengthy e-mail. “It is apparent that the person(s) behind the Satoshi name accumulated a not insignificant knowledge of applied cryptography,” he wrote, adding that the design was “elegant” and required “considerable effort and dedication, and programming proficiency.” But Clear also described some of bitcoin’s weaknesses. He pointed out that users were expected to download their own encryption software to secure their virtual wallets. Clear felt that the bitcoin software should automatically provide such security. He also worried about the system’s ability to grow and the fact that early adopters received an outsized share of bitcoins.

“As far as the identity of the author, it would be unfair to publish an identity when the person or persons has/have taken major steps to remain anonymous,” he wrote. “But you may wish to talk to a certain individual who matches the profile of the author on many levels.”

He then gave me a name.

For a few seconds, all I could hear on the other end of the line was laughter.

“I would love to say that I’m Satoshi, because bitcoin is very clever,” Vili Lehdonvirta said, finally. “But it’s not me.”

Lehdonvirta is a thirty-one-year-old Finnish researcher at the Helsinki Institute for Information Technology. Clear had discovered that Lehdonvirta used to be a video-game programmer and now studies virtual currencies. Clear suggested that he was a solid fit for Nakamoto.

Lehdonvirta, however, pointed out that he has no background in cryptography and limited C++ programming skills. “You need to be a crypto expert to build something as sophisticated as bitcoin,” Lehdonvirta said. “There aren’t many of those people, and I’m definitely not one of them.”

Still, Lehdonvirta had researched bitcoin and worried about it. “The only people who need cash in large denominations right now are criminals,” he said, pointing out that cash is hard to move around and store. Bitcoin removes those obstacles while preserving the anonymity of cash.

Lehdonvirta is on the advisory board of Electronic Frontier Finland, an organization that advocates for online privacy, among other things. Nonetheless, he believes that bitcoin takes privacy too far. “Only anarchists want absolute, unbreakable financial privacy,” he said. “We need to have a back door so that law enforcement can intercede.”

But Lehdonvirta admitted that it’s hard to stop new technology, particularly when it has a compelling story. And part of what attracts people to bitcoin, he said, is the mystery of Nakamoto’s true identity. “Having a mythical background is an excellent marketing trick,” Lehdonvirta said.

A few days later, I spoke with Clear again. “Did you find Satoshi?” he asked cheerfully.

I told him that Lehdonvirta had made a convincing denial, and that every other lead I’d been working on had gone nowhere. I then took one more opportunity to question him and to explain all the reasons that I suspected his involvement. Clear responded that his work for Allied Irish Banks was brief and of “no importance.” He admitted that he was a good programmer, understood cryptography, and appreciated the bitcoin design. But, he said, economics had never been a particular interest of his. “I’m not Satoshi,” Clear said. “But even if I was I wouldn’t tell you.”

The point, Clear continued, is that Nakamoto’s identity shouldn’t matter. The system was built so that we don’t have

to trust an individual, a company, or a government. Anybody can review the code, and the network isn't controlled by any one entity. That's what inspires confidence in the system. Bitcoin, in other words, survives because of what you can see and what you can't. Users are hidden, but transactions are exposed. The code is visible to all, but its origins are mysterious. The currency is both real and elusive—just like its founder.

"You can't kill it," Clear said, with a touch of bravado. "Bitcoin would survive a nuclear attack."

Over the summer, bitcoin actually experienced a sort of nuclear attack. Hackers targeted the burgeoning currency, and though they couldn't break Nakamoto's code, they were able to disrupt the exchanges and destroy Web sites that helped users store bitcoins. The number of transactions decreased and the exchange rate plummeted.

Commentators predicted the end of bitcoin. In September, however, volume began to increase again, and the price stabilized, at least temporarily.

Meanwhile, in Kentucky, Kevin Groce added two new systems to his bitcoin-mining operation at the garbage depot and planned to build a dozen more. Ricky Wells, his uncle and a co-owner of the garbage business, had offered to invest thirty thousand dollars, even though he didn't understand how bitcoin worked. "I'm just a risk-taking son of a bitch and I know this thing's making money," Wells said. "Plus, these things are so damn hot they'll heat the whole building this winter."

To Groce, bitcoin was an inevitable evolution in money. People use printed money less and less as it is, he said. Consumers need something like bitcoin to take its place. "It's like eight-tracks going to cassettes to CDs and now MP3s," he said.

Even though his friends and most of his relatives questioned his enthusiasm, Groce didn't hide his confidence. He liked to

wear a T-shirt he designed that had the words “Bitcoin Millionaire” emblazoned in gold on the chest. He admitted that people made fun of him for it. “My fiancée keeps saying she’d rather I was just a regular old millionaire,” he said. “But maybe I will be someday, if these rigs keep working for me.”



BEYOND ENDLESS WINTER: AN INTERVIEW WITH NICK SRNICEK

tripleampersand.org/beyond-endless-winter-interview-nick-srnicek/

February 20, 2018



FEBRUARY 20, 2018

The following interview was conducted in October 2017 and was originally intended to serve as printed material to accompany the [Grammar of Postcontemporary](#) autumn school near Moscow, Russia, that Nick Srnicek participated in. Beyond a simple introduction to accelerationist theory and its consequences, the talk evolved into a full-fledged discussion that touched upon much deeper and broader topics, enabling it to become a distinct publication. The Russian translation of the interview is published in [Logos Journal](#) (Vol. 28 #2, 2018) while the English version appears here for the first time on The New Centre's &&&.

Artem Gureev: So let's begin with what is Accelerationism?

Nick Srnicek: When Alex Williams and I wrote the #Accelerate Manifesto it wasn't really a term that was well known. It had been coined by Benjamin Noys as a critical term when he set a philosophy of negation against the accelerationist affirmation that he found in thinkers like Gilles Deleuze and Felix Guattari. But when Alex and I took up the term it was meant to be a very Marxist project – it was building upon the basic Marxist belief that capitalism was not something that you would try to destroy and reverse away from. Instead, capitalism was building the basis for post-capitalism, for the movement beyond itself. And this is what accelerationism meant for Alex and I: this simple idea. In more concrete terms, this meant taking an interest in the latest technology, thinking about how exactly they can be used as technologies for liberation rather than tools of control, and thinking about the ways in which we can build a world of abundance and experimentation beyond the strictures of capitalist society. So we ended up with a lot of focus on technology, thinking about “What does it really mean to be human?”, trying to get beyond the essentialist idea of the human and integrating this with recent ideas around artificial intelligence, on the nature of reasoning, and collective rationality. Effectively, what we were trying to grasp at was a post-human and post-capitalist vision of the future.

AG: You just mentioned Marxism. One of its central tenets being dialectical materialism, how does dialectics as a method, as a paradigm of thought impact Accelerationism? Does the concept of non-foundationalist, evolutionary reasoning play a large role in the movement? A lot of attention has been paid to Brandom in recent years.

NS: Well, my initial take on dialectics was filtered through my Deleuzian training: dialectics was this blunt instrument to try and understand the nature of development, and that

actually we needed a much more subtle and materialist view of non-dialectical becoming. I think this played a large part in the original work on accelerationism when Alex and I were working on it; we both came from that sort of background and it implicitly informed much of the image of change that we have in mind there. But since then, I've come around more to dialectics in part due to Ray Brassier and Reza Negarestani's work, but also becoming a bit more intrigued by the potential of value-form Marxism. With Ray and Reza, I take it that one of their projects is to rethink dialectics using Brandom and Wilfrid Sellars, who have given us much more sophisticated tools to understand the dynamics and intricacies of reasoning processes and the ways in which conceptual apparatus latch onto the real. Philosophically, I think this marks Ray and Reza's work as some of the most interesting and inventive stuff going on right now.

AG: Maybe something like "creative" dialectics that conceptually allows for emergence rather than determinism?

NS: Yes, I can see something like that taking place – and it aligns nicely with Deleuzian conceptions as well.

AG: Currently there seems to be two currents of Accelerationism: right and left-wing. Is there any ontological principle that can be used to distinguish them, relating to technology perhaps?

NS: To be honest, I'm not sure the idea of a right and left accelerationism makes sense, given that it presupposes some common basis between the two, with a politico-philosophical decision choosing between the two. It's why I think the term 'accelerationism' has become useless; liable to mean anything to anyone. I've yet to see any interesting questions, provocations, or insights emerge from the idea that there's a common accelerationist project that subdivides

into a right and left genre. But when people talk about right accelerationism, they mean Nick Land (I'm not sure there are any other 'right accelerationists'?) And in terms of his 90s work (I must admit to having read very little of his recent stuff), I think Ray gave the definitive critique of it some time ago – which is that it may be an aesthetically and intellectually invigorating project, but it's one that cashes out in practical and logical contradictions by effacing the question of representation. It's this sort of analysis which has led Ray from tarrying with eliminative materialism to tarrying with normative reasoning, and which has led a lot of us to rethinking the role of reasoning. Once you recognize the internal contradictions of the eliminative materialist project, you're forced towards some difficult questions that get otherwise brushed aside. More broadly, I think Land's 90s project was of a piece with the historical triumph of capitalism over the USSR, and it was an attempt to ontologize that victory. But that idea, like much of the 90s, seems dated by today's standards. Far from being an engine of dynamism, capitalism today is defined by stagnation and decrepitude.

AG: To expand on that: Accelerationism criticises capitalism for not being productive enough, not being an absolute deterritorializing agent, yet is it concerned only with something material, like technologies, or also with abstract entities such as social spaces?

NS: I don't think technology can be separated from the social structure around it and partly this is, once again, a classic Marxist thesis that the relations of production end up constraining the forces of production. And that seems like an apt description of what is happening today. Capitalism has reached this point where it's unable to develop the forces of production in any significant sense. Here's the challenge for any proponent of capitalism's endless dynamic force: why

has global capitalism being slowing down on every major indicator since the 1970s? GDP, labor productivity, patent creation, total factor productivity, wages, profits, and so on – all slowing down. The neoliberal era has been terrible for capitalism even on its own terms.

AG: So are there any possible/visible “Events,” in the Badiouian sense, happening to technology and its advancement in the near future even with such stagnation?

NS: I’m hesitant to use language of “events,” in part because it tends towards an approach to politics that is quite Messianic in nature. It also risks courting the ineffable as something valuable in itself – a stance which I think has a rather terrible political and philosophical history. But if we move away from the language of events, I do think there are significant changes going on with things like machine learning and particularly some efforts to create a more general form of artificial intelligence. The issue here is not so much that we might create an AI that takes over the world and Terminator-style decide to wipe out humanity (complete with the anthropocentric belief that a superhuman AI would care enough to eliminate us).

I think the more real threat is the monopolistic use of artificial intelligence and the ways in which it generates political and economic power. What we’re seeing happen right now is the consolidation of AI’s power for control being consolidated into the hands of a few companies with the resources, expertise, and data to be able to build world-leading AI. This seems to be a much more realistic problem to be concerning ourselves with. In any case, present AI research is still heavily constrained, despite the apparent magic it can carry out at times. The AIs that we have now, for instance, are very good at the single tasks that we train them for, but tend to fall apart when we try to move them to a different task. We

also have a basic technique – back propagation – that has been around for decades, and is now being mined for all its worth, but with dwindling results. If you look at the industrial internet, for example, Siemens and GE are really struggling with being able to transfer success in one industry into success in another industry. The techniques of modern AI don't allow for that for that sort of transfer. Likewise with smartphones and apps – we seem to have basically exhausted their impact, so that each new annual replacement makes less and less difference to our world. I think a similar thing could happen soon with machine learning, and it's quite possible that we'll see another AI winter.

AG: Maybe we should return to the figure of Nick Land. You have once mentioned that he is "too '90s." This seems to be a theme, rather than an incident with the rise of "retrofuturistic" movements. How can one conceptually escape that?

NS: We can't escape the past. When we are trying to imagine a future and trying to imagine utopia we are constantly going to be using the tools, ideas, and concepts from the past – we have an arsenal of elements in front of us, and we try to reconstruct something novel from them. This is the basic empiricist retort to utopian thinking: one can't imagine what one hasn't experienced. What I think is missed here is that imagination is more a matter of recombining elements in unique ways, along the lines of a more combinatorial approach to imagining the future rather than thinking that we can imagine a future out of nothing. In that sense, I think retrofuturism is inevitable to some degree.

AG: In terms of such processes, what can we say about Science Fiction, especially in regards to rising scholarly interest in this literary genre?

NS: I will say that I think that the recent resurgence in Science Fiction is indicative of the broader interest in the future. And I don't think it's any surprise that this occurred post-2008. Prior to the financial crisis, there was very much the sense – on the left and the right – that neoliberal capitalism was at least a pretty stable system that would grow fast enough to be able to dampen down any major criticism or revolt that might arise. The big dot-com bust of the early 2000s, for instance, hadn't slowed the economy down in any significant way – it was as though neoliberalism really had overcome the boom-bust cycle. Whereas in 2008 that all breaks apart. And 10 years later, we still have a situation where no one knows how to restart the capitalist accumulation process. Neoliberal hegemony has truly been broken – first in a materialist way, and now increasingly in a social and political way. As a result, this re-opens the question of the future in a way that hasn't really been posed since at least the fall of the Soviet Union. That turn of the century moment when global capitalism appeared unimpeachable is now completely gone. I think that the broader academic interest – and I don't think it's just academic interest; there is more science fiction being written itself – is indicative of a broad historical moment that we find ourselves in.

AG: After derivative mentions of certain writers and movements, how would you place such emerging movements as Prometheanism or Inhumanism, which were included in the Accelerationist Reader, in relation to Accelerationism? Do they encompass each other?

NS: Perhaps better than movements might be to see them as conceptual decisions on various issues that then form the basis for further exploration. So, for instance, when Ray talks about Prometheanism he is referencing the basic political and philosophical belief that there are no immutable

givens – there is no transcendental which cannot be altered, and that claim then licenses a further series of conceptual and practical moves. A similar sort of disposition lies behind Alex and I's emphasis on post-work. The project of ending wage labor is underpinned by a strategic analysis that capitalism relies upon – and naturalizes – the condition of the wage laborer. Far from being a deterritorialising movement, capitalism is premised upon the reproduction of a highly constrained class structure that determines and limits what it means to be human. Under capitalism, we get a restrictive image of the human, and the project of moving beyond work is the first step in tearing down those constraints.

AG: It also seems like, at least ideologically, these projects share a lot with Enlightenment. Do they in a way try to revive its ideas?

NS: Yes, though in a very particular way. The basic notion of the Enlightenment as progress through reasoning certainly plays an indispensable role. One issue though is that the original notion relied upon a disinterested, disembodied – but implicitly white, male, property-owning – subject. And numerous critics, postcolonial and poststructuralist, have rightly critiqued that presupposition. That doesn't mean, however, that we need to give up on the idea of rationality or conceptual progress; it just means we need to complicate our images of these elements. And that's partly what I find interesting in the work of people like Reza – who try and reinvigorate some idea of the Enlightenment and progress of reason but to do so in a way which also takes into account the critiques that have been made of the Enlightenment. So, yes to reinvigorating the Enlightenment but in a way that is responsive to the legitimate critiques made of it.

AG: One of the concepts that stemmed out of post-Enlightenment criticism is alienation, arguably one of the

most important ones. How does it fit into Accelerationist and other contemporary theory? As I understand it, Xenofeminism even describes it as a driving force.

NS: For us, I'd say that alienation begins with the denial of any authentic self. In that sense, subjectivity just is alienation, and the process of determining what it means to be human is a process of continual alienation. Alienation isn't some aberrant state of existence then, but the basic process of constructing the human.

AG: The accelerationist manifesto posits the viability of both horizontal and vertical actions in political praxis. How does that show up in particular examples?

NS: At the time of the manifesto and when we wrote "Inventing the Future", we were very much writing in response to Occupy Wall Street. This was from our own experience and watching the movement spread around the world, where we saw the constant emphasis on the horizontal nature of Occupy. This led, predictably, to the rejection of any sort of verticality whatsoever (this was often the rhetoric of the movement, though in practice there were some exceptions). This also led to a number of problems, culminating in the collapse and ultimate failure of these movements to effectuate any significant change. So when we talk about the need to move beyond the limit of pure horizontalism, it's the experience and lessons of Occupy Wall Street that we have in mind.

Now, in terms of what represents an alternative, I would say we've seen a range of experiments with this since the fall of OWS. Something like Podemos is good example at an organisation level, as a vertical party combined with horizontal, common circles that are more localized forms of groups which can interact and feedback into that vertical system. There is an interesting interchange going on in the

way these two systems, in a paradigm which you cannot really describe as being a traditional hierarchy or a traditional horizontal movement. Another example would be Momentum here in the UK. You have the Labour party which is more or less hierarchical, yet which also incorporated more horizontal elements from its very beginnings. With Momentum you have something even more peculiar, a system which enables a spontaneity of people from the bottom up. This enables horizontal organizing to go on as well as feed into a vertical system in a way which has been very productive in terms of what has been achieved in the last general election. I think these are interesting examples that can be learned from (and let me emphasize them as experiments to learn from, rather than models to copy). You cannot categorize them in classical terms of horizontal or vertical. This idea was really what Alex and I were trying to get at: to say that the categories of horizontal/vertical are constraining our imaginations about what's possible, and that the constant emphasis on one pole or the other is leading us into dead-ends. I think the failure of Occupy and similar movements has, fortunately, spurred on a lot of people to start thinking beyond these categories.

AG: Does it have to do something with cybernetic theory?

NS: Maybe... I'm a bit sceptical of throwing the term "cybernetics" into everything. More often than not it gets used as a trendy term to label something that can be described in a much simpler, more profound way.

AG: In terms of communications then: Ray Brassier has once stated that the internet is not an "appropriate medium for a serious philosophical debate." Does that, in your opinion, maybe, describe the state of the entire communication system of the internet in general?

NS: I think that effectively the internet is a great medium for

discussion under the right conditions (a claim that holds for every communications medium). One of the major differences between discussion on the internet and discussion elsewhere is that there is often an imagined audience online. What happens is that you end up writing not to learn something, nor to necessarily engage with an idea, nor to question something or even question yourself, but instead to perform for this audience. This is extremely detrimental to any type of proper discussion – it leads to a game of trying to appease this imagined audience, with likes and RTs being the most salient metric of success. For that reason, I don't think Facebook, let alone Twitter, lend themselves to meaningful discussion. That doesn't mean these media aren't useful for other reasons, since politics isn't only about reasonable discussion (for example, what often gets derided as Twitter pile-ons seems to me more often a matter of the weak using their traditional weapon of shame against the strong). But these limits do help explain the (often humorous) frustration that earnest people get when trying to have a reasonable conversation online, and any effective political use of these media needs to recognize them.

Blogging, on the other hand, at least had a moment of utility for developing ideas collectively. At its origins, it was a pretty small community of people who looked at the process of discussion not as a matter of one-up-manship or proof of omniscience. It was a space where you could make mistakes quite openly as well as test ideas and do so in a way that recognized epistemic humility. Those aspects have mostly disappeared from the public eye today, but in my experience it's because they've been recreated in more private ways. So instead of a public blog for anyone to comment on, people use WhatsApp, or Slack, or even G+ to build smaller and more private communities to develop ideas.

AG: Would you then say that the public internet should be re-appropriated? Its former state seems to be much less commercialized and power-driven. Is there such a possibility?

NS: I think so, yes. We can imagine different forms of public ownership that involve taking control of these platforms away from capitalist firms. The demands of capitalism are often at odds with the requirements of a functional public sphere. Twitter is a good example. It could be a fairly interesting space to meaningfully engage with others, but instead the company is concentrated on trying to generate more attention on their service, attracting more advertisers, and incentivizing more superficial engagements. The same thing happens everywhere on the web: from SEO, to content farms, to clickbait, to “fake news”. We can imagine alternatives though. For instance, a cooperatively owned Twitter, where it would be owned and managed by the users who could build a social media platform that incentivized less profitable, but more useful behaviors. And the blockchain presents some entirely new possibilities for decentralized ownership of these platforms – though at the moment these exist more in the hype of their backers than in any practical model. But whatever answer we come up with, the point is that we desperately need to claw back control of digital platforms, especially as they come to own and dominate the rest of the economy.

AG: You seem to share the awareness of the possible usage of the internet for manipulation that have been outlined by people like Bifo Berardi.

NS: It’s undoubtedly true that social media has been manipulating people, but the real question is whether it’s to a different degree than previous media. Look at the uproar around “fake news” influencing the US election and bringing

in Trump. When you go and look at the data you realize that the biggest influence on the outcome wasn't Twitter or social media in general. Instead it was talk radio – a very old medium that is heavily political biased, and that a lot of elderly people frequently listen to. That has been influencing them for decades now. (We could also look at the role of tabloid newspapers in the UK for a similar “old” media example.) There is a rush to blame the newest technologies for our ills, but oftentimes that claim doesn't hold up under scrutiny. I would say that the influence of 4chan was extremely minor during the election, as was the influence of “meme wars.” It is much more traditional things that have been influencing the bringing of Trump to power.

AG: Now, to move a bit back from the particulars: would you say that the 20th century has shown the limits of human politics and economics if not thought in general?

NS: That's a good question. In one, a bit rudimentary, sense – yes. The sort of humanism that doesn't give any consideration to non-humans is, obviously, completely obsolete in an age of ecological crisis. Likewise, the romantic ideals of classical humanism seem to me have been definitely taken apart by poststructuralism and neuroscience. These ideals are still effective as rhetorical tools, but as proper guides to politics, we need to move beyond them.

AG: What does that imply for praxis in contemporary society where direct action and what you call “folk politics” alongside dogmatical humanism does not bring about the absolute change?

NS: I think part of it has to do with developing our capacities for abstract and strategic long-term thinking. That is something that, for example, in the early 20th century was very much built up. You would have something along the lines of the vanguard party, that would look out over the

course of history, determining where things are going and what the role of the working classes was going to be in bringing about the revolution to a new stage of history. It wasn't necessarily the correct analysis of history's structural forces, but it at least gave priority of place to these beyond human elements. Today, we mostly lack these sorts of capacities for thinking long-term and strategically. The result has been more and more focus on tactics and immediacy, and an instinctually reactive politics. So one way to get beyond the limits of humanism and the fetishisation of tactics is to build these capacities again. I think there's more awareness of the need for this stuff lately, and it appears as though there's more engagement with trying to solve this problem. But it's still in the beginning stages.

AG: Is that analysis impacted by "Platform capitalism" in any way? If not, what does such an economical state impact in term of theory?

NS: I think platform capitalism enters in as one of the key actors in the future of politics. If we want to think strategically, these major tech companies need to be in our analysis. Now there's a couple of elements of how they impact future politics. One major one is the ways in which they exert control over other companies – not only through economic means, but also political means. Google and Facebook's dominance over the traditional media industry is a perfect example of this, and to me, quite suggestive of the likely future for other industries as they take on platforms. So, the first way is the influence of platforms on intracapitalist competition. Second is the way that platforms influence social movements and people politics, broadly speaking. Jeremy Gilbert has written some excellent stuff on this, pointing out that much like Fordism and post-Fordism make possible certain forms of organizing and certain forms of political action, so does platform capitalism make possible new forms of political action. These platforms offer

organizing tools and ways of connecting actions that enable us to act in collective ways that just weren't possible 20 years ago. Whether or not this is actually sufficient to take down these platforms, I'm not entirely sure. But the awareness of these material changes is important to thinking about strategy and how we approach political action today.

AG: And in terms of simple economic development, the uniting element of different kinds of platforms does seem not only to be raw data mining but also rent. Can it be said that this is the return of the Marxian "rentier"?

NS: I do think that there is something to be said for that. I need to give more thought to the category of rent, because I'm not entirely convinced that it's the best concept to use here. Oftentimes what we refer to as "rent" can just mean excess profits. But I do think that there is a sort of siphoning of value by platform companies from non-platform ones in ways that are quite intriguing when we think about the aggregate nature and state of capitalism today. I think that the massive accumulation of value by these platform companies is actually not very good for capitalism overall. Far from indicating any kind of revival of capitalism, what we're witnessing is the concentration and centralization of capital within the hand of fewer and fewer platform monopolies. So there are really important questions on the aggregate levels of capitalism about what platform capitalism means. Despite the hype given to these companies, I think they're symptomatic of a period of generalized stagnation.

AG: What about race and gender? Do their identities as oppressed subjects also remain stagnant as does the system, or do they change in times of platforms?

NS: On one hand you have – this is not novel to platform capitalism, just a continuation of a neoliberal period – an

outsourcing of work back onto the family structure, which remains a highly gendered one. So women still largely do most childcare, do most long term care alongside elderly care, most housekeeping, and all the other tasks of social reproduction. What we have been seeing over the last four years is more of this is being pushed back onto an unwaged sector of the family.

And in terms of race, I'm not convinced that platform capitalism has added anything new, so much as inflected existing racial hierarchies through slightly new mechanisms. We have of course the rise of all sorts of algorithmic biases, and the ways in which machine learning draws upon social data means that it too often transfers existing biases into these automated systems. That's perhaps a new type of problem, but it seems a relatively minor inflection of racism when compared to the violence perpetuated by racism through more traditional means. Where race intersects with digital capitalism in more significant ways is perhaps the effects of automation and the production of workless subjects, often in racialised and segregated urban areas. This, again, is nothing new, but it may take on new force as automation proceeds ahead.

AG: Returning to technology: how does the Dot Com boom reflect upon the contemporary platform state of capitalism? Does the possible analogy signify a new bubble?

NS: The economist, Lawrence Summers, has been arguing recently about the significance of financial booms and busts to modern capitalism. His argument in principle is: the equilibrium rate of interest is far too low to bring about the balance between savings and investment and the only way in which that gets resolved is by capitalism constantly inciting cheap money and financial booms in order to get any sort of an economic growth. He points to the Japanese

housing crisis, the American dot com boom, the kind of boom that happened in European peripheral bonds, and the housing boom in US, all in the last 20 years. Looking at these booms and busts, he says that without them we wouldn't have had any growth in the main capitalist economies – they've been essential to any sense of forward momentum in contemporary capitalism. There is something to be said for that.

But while we undoubtedly have some form of unsustainable boom today (it'd be difficult to think otherwise given the effects of quantitative easing and low interest rates), I think it's different from the 90s tech boom. One of the major differences is that in the 90s the aim of a lot of these startup companies was to list themselves on stock market, make a massive amount of money from their IPO and then watch their stock value grow and grow. Today we actually see very few IPOs. There are very few startups moving towards the stock market as a way to make profit (Snap being perhaps the most recent big name one). But most of the tech startups have relied on venture capital and staying private. And if they grow large enough, they eventually get bought out by a company like Google or Facebook. Success for tech firms today is getting bought out by a platform monopoly; whereas success in the 90s dot com boom was making money off of the stock market. Now that has a big effect on the potential impact of these companies going bust, because while many Americans are involved with the stock market in some way (whether through pension plans or some other savings), only a miniscule amount are involved in venture capital. So if the tech sector today is seeing a boom, and a bust happens, I think the impact will be relatively small. (And it's worth recalling that the collapse of the 90s tech boom was limited as well, thanks to it being constrained to the stock market and supported by the Fed's interest rate cuts.)

AG: Does cryptocurrency somehow fit as a possible future influence on such market conditions? Bitcoin seems to be a financial fetish currently.

NS: I think that it has a future as a marginal currency that serves a few functions. I don't see any way in which it replaces national currencies. The technical limitations of something like Bitcoin for rapid and frequent everyday transactions are quite significant. There's also the ecological impact of a lot of blockchain-based systems which again puts heavy limits on how widespread it can become. I think blockchain and, more broadly speaking, digital ledger-based technologies can be quite interesting in use and they have some fascinating potential functions. But I'm quite skeptical that these digital currencies are going to compete with national currencies in any significant way.

AG: Yet speaking solely of blockchain, are there any possible "revolutionary" applications?

NS: Possibly. I need to give it more thought since at the moment it's incredibly difficult to separate the hype from the reality of the blockchain field. When C-list celebrities are marketing their ICO, you know that things have gone a bit crazy. That being said, there's undoubtedly some significant transformative potential from blockchain, but as far as I can see, virtually all of it is conceptual at the moment, and little has been proven a success in actual practice.

AG: It would be justified to bring up the concept of Hyperstition then. Alongside platform capitalism are novel structures as the brand, volatile trading, both of which question our conceptions of classical time orientation. With this apparent dependence on the future, is Hyperstition simply a phenomenon or a tool to be used?

NS: I think it's a tool to be used. The way Alex and I try to formulate it in "Inventing the Future" is basically to see it as one of the instruments through which non-deterministic progress gets embodied and enacted. This was one of the challenges we tried to think through when we were writing: how to get away from these deterministic ideas of progress? If you give up on those absolutes, does that mean the end of progress per se, do you just have this play of differences and that is it? Hyperstition, by contrast, invokes a sense of direction, it orients momentum towards something, without at the same time positing some absolute trajectory of history. So it's a way to conceptualize progress without falling back into more classical motifs.

AG: The last question should probably be easy on the ear. Why become leftist today?

NS: The simplest answer is that capitalism is an elaborate system of constraint and ontological stasis, and that we can do so much better. There is the traditional leftist argument that's based around equality and justice that I find persuasive as well. But one doesn't have to buy into that in order to recognize that capitalism massively restricts our possibilities and ties us into a repetitive cycle of accumulation, and that the project of the left must be to liberate us from it.

Name of Core

MAGENTA PILL

Political Breakdown

LIBERALS, LIBERTARIANS, CRYPTO-SCAMERS, TRADER-
GAMBLERS, GAMBLER-MINERS

Common Beliefs

THE NEW IS COMING AND I SHALL NOT DROWN

Social Constructs

UNSURE, SWING STATE, STARTUP BY NATURE, GETTING AHEAD


Coders

PEOPLE TRYING TO MAKE A FAST BUCK / LAUNCH CRYPTO
ICOS OF DUBIOUS QUALITY / TECHNO-GEEKS AND
PROBLEM SOLVERS WHO HAVE BOUGHT INTO THE HYPE.
FOLLOWERS OF DON TAPSCOTT, DON TAPSCOTT, ANDREAS
M. ANTONOPOULOS, DAVE ASPREY, DANIEL LARIMER,
KATHLEEN BREITMA

Coin

ETHEREUM, TEZOS, STABLE COINS, SCAM ICOS

INTO THE BITCOIN MINES

 dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines

DealB%k WITH FOUNDER
ANDREW ROSS SORKIN

BY NATHANIEL POPPER

DECEMBER 21, 2013 1:42 PM

MINING FOR BITCOINS IN ICELAND

BY RICHARD PERRY ON DECEMBER 21, 2013.

On the flat lava plain of Reykjanesbaer, Iceland, near the Arctic Circle, you can find the mines of Bitcoin.

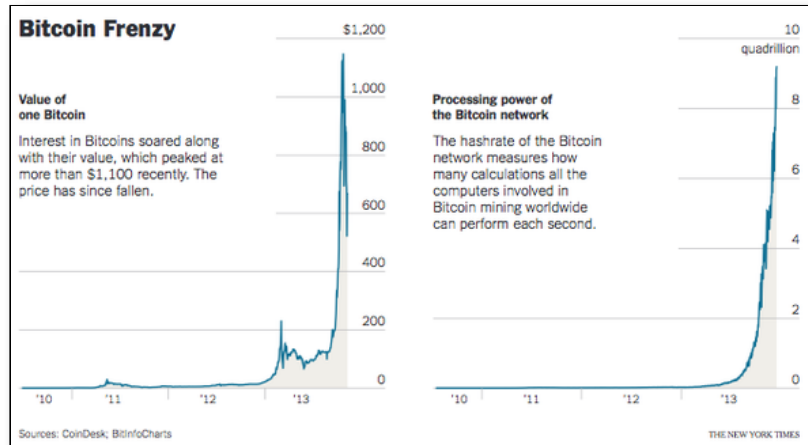
To get there, you pass through a fortified gate and enter a featureless yellow building. After checking in with a guard behind bulletproof glass, you face four more security checkpoints, including a so-called man trap that allows passage only after the door behind you has shut. This brings you to the center of the operation, a fluorescent-lit room with more than 100 whirring silver computers, each in a locked cabinet and each cooled by blasts of Arctic air shot up from vents in the floor.

These computers are the laborers of the virtual mines where Bitcoins are unearthed. Instead of swinging pickaxes, these custom-built machines, which are running an open-source Bitcoin program, perform complex algorithms 24 hours a day. If they come up with the right answers before competitors around the world do, they win a block of 25 new Bitcoins from the virtual currency's decentralized network.

The network is programmed to release 21 million coins eventually. A little more than half are already out in the

world, but because the system will release Bitcoins at a progressively slower rate, the work of mining could take more than 100 years.

The scarcity — along with a speculative mania that has grown up around digital money — has made each new Bitcoin worth as much as \$1,100 in recent weeks.



Bitcoins are invisible money, backed by no government, useful only as a speculative investment or online currency, but creating them commands a surprisingly hefty real-world infrastructure.

“What we have here are money-printing machines,” said Emmanuel Abiodun, 31, founder of the company that built the Iceland installation, shouting above the din of the computers. “We cannot risk that anyone will get to them.”

Mr. Abiodun is one of a number of entrepreneurs who have rushed, gold-fever style, into large-scale Bitcoin mining operations in just the last few months. All of these people are making enormous bets that Bitcoin will not collapse, as it has threatened to do several times.

Just last week, moves by Chinese authorities caused the price of a Bitcoin to drop briefly below \$500. If the system did crash, the new computers would be essentially useless because they are custom-built for Bitcoin mining.

Miners, though, are among the virtual-currency faithful, believing that Bitcoin will turn into a new, cheaper way of sending money around the world, leaving behind its current status as a largely speculative commodity.

Most of the new operations popping up guard their secrecy closely, but Mr. Abiodun agreed to show his installation for the first time. An earnest young Briton, with the casual fashion taste of the tech cognoscenti, he was a computer programmer at HSBC in London when he decided to invest in specialized computers that would carry out constant Bitcoin mining.

The computers that do the work eat up so much energy that electricity costs can be the deciding factor in profitability. There are Bitcoin mining installations in Hong Kong and Washington State, among other places, but Mr. Abiodun chose Iceland, where geothermal and hydroelectric energy are plentiful and cheap. And the arctic air is free and piped in to cool the machines, which often overheat when they are pushed to the outer limits of their computing capacity.



The energy required to run these computers is huge, and has led to criticism that Bitcoin mining is wasteful, not to mention socially useless.

RICHARD PERRY/THE NEW YORK TIMES

The operation can baffle even those entrusted with its care. Helgi Helgason, a burly, bald Icelandic man who oversees the data center that houses the machines, said that when he first heard that a Bitcoin mining operation was moving in he

expected something very different. “I thought we’d bring in machines and put bags behind them and the coins would fall into them,” said Mr. Helgason, with a laugh.

Since then, the education he has received about Bitcoins has been enlightening, but only to a point.

“It’s a strange business,” he said, “and I can’t say that I understand it.”

Until just a few months ago, most Bitcoin mining was done on the home computers of digital-money fanatics. But as the value of a single Bitcoin skyrocketed over the last few months, the competition for new coins set off a race that quickly turned mining into an industrial enterprise.

“Even if you had hardware earlier this year, that is becoming obsolete,” said Greg Schvey, a co-founder of Genesis Block, a virtual-currency research firm. “You are talking about order-of-magnitude jumps.”

The work the computers do is akin to guessing at a lottery number. The faster the computers run, the better chance of guessing that right number and winning valuable coins. So mining entrepreneurs are buying chips and computers designed specifically — and only — for this work. The machines in Iceland are worth about \$20,000 each on the open market.

The energy required to run these computers is huge, and has led to criticism that Bitcoin mining is wasteful, not to mention socially useless. But Mr. Abiodun prides himself on using renewable power, at least in Iceland.

When Mr. Abiodun first heard about Bitcoin mining in 2010, he thought it was a scam. Begun in 2009 as the imaginative creation of an anonymous programmer (or group of programmers) known as Satoshi Nakamoto, it was initially little more than a tech world curiosity. As early users connected their computers into the network, they became a part of the decentralized infrastructure that hosts Bitcoin’s

open-source program. The computers joining the network immediately began capturing virtual coins. The network's protocol was designed to release a new block of Bitcoins every 10 minutes until all 21 million were released, with the blocks getting smaller as time goes on. If the miners in the network take more than 10 minutes to guess the correct code, the Bitcoin program adapts to make the puzzle easier. If they solve the problems in less than 10 minutes, the code becomes harder.

Mr. Abiodun's opinion of Bitcoin changed in January, when he saw the price rising. He installed a free application on his home computer that linked him into the Bitcoin network and set it to mining, harnessing the power of his graphics card, which is the part of a normal computer best suited to doing the code work.

Mr. Abiodun's computer was in the guest room of his house in southeast London. Working at HSBC during the day and tinkering with his Bitcoin system at night, he realized if he wanted to make any money, his computer would have to run around the clock.

The constant computing, however, overheated the graphics card and pushed the computer's exhaust fans into overdrive. When he added another graphics card, then a new computer, the room became too noisy for guests to sleep, and the windows had to be kept open to release the heat. That did not make his wife, Gloria, who was pregnant at the time, very happy.

"It just created a scenario where there was no way our parents would come over to stay," he said. "I did offer to put her parents in a hotel, but that didn't go down well."

Mr. Abiodun's wife finally gave him an ultimatum — either the computers had to go, or he did. At the same time, he was making money, and friends were asking if they could invest in his mining operation.

In February, Mr. Abiodun used the investors' money to buy machines from a start-up dedicated solely to manufacturing specialized mining computers. The competition for those computers is so intense that he had to pay for them and wait for delivery.

When the delays became lengthy, however, he went on eBay and paid \$130,000 for two high-powered machines, which he set up in June in a data center in Kansas City, Kan.

This was the beginning of Mr. Abiodun's company, Cloud Hashing, which rents out computing power to people who want to mine without buying computers themselves. The term hashing refers to the repetitive code guessing that miners do.

Today, all of the machines dedicated to mining Bitcoin have a computing power about 4,500 times the capacity of the United States government's mightiest supercomputer, the IBM Sequoia, according to calculations done by Michael B. Taylor, a professor at the University of California, San Diego. The computing capacity of the Bitcoin network has grown by around 30,000 percent since the beginning of the year.

"This whole new kind of machine has come into existence in the last 12 months," said Professor Taylor, who is studying mining hardware. In the chase for the lucky code that will unlock new Bitcoins, mining computers are also verifying and assigning unique identifying tags to each Bitcoin transaction, acting as accountants for the virtual currency world.

"The network is providing the infrastructure for making sure the currency is being transferred between people according to the rules," Professor Taylor said, "and making sure people aren't creating currency illegally."

Even before Mr. Abiodun's machines in Kansas City were up and running, it was clear that they wouldn't be enough. So he ordered about 100 machines from a start-up in Sweden and, in October, had them moved to the facility in Iceland. In

just a few months, that installation has generated more than \$4 million worth of Bitcoins, at the current value, according to the company's account on the public Bitcoin network.

At the end of each day, the spoils are divided up and sent to Cloud Hashing's customers. Last Wednesday, for example, the entire operation unlocked 225 Bitcoins, valued at around \$160,000 at recent prices. Cloud Hashing keeps about 20 percent of the capacity for its own mining.



Inside a high-security facility in Iceland, one company's powerful computers toil nonstop on the project.

RICHARD PERRY/THE NEW YORK TIMES

The unregulated Bitcoin-mining industry is ripe for abuse, and ventures that sound similar to Cloud Hashing have turned out to be scams. Mr. Abiodun's company has proved itself real, but it is still unclear if it is a good deal for customers. Cloud Hashing charges \$999 to rent a tiny portion of the company's computing power for one year. That's an expensive price for the computing capacity they are getting, but Mr. Abiodun argues that it's a good value because individual miners would not be able to buy his modern machines outright. It's a little like buying a fractional ownership in a private jet; you might not want responsibility for the jet itself, and it's out of your price range anyway. He

also says he provides the maintenance and keeps away thieves and hackers.

Some Cloud Hashing customers have also complained on Internet forums that it can be hard to get a response from the company when something goes wrong. But this has not stopped new contracts from pouring in. Cloud Hashing now has 4,500 customers, up from 1,000 in September.

Mr. Abiodun acknowledges that the company has not been prepared to deal with its rapid growth. He said he had used \$4 million raised from two angel investors to add customer service representatives to offices in Austin, Tex., and London. Cloud Hashing is now preparing to open a mining facility in a data center near Dallas, which will hold more than \$3 million worth of new machines being produced by CoinTerra, a Texas start-up run by a former Samsung chip designer.

The higher energy costs — and required air-conditioning — in Texas are worth it for Mr. Abiodun. He wants his operation to be widely distributed in case of power shortages or regulatory issues in one location. But he is also expanding his Icelandic operation, shipping in about 66 machines that have been running for the last few months near their manufacturer in Ukraine.

Mr. Abiodun said that by February, he hopes to have about 15 percent of the entire computing power of the Bitcoin network, significantly more than any other operation.

Inside the Iceland data center, which also hosts servers for large companies like BMW and is guarded and maintained by a company called Verne Global, strapping Icelandic men in black outfits were at work recently setting up the racks for the machines coming from Ukraine. Gazing over his creation, Mr. Abiodun had a look that was somewhere between pride and anxiety, and spoke about the virtues of this Icelandic facility where the power has not gone down once.

“We don’t want downtime — ever, never,” he said. “Not with what we paid. Not with Bitcoin.”

IN CHINA'S HINTERLANDS, WORKERS MINE BITCOIN FOR A DIGITAL FORTUNE

nytimes.com/2017/09/13/business/bitcoin-mine-china.html

September 13, 2017

BY CAO LI AND GIULIA MARCHI



Credit Giulia Marchi for The New York Times

DALAD BANNER, China — They worked as factory hands, in the coal business and as farmers. Their spirits rose when a coal boom promised to bring factories and jobs to this land of grassy plains in Inner Mongolia. When the boom ebbed, they looked for work wherever they could.

Today, many have found it at a place that makes money — the digital kind.

Here, in what is locally called the Dalad Economic Development Zone, lies one of the biggest Bitcoin farms in the world. These eight factory buildings with blue-tin roofs

account for nearly one-twentieth of the world's daily production of the cryptocurrency.



Credit Giulia Marchi for The New York Times

Based on today's prices, it issues \$318,000 in digital currency a day.

From the outside, the factory — owned by a company called Bitmain China — does not look much different from the other buildings in the industrial park.



Credit Giulia Marchi for The New York Times

Its neighbors include chemical plants and aluminum smelters. Some of the buildings in the zone were never finished.

Except for the occasional coal-carrying truck, the roads are largely silent.

Inside, instead of heavy industrial machinery, workers tend rows and rows of computers — nearly 25,000 computers in all — crunching the mathematical problems that create Bitcoin.

Workers carry laptop computers as they walk the aisles looking for breakdowns and checking cable connections. They fill water tanks that keep the computers from melting down or bursting into flame. Around them, hundreds of thousands of cooling fans fill the building with whooshing white noise.



Credit Giulia Marchi for The New York Times

Bitcoin's believers say it will be the currency of the future. Purely electronic, it can be sent across borders anonymously without oversight by a central authority. That makes it appealing to a diverse and sometimes mismatched group that includes tech enthusiasts, civil libertarians, hackers and criminals.

Bitcoin is also, by and large, made in China. The country makes more than two-thirds of all Bitcoin issued daily. Bitmain, founded by Jihan Wu, a former investment analyst,

makes money mostly by selling equipment to make Bitcoins, as well as mining the currency itself.



Credit Giulia Marchi for The New York Times

China has mixed feelings about Bitcoin.

On one hand, the government worries that Bitcoin will allow Chinese people to bypass its strict limits on how much money they can send abroad, and could also be used to commit crimes. Chinese officials are moving to close Bitcoin exchanges, where the currency is bought and sold, though they have not set a time frame. While that would not affect Bitcoin manufacturing directly, it would make buying and selling Bitcoin more expensive in one of its major markets, potentially hurting prices.

On the other hand, the digital currency may represent an opportunity for China to push into new technologies, a motivation behind its extensive push into [other cutting-edge areas](#), like driverless cars and artificial intelligence. China continues to offer Bitcoin makers like Bitmain cheap electricity — making Bitcoin requires immense amounts of power — and other inducements.



Credit Giulia Marchi for The New York Times

Dalad Banner may be far away from Beijing's internet start-up scene and southern China's gadget hub. Still, many of the workers and surrounding residents see a digital opportunity for Dalad Banner and the rest of their part of Inner Mongolia, an area famous in China for half-finished factories and towns so empty that they are sometimes called ghost cities.

"Now the mine has about 50 employees," said Wang Wei, the manager of Bitmain China's Dalad Banner facility, using one of several metaphors for the work being done there. "I feel in the future it might bring hundreds or even thousands of jobs, like the big factories."

Mr. Wang, a 36-year-old resident and former coal salesman, purchased one Bitcoin about six months ago. It has since more than doubled in value. "I made quite a lot of money," he said.



Credit Giulia Marchi for The New York Times

China also sees a potential new source of jobs, particularly in underdeveloped places like Dalad Banner. The county of about 370,000 people on the edge of the vast Kubuqi Desert boasts coal reserves and coal-powered heavy industries like steel. But it lags behind much of the rest of the country in broadly developing its economy. It is part of the urban area of Ordos, a city about 350 miles away from Beijing [famous](#) for its [empty buildings](#) .



Credit Giulia Marchi for The New York Times

Dalad Banner is not the sort of place that at first glance looks like a home for high-tech work. Indeed, the idea took some

getting used to, even among the workers.

“I didn’t know anything about Bitcoin then,” said Li Shuangsheng, a 28-year-old resident who maintains the operations of one of the eight factories.

He bounced from job to job — the chemical plant was too noisy and polluted, he said — before he landed about one month ago at Bitmain China’s Dalad Banner factory, one of the few lucrative job opportunities in the sparsely populated region.



Credit Giulia Marchi for The New York Times

Mr. Li does not yet own any Bitcoin, but he is happy with the work and studying up on the subject online when family time permits.

“Now,” he said, “I’m starting to have some idea.”

Many at the farm have experienced the ups and downs of the local economy.

Bai Xiaotu was laid off from a state-owned furniture factory in 1997. He had been doing different menial jobs until he went to work at Bitmain’s Dalad Banner farm in December as a cleaner.



Credit Giulia Marchi for The New York Times

“Look around, there are abandoned factories on both sides of our farm,” said Mr. Bai, a 53-year-old with a weather-beaten face. “Many factories are not doing that great.”

But the industry is still new to most. Bai Dong, Mr. Bai’s 31-year-old son, had never heard of Bitcoin when his father first got the job. After searching on the internet, he found that the Bitcoin price was rising quickly and that the farm was one of the biggest in the world. “I feel positive about the future of the industry,” Mr. Bai said.

But he is still confused what Bitcoin mining is.

“We have coal mines,” he said. “Now we have a Bitcoin mine. They are both mines. What’s their relationship?”

CRYPTORAVE READER



Credit Giulia Marchi for The New York Times

WHAT TO EXPECT IN 2019 AND BEYOND, ACCORDING TO 14 CRYPTO LUMINARIES

breakermag.com/what-to-expect-in-2019-and-beyond-according-to-14-crypto-luminaries/

BY MARK YARM

December 26, 2018

In BREAKER's first (not even full) year of operation, we conducted dozens of Q&As with some of the biggest names in blockchain and cryptocurrency. As you might imagine, the subject of the future came up quite a bit. Here's a sampling of what those tech luminaries predicted for 2019 and beyond:

"I'm assuming within the next year or so, we're going to make it so that everyone can just, with their cell phone, buy a cup of coffee with bitcoin."

— [Tim Draper](#) , founder of [Draper Associates](#)

"We just have to work much harder on helping [people] understand where ConsenSys came from and what it is, philosophically. It keeps evolving. It's been several different ConsenSyses since the start.... We have to up our game and compete. It no longer is sufficient to show up and do something cool; now we have to do something excellent."

— [Joseph Lubin](#) , founder of [ConsenSys](#)

"I think we've gone through this orgy of unfettered capitalism. And [the space] has become very tone deaf. It's become very illogical, and frankly, it's become unproductive. We're throwing good money after bad. I'm excited about a period of depressed prices where we can focus on really building . Now we need to bring some rationality, pragmatism, and risk management to the crypto asset space."

— [Meltem Demirors](#) , chief strategy officer at [CoinShares](#)

“Do I think I’ll be found guilty of embezzlement and data manipulation? I still think so, yes. I declared at the beginning of the trial I am innocent of the charges brought against me. But the fact is I’m fighting an uphill battle because in Japan there’s a lot of cases like this ending with conviction. Something like 99 percent.”

— [Mark Karpeles , former CEO of Mt. Gox](#)

“If the [Ethereum] community does continue to rely on me, then I think that would definitely be a problem. The whole point of decentralization is that you can make a system where you don’t need to know which specific people are involved in it and that they’re trustworthy in order to be able to participate in it. So if the de facto assumption for Ethereum’s continued existence is that I do certain specific things, then that’s a big risk to anyone in the Ethereum ecosystem—and obviously a large loss of freedom for myself.”

— [Vitalik Buterin , cofounder of Ethereum](#)

“Whether Ethereum is able to get to the levels of scaling that are needed, I think, is yet to be seen. [But] once the scaling problems are solved, once governance issues are solved, I think it’s going to take off and we’re going to see the next evolution of things. It’s very early days.”

— [Anthony Di Iorio , cofounder of Ethereum](#)

“If I win the [2020 presidential] nomination, I’m going to start on a rant about the marginalization of third parties—and when I go on a fucking rant, the world listens.”

— [John McAfee , antivirus-software pioneer and cryptocurrency evangelist](#)

“Maybe [seven] years from now, when I’m 35, I’ll try to become the president. I have a lot of learning to do, a lot of people to learn from. I have to learn how to build a company, how to build relationships. I’m going back to school—not physical school. But I’m going back to learning, which is what I’m doing here with my partners and my company.”

— [Charlie Shrem , founder of Crypto.IQ](#)

“Blockchains haven’t even begun to scratch the surface of their biggest use case, which is digital money. That’s huge, and there’s a lot to chew on before you get into any of the other, exotic use cases for medical records or whatever. It’s really hard to do digital cash, so I think people have been like, ‘What if we try to do something else instead?’ And I think that’s not a very pragmatic route, actually.”

— [Kathleen Breitman , cofounder of Tezos](#)

“There’s a whole chunk of the American dream wrapped up in this idea that you just need a laptop and a great idea to build a billion-dollar company and win because people love it. That’s something worth fighting for, and something we’ll keep fighting for. I think we’ll win, but it’s been a bad year [with the repeal of net neutrality] for sure.”

— [Alexis Ohanian , cofounder of Reddit](#)

“In the next 10 years? I think that there will be more real-world use cases for blockchain and cryptocurrency. They’ll be more obvious than innovative.... I just made [more obvious than innovative] up today. The first time I’ve ever used it was in this interview. We’ll see.”

— [Tammy Camp , CEO and cofounder of Stronghold](#)

“In 30 years, [bitcoin] will become mainstream. We will see bitcoin as plumbing.... Basically, it will get to be the underlying value network of the world.”

— [Craig Wright , chief scientist at nChain](#)

“Do I have a bleak view about the future? The rosier scenario has never actually existed.... And I used to say, about people who are worried about collapse in the U.S. and U.K., that collapse just means living in the same conditions as the people who grow your coffee. The privileged first-world bubble shatters, and you end up being dumped into the real world where everybody else lives.”

— [Vinay Gupta , CEO of Mattereum](#)

“I’m an eternal optimist. I think we’re going to get there. But the universe loves drama, and if all of this were a movie, you’d want to take it right to the brink. And then

the day is saved at the very end. Of course, the universe wouldn't just make it smooth and simple. It's gonna have suspense."

— *Brock Pierce , chairman of the Bitcoin Foundation*

Name of Core

GREEN PILL

Political Breakdown

ANARCHISTS, HACKERS, ETHICAL CODERS, HIGHLY MOBILE
CLASS

Common Beliefs

TECHNOLOGY IS POLITICAL, TECHNOLOGY TRANSFORMS
THE SOCIAL. CODERS, HACKERS AND THINKERS HAVE A
RESPONSIBILITY TOWARDS CREATING "FAIR" TECH FOR ALL.
WE DO NOT WANT TO EMANCIPATE THE PEOPLE, WE WANT
THEM TO EMANCIPATE THEMSELVES...AND NO REVOLUTION
WAS EVER PEACEFUL.

Social Constructs

NO BORDERS NO NATIONS, NO MASTERS NO GODS.

Coders

FIRST GENERATION CRYPTO MINERS (SOME ARE NOW WELL-
OFF AND INVESTING THEIR "LOTTERY-WINNINGS" INTO
PROJECTS AND COLLECTIVES THEY BELIEVE IN. HAVING BEEN
FREED BY CRYPTO FROM THE SHACKLES OF THE LABOUR
MARKET, THEY INVEST TIME AND MONEY IN THE CAUSES
THEY BELIEVE IN), HACKERS, CODERS, AMIR TAAKI, SUSANNE
TARKOWSKI TEMPELHOF, VITALIK BUTERIN, GAVIN WOOD,
INSTITUTE OF CRYPTOANARCHY, GLEN WEYL

Coin

ETHEREUM, MONERO, BITCOIN, ZCASH, HOLO

THE CRYPTO ANARCHIST MANIFESTO

 activism.net/cypherpunk/crypto-anarchy.html

From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST

Cypherpunks of the World,

Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May

.....

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business,

and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be

active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

--

.....
 Timothy C. May | Crypto Anarchy: encryption, digital money,
 tcmay@netcom.com | anonymous networks, digital pseudonyms, zero
 408-688-5409 | knowledge, reputations, information markets,
 W.A.S.T.E.: Aptos, CA | black markets, collapse of governments.
 Higher Power: 2^756839 | PGP Public Key: by arrangement.

Bitcoin, the end of the Taboo on Money

Denis Jaromil Roio, Planetary Collegium Ph.D. candidate, M-Node

6 April 2013, version 1.0

Abstract: Bitcoin is a decentralized system of digital authentication that facilitates the circulation of value on the Internet without the presence of any intermediaries, a characteristic that has often gained it the definition of “digital cash” or “crypto currency”, since it can be used as money for payments. This article consists in a technoetic inquiry into the origins of this technology and its evolution. This inquiry will take in consideration the biopolitical dynamics that govern the Bitcoin community as well specific characteristics of the technical realization, aiming to provide insights on the future of this technology as well a post-humanist interpretation of its emergence.

Keywords: Bitcoin, Crypto, Currency, Digital, Network, Community, Technoetic

Contents

1	Acknowledgments	2
2	Introduction	3
3	Origins	3
4	Memorable events	4
5	Innovation	5
5.1	Networked computing	5
5.2	Why mining	6
5.3	Accounting science	6
6	Community	8
7	Passion	10
8	Glory	12
9	Popularity	14
10	Conclusion	15
11	Contributor details	16
12	References	17

1 Acknowledgments

Bitcoin, the end of the Taboo on Money

from the DYNDY.net article series

© 2013 Dyne.org Digital Press

E-mail: <press@dyne.org>

Author: Denis Roio aka Jaromil

Peer reviewed by: Christian Nold, Susanne Jaschko, Debra Solomon, Marco Sachy, Amir Taaki

Revisions:

- 6 April 2013 - first public edition

The original source of distribution for this article, also providing its most up to date version, is the Internet website
<http://jaromil.dyne.org/writings>

This content is licensed as Creative Commons "BY-NC-SA" 3.0 in the jurisdiction of the Netherlands: it is free to be copied, republished for non-commercial use, quoted and remixed by providing correct attribution to its author(s), while all derivative works must adopt the same license. Different licensing conditions can be arranged, those interested can write to Dyne.org Press <press@dyne.org>

Please support free publishing donating Bitcoins to 1LwSugK8X8kRpV3sex9f8KTjVPc52FPaEq

More ways to donate are available, see <http://www.dyne.org/donate>

ENGLISH LICENSE TEXT (TRANSLATION)

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Netherlands License. To view a copy of this license (english translation), visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

DUTCH LICENSE TEXT (ORIGINAL)

Dit werk is gelicenseerd onder een Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 3.0 Nederland. Bezoek <http://creativecommons.org/licenses/by-nc-sa/3.0/nl/> om een kopie te zien van de licentie of stuur een brief naar Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

2 Introduction

The most powerful forces, those that interest us the most, are not in a specular and negative relation to modernity, to the contrary they move on transversal trajectories. On this basis we shouldn't conclude that they oppose everything that is modern and rational, but that are engaged in creating new forms of rationality and new forms of liberation.

Negri and Hardt, 2010, "Commonwealth"

This article doesn't aim to describe what Bitcoin is to the reader: there are several information sources that already accomplish that, starting from well designed video animations¹, vast numbers of press and academic articles listed on the wikipedia entry², and even a rather positive dramatization in an episode of the popular TV series "The Good Wife"³.

Rather than divulging the functionality of Bitcoin or its vulnerabilities, or even building an interpretation of it according to economic theories, this article investigates historical and philosophical aspects related to the emergence of this technology. In order to do so, the writer has been involved for more than two years within the Bitcoin community, engaging in both cooperative and critical exchanges with its peers.

Money is a fundamental medium upon which to build constituency and consolidate sovereignty. This research investigates the need for such a constituency, its urgency and emergence as a form of subjectivation. Ultimately this article provides a picture of the cultural context in which Bitcoin was grafted and has grown up to what it is now, offering keys to interpretation of its social and political aspects.

3 Origins

In 1994, almost two decades ago, a vast amount of time for the rythms of digital life, Steven Levy published in Wired an article titled "E-Money (That's What I Want)"⁴ with an introduction that left no doubts to the reader:

"The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's, not only going to revolutionize the Net, it will change the global economy."

For those who don't know Steven Levy, author of books like "Crypto" or "Hackers", let me just say that he is not the visionary type: his writings contain very little fantasy at all, and follow a journalistic approach in documenting the stories he investigates. In this article he voices the case of David Chaum "the bearded and ponytailed founder of DigiCash" who was working in Amsterdam to "catapult our currency system into the 21st century". In fact almost 20 years ago David Chaum was a researcher in the CWI, the national research institute for mathematics and computer science in the Netherlands, where in recent times I've had the honor to explain how Bitcoin functions⁵ in front of an audience of scientists that have worked with Chaum and, who honestly made me feel quite embarassed until I understood modesty is definitely one of their qualities.

Because I would like to start this article with an historical perspective, I can't help but track the origins of the evolution that Bitcoin represents into circumstances so well debunked in Levy's article, which once again was absolutely ahead of its time.

But that's not all. Bitcoin is not just "digital cash". Its birth and growth has been fostered by a network of trust that, to some degrees, shared ethical principles and the gestation of a constituency: I'm talking about hackers.

Bitcoin first appeared to the eyes of the hacker community in a Slashdot post⁶ which, on August 2010, announced the release of version 0.3. Previous to that, Bitcoin was only known on some minor cryptographer's mailinglist

¹Video introduction to Bitcoin "We Use Coins" <http://www.weusecoins.com>

²References for the Bitcoin entry on Wikipedia <http://en.wikipedia.org/wiki/Bitcoin#References>

³The Good Wife TV series on CBS, season 3 episode 13, recap: <http://blogs.wsj.com/speakeasy/2012/01/16/the-good-wife-season-3-episode-13-bitcoin-for-dummies-tv-recap/>

⁴Levy's article on Wired: <http://www.wired.com/wired/archive/2.12/emoney.html>

⁵Software Freedom Day, 2011, video recording online here: <http://www.youtube.com/watch?v=hdNRw-LWDUY>

⁶Slashdot post on <http://news.slashdot.org/story/10/07/11/1747245/Bitcoin-Releases-Version-03>

which as of today stopped to function. The post I'm mentioning announced the birth of a software that, through the distributed work of all on-line participants, would have created some unique "hashes" which could then be interchanged as "digital cash". Hackers at that time were already familiar with this concept as a similar implementation was circulating already for using a so called "hashcash" to fight spam online, basically putting a computational price on every email server willing to exchange emails. Also the distributed, or clustered architecture of this software sounded familiar, since many of us thought this would be some kind of SETI@Home, a software that distributed the computational work needed to analyze signals from outer space gathered by NASA observatories.

4 Memorable events

In two and a half years following the presentation to the hacker community at large, I'm individuating 2 memorable events that will help us understand Bitcoin's historical progression.

January 2011 Wikileaks financial blockade
9 May 2011 Forbes publishes its first article on Bitcoin

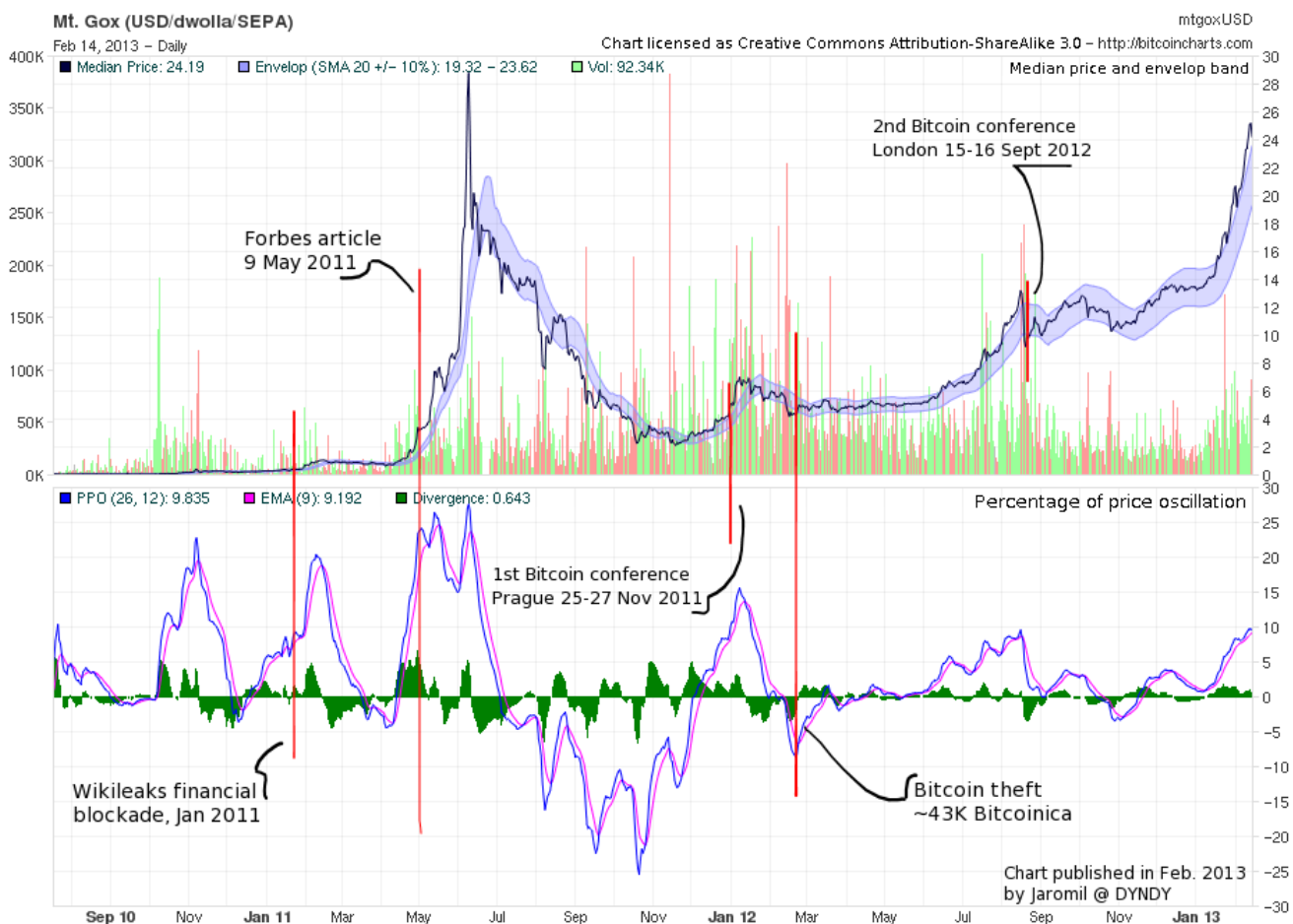


Figure 1: Price graph of memorable events

In *Figure 1* we overlap the chronology of these events to a graph showing the exchange rate of dollar vs Bitcoin on its biggest market "MtGox". The graph is doubled: above is the average exchange value and below is the

percentage of oscillation of the price. This graph helps to outline the influence that socially relevant events have on Bitcoin's financial values.

In the rest of this article I will refer to these two events, trying to explain the complex relationships that govern social and political aspects of Bitcoin. The chart in Figure 1 is probably as close as I'll get in linking such relationships to *financial phenomena*, because as abstract models of human action they have very little importance in my enquiry.

My ambition is to describe Bitcoin's technopolitical innovation without following universals - such universals as those populating most academic disciplined views in *economy*.

Hence, I declare the method of this analysis as *biopolitical*, in the sense that Michel Foucault gave to this word: the early genealogy of a new ethical sense, an enquiry into its gestation phase through the analysis of its processes of subjectivation. *This is Post-humanist Economics*.

5 Innovation

5.1 Networked computing

The physical property of symbols influences decisively the structure of the codes. It is influenced more by this than by the criterion of meaning. The structure of a message reflects the physical character of its symbols more than the structure of the universe it communicates. This explains the famous sentence "The medium is the message".

Vilém Flusser

First of all we need to better explain to the reader what networked computing actually is, a concept to which we'll also refer as clustering.

Clustering is a way to approach problems that are too big to be solved by a single computer, because for instance they require too much computation over a too wide range of data. Clustering a problem means to break it into smaller chunks and then to distribute these chunks to different computer units which all work towards the common goal, such that everyone does a part. It also means that those computers that have less to do, for instance because they are not used at certain moments, can autonomously offer their help to the cluster network that are a part of. One can imagine the situation in which, in a single room with 10 computers, only 5 are being used, those few users can benefit from a faster performance thanks to clustering.

This is no science-fiction, nor a brilliant new idea, although it has been never implemented on the consumer market, probably because it doesn't make a profit for hardware or software manufacturers. Still, back in 2001, when we published the free operating system Dyne:bolic⁷, its clustering feature, implemented via the Linux kernel patch called OpenMosix, was one of the most appreciated by its users. The feature was announced with the slogan *El computador unido jamas sera' vencido* and it let people accelerate onerous tasks on slow computers (i.e. 3d renderings) by sharing the computational load amongst multiple machines: a perfect situation for grass-roots media-labs that have no money to buy computers and, rather than upgrading their hardware, tend to rely on the number of cheap units that they can recycle from the trash and donations.

The OpenMosix cluster implementation in Dyne:bolic is just an example of how networked computing relates to the economical and political aspects of digital societies. Out of the digital and back to the physical world, the mode of production and distribution of resources in networked computing is extremely relevant for the "energy grid" contemporary discourse.

Back to Bitcoin, while we individuate a clustering architecture in its implementation of a proof of work, we are still far from comprehending the real value that backs Bitcoins. In fact, the kind of work required to "mine" Bitcoins is very far from being connected to real life values: looking for particular numbers whose hashes start with 6 zeros, to make it simple, is nothing more than a quest for numbers.

We need to dig further than that to understand the sense of Bitcoin mining and dispel some legitimate doubts about it being a waste of energy. While its networked computing approach was appealing (hackers inherently love to "cluster things") it is hard to be immediately convinced about the real value of such an operation: only a

⁷The dyne:bolic GNU/Linux OS homepage is <http://www.dynebolic.org>

few initially understood why one should run such an algorithm to transform electricity and tech gear in somehow spendable numbers.

5.2 Why mining

Mining is the act of creating Bitcoins, basically the act of finding this “algorithmical mineral” and minting it into usable tokens. The process of mining is therefore remunerative for those who challenge it, by running the Bitcoin mining software on their computers. In simple terms, mining transforms electricity into Bitcoins: computers look for numbers that are not yet discovered and, once they found them, they can be relayed as coins within the network. Miners are generating the wealth, then they put it in circulation at their own discretion.

Back in March 2011, still a few months before the popularization of Bitcoin which unavoidably raised the level of noise for the discussion about it, netizen Mira Luna blogged on his/her journal “Trust is the Only Currency” what I believe to be the best criticism elaborated upon Bitcoin. I’ll quote here the conclusion of this blog post, titled “BitCoin: a Rube-Goldberg machine for buying electricity”⁸:

In the end, the artificial creation of the limited number of possible BitCoins via this "proof of work" (doing millions of SHA-256 hashes over and over) is madness. All you really need is to have "proof of limitation" without the politics—was the market restrained from creating too much money too fast? BitCoin's use of a procedural solution is the wrong track when all you need do is define a constraint via a formula and apply it as needed over time, instead of everyone continuously spinning a hash function and wasting electricity. Keep the transactions public, cryptographically sign them, and audit them with a money model and you'll be able to keep much of what is good about BitCoin. And of course, use a "commodity" the people can intuitively understand, something like... time.

To go further this criticism we need to explain what this *madness* is and why it can be considered instead an interesting innovation. When miners do their work (hence consuming electricity) Bitcoins “magically” appear, but their work also benefits the community: they strenghten the network of trust by making bitcoins less likely to be counterfeited.

The computation of mining and hence the electricity, is to strenghten the authentication of Bitcoin. Now let us consider the energy that was required, before the existence of Bitcoin, to authenticate the minting process of currency made in paper and less noble metals. It consists of a secret minting procedure, big machinery, a monumental building with thick walls and armed guards on its perimeter: an unstable kind of energy, very difficult to govern, as it relates to a *monopoly on violence* imposed by the sovereign state.

This very energy is substituted by Bitcoin with a qualitatively different approach: Bitcoin distributes peers to the task of building *trust in its authenticity*. The networked computation of all miners serves as a mint and dissolves the need for violence into an unlimited, unreachable and decentralized power.

Clustering the mint gathers the energy necessary to establish and protect the authenticity of the currency.

In other words: participation has substituted violence in the physical implementation of currency authentication: a recognizable pattern when we observe historical manifestations of the digital plane of immanence.

This passages leaves still open the problem of redistribution for the minted coins: it does not solve the problem of shared wealth. But we are now back to a familiar problem for money, after having dispelled the risk of a paradoxical machine, the Rube-Goldberg, which would have dissolved the Bitcoin’s concept of work in pure entropy.

5.3 Accounting science

The most remarkable innovation brought by Bitcoin deals with the system of accounting that we use today. Double-entry bookkeeping is what we use today to make sure that earnings and expenditures match, basically authenticating the flow of money and making sure “nothing is duplicated”.

From an historical perspective, the double-entry bookkeeping system is very ancient and barely actualised through the ages: it was described by an Italian mathematician and Franciscan friar named Luca Pacioli in his book “Summa de arithmetica, geometria, proportioni et proportionalità” published in 1494 in Venice. The second

⁸Blog article on <http://trustcurrency.blogspot.nl/2011/03/bitcoin-rube-goldberg-machine-for.html>



Figure 2: Friar Luca Pacioli (portrait by Jacopo de Barbari, 1495)

half of his book, dedicated to geometry, is a section titled “Trattato de computi e delle scritture” in which he describes the necessity of mathematics in accountancy. Those principles were certainly not invented by Pacioli, but mostly actualised, formalised and translated in his tractatus, as demonstrated by the existence of a previous book “Della mercatura e del mercante perfetto” by Benedikt Kotruljević published in Latin some decades before, or as hinted by the presence of another figure behind his portrait in the famous painting attributed to Jacopo de’ Barbari (*Figure 2*) who is believed to be Albrecht Dürer, an artist and traveler who shared Pacioli’s passion for geometry and magic.

Such a system is still, as of today and despite its flaws, the one in use on large scale around the world by most accountancy systems. Being a system that ensures the univoque matching of what is written with what is real, it can be seen as gateway to the digital dimension and can undoubtedly benefit from the technical innovation through digital tools. Hence my argument that Bitcoin is basically this innovation or, more precisely, the implementation of an innovation as the *triple-signed receipt* method. Quoting Ian Grigg:

The digitally signed receipt, with the entire authorisation for a transaction, represents a dramatic challenge to double entry bookkeeping at least at the conceptual level. The cryptographic invention of the digital signature gives powerful evidentiary force to the receipt, and in practice reduces the accounting problem to one of the receipt’s presence or its absence. This problem is solved by sharing the

records - each of the agents has a good copy. In some strict sense of relational database theory, double entry book keeping is now redundant.⁹

The accounting system of triple-signed receipts in Bitcoin respects the original role of money as contract (and digitized speech, I'd argue). Quoting Marco Sacy's research on complementary and alternative currency:

The ontology of money is as relational, abstract and cogent as agreements are in general and the possibilities to formulate these agreements are unimaginable, bearing in mind that the orthodox process of currency design and creation is - drawing from Adorno and Horkheimer's Dialectic of the Enlightenment - an arbitrary and historically determined one.

It is the very substance of those *cogent agreements* that money represents and can be verified by matching declarations on two books or, as Bitcoin does, calling the whole network of participating peers to witness every contract and entangling it into a cryptographic blockchain. Simply put, this is bookkeeping in the age of Bitcoin.

6 Community

At the core... is the idea that people should design for themselves their own houses, streets and communities. This idea... comes simply from the observation that most of the wonderful places of the world were not made by architects but by the people.

Christopher Alexander

When talking about Bitcoin, of its inherent qualities of networked creation of value that were just mentioned, we can't ignore the fact that this technology relies on community dynamics to the point one could state that Bitcoin makes it possible for *money to become a common* and no longer a top-down convention imposed by a sovereign and its liturgy of power.

But then we are faced by a crucial question about Bitcoin: what for? who benefits from it? or, in other words, if the community aspect of Bitcoin is crucial (as in: distributing the computation needed for its authentication, sharing a common currency, a common history of transactions, a common way to quantify wealth) what do the communities use Bitcoin for?

The earliest communities that adopted Bitcoin, aside from the hacker community that never really used it much as a currency to exchange goods, are perfect scapegoats for those who want to turn Bitcoin down. In fact, anyone willing to take a moralistic approach and prohibit the innovation that we are talking about doesn't even need to approach itching concepts such as state sovereignty. It is very easy for witch-hunters to emphasize the fact that drugs were bought and sold with Bitcoins, that gamblers love Bitcoins and that some website claims to accept Bitcoin payments for assassination missions. Criminalizing campaigns have been overly present in the mainstream media coverage immediately following the popularization of Bitcoin, in Italy we've seen even popular prophets of Internet optimism turning against Bitcoin in the blink of an eye¹⁰.

But then, speaking about new technologies, we should never rush to judge their nature and goals from their early adoption. It is natural that those who were excluded from the use of established technologies will look for new as yet unregulated platforms: pioneers at the margins are always attentive about the concrete possibilities of liberation offered by new and unknown tech. When speaking of communication technologies this becomes very clear: all kinds of marginalized and criminalized communities resort to lesser known channels of communication for their needs, while mass communication channels are well policed and in general dominated by the sanitized discourse of the conformed majority. The motivation to debate what moves prohibitionists in their crusade is far from this article, yet what needs to be stated here is that the potential of new tech cannot be studied, understood and judged referring to such circumstances. The examples provided on the early adoption of Bitcoin are in fact misleading to obtain a balanced comprehension of this tech.

The fact is that many hackers love to tease and this attitude, united with a discrete amount of criminals that found it convenient to use Bitcoin since the early phases of its popularization, still offer grounds for the mystification of it as an "evil technology".

⁹Grigg, 2005 - http://iang.org/papers/triple_entry.html

¹⁰People like Riccardo Luna for instance, a televised advocate of Internet and digital innovation in Italy, started a media crusade against what he calls the "Dark web"

Being involved in the community that has grown around Bitcoin I can see that the community is comprised primarily of young idealists rebelling against the status-quo, especially when it consists of a centralized administration prone to corruption. It is clear to many how unjust monopolies are often dominating various contexts, curbing the possibilities of innovation that are in the hands of younger generations. The liberation of the medium of value exchange is an act we refer to as “breaking the Taboo on Money”. Bitcoin has a role in history: its epos coalesces in communities, new ethical reflections, new tales of passion, the glory in all the mystery around its origins. The will for liberation, decentralization and disintermediation is central to Bitcoin - it is ethical and should not be seen as more conflictual than the concrete need to disintermediate many of the systemic functions that are governing modern society. Mind your own long-tailed problems, modern finance!

Many see in Bitcoin the opportunity to challenge the bank monopoly on value transactions. Most goods that were first exchanged on-line for Bitcoins, beyond the dark waters, digital or not, are artisanal creations. The Bitcoin dream is the autonomy of content producers, to exchange their production freely, without aggregations, without intermediaries. After all, most financial transaction operators know well that the reason that small artisans cannot enter on-line markets are the high marginal costs they need to face if they want to accept on-line payments, while the apparata that are able to negotiate trust with banks are imposing themselves as taxing intermediaries.

As a concrete yet slanted hint to the reader, he is my little protest against the **capitalism of flows**, an informal text that I’ve posted on the Nettime discussion list back in April 2011, slightly before the popularization of Bitcoin in the Forbes article published in May. While responding to early criticism of Bitcoin, this letter ended up being circulated on the Bitcoin forum and as the “Bitcoin Manifesto”, gathering approval from different members of the community¹¹:

On Thu, 07 Apr 2011, a...@aharonic.net wrote:

> bitcoins - isn't this simply a distributed structure to do capitalism with?

That's not even the worst you can do with it. you can do money laundering, buy drugs online and sex toys, all anonymously. but that's not the point, because despite the coercion imposed by all kinds of regulatory systems so far, also current official monetary systems are full of that shit, on top of the capitalist pie.

Emerging technologies should never be judged by the sensationally bad taste of early adopters. it's like being concerned about the shit that fertilizes some beautiful flowers, wasting their seeds.

What bitcoin really is, I finally understood on the 6 april (which somehow always ends up being a magic day, eh!): this is now the end of the **flow capitalism**, which consists of the monopoly on transactions, the hegemony of banks on the movement of values and not just their storage, this middle-man mafia strangling the world as we speak.

How right are those South American countries asking for the “taxation of transactions”, an argument refrained in many speeches of the *compañeros*. They studied the system and understood that there is a crucial problem, that needs to be solved urgently. Yet I'd argue that taxation on transactions cannot be the solution. The solution is to eliminate the flow capitalists.

If I want to give you money I'll give it to you. Me and you, period. Its fine that we'll pay our taxes for our communities, don't get me wrong this is not a tea bagger argument. Its just not right that all what we do is in the hands of a third party that has already been caught cheating many times: look at what happened at the Paypal accounts of the Iraqi Linux user group back in 2004, or even more recently to Wikileaks.

We don't need those fat cheaters to be in between our value transactions anymore; the flow capital has played its disgusting role in the little laps of history for which it has been needed, now sadly these people won't give up what they have accumulated, so it makes more sense to leave them alone and multiply more monetary systems that work efficiently across diverse networks and that rely on the neutrality of a cryptographic authentication.

The death of the flow capital is a new stage for the necrotization of capitalism.

¹¹Bitcoin forum thread “Bitcoin Manifesto” on <https://bitcointalk.org/index.php?topic=5671.0>

Beyond the shouted points made in this little speech lies an important hint: *Bitcoin will be of central importance for migrant economies.*

Today it is easy to witness the existence of large communities that are displaced around the world in the desperate attempt to recuperate over the territorial differential of value for their labour. Many of those who work abroad are sending money back to their families and communicating constantly with them, a natural phenomenon by which the market of telephone and money transfer shops all over the world flourish. These nodes of communication are extremely important for migrants, who can't live without them and most of the time end up being harshly taxed for their use. Monopolies like that of Moneygram or Western Union claim that no commission is applied to transactions, but their de-facto currency rates sometimes hide up to 20% for their profit.

Such profit on transactions is made upon data transfer that is comparable to that of a telephone call and it is not a coincidence that such shops often offer both services. Today there is no reason why such market of digital transaction shouldn't be freed in a fashion similar to what Voice over IP did for telephone monopolies. This is an old vector of evolution offered by the digital dimension and its progressive interaction with reality, that I call *digital immanence*: yet another scheme based on the artificial economy of scarcity is trembling!

7 Passion

Previously I've mentioned that Bitcoin's epos coalesces in new tales of passion.

For every process of subjectivity emerging in history, passion is crucial. Analyses such as the one conducted by Giorgio Agamben in his enquiry on sovereignty and glory show that it was historically possible to codify passion (and its mysteries) into power. Through the analysis of the ancient codes constituting laws and ethics (while also celebrating the glory of angels), Agamben shows that the power (and mystery) of passion is close to that of economy and its birth.

```

---BEGIN TRIBUTE---
#./BitLen
::::::::::::::::::
::::::::::::::::::
::: ' ' ' ' ' ' :
::: ' ' ,xiW,"4x, '
: ,dWWWWXXXxi,4WX,
' dWWWWXXX7" 'X,
  lWWWWXX7 __ _ X
:WWWWXX7 ,xXX7' "^^X
lWWWWX7, _.,+, _.,+,
:WWW7,. '^"- ,'^-'
WW",X: X,
"7^^Xl. _(_x7'
l ( :X: __ _
' . " XX ,xxWWWWX7
)X- "" 4X" .____.
,W X :Xi _.,_
WW X 4XiyXWWXd
"" ,, 4XWWWWXX
, R7X, "447^
R, "4RXk, _ ,
TWk "4RXXi, X',x
lTWk, "4RRR7' 4 XH
:lWWWk, ^" '4
::TTXWWi,_ Xll :..
=====
LEN "rabbi" SASSAMA
1980-2011

```

Figure 3. Extract from a very early chunk of Bitcoin's main blockchain

Figure 3 shows an ASCII extract from the Bitcoin blockchain, a tribute that was irremediably inscribed in the transaction history chain. A memorial to a leader of the “cypherpunk movement” is codified, literally, into Bitcoin’s “blockchain”, decorated with typical hacker irony. This is just a hint of what may appear as an “insider joke”, but is in fact the strong trace of a shared narrative.

The historical episode of passion in Bitcoin is connected to another project that is strictly related to the cypherpunk movement: its name, incredibly well known today, is Wikileaks.

Wikileaks has provided the supreme moment (καρμός) for Bitcoin to become an urgency within the cypherpunk imagination and that of hackers at large; I'm talking about the financial blockade to Wikileaks.

Below is an excerpt of the account that Wikileaks staff makes of this episode on their website, to which is dedicated a whole page:

Since 7th December 2010 an arbitrary and unlawful financial blockade has been imposed by Bank of America, VISA, MasterCard, PayPal and Western Union. The attack has destroyed 95% of our revenue. [...] The blockade is outside of any accountable, public process. It is without democratic oversight or transparency. The US government itself found that there were no lawful grounds to add WikiLeaks to a US financial blockade. [...] The UN High Commissioner for Human Rights has openly criticized the financial blockade against WikiLeaks. [...] The blockade erects a wall between us and our supporters, preventing them from affiliating with and defending the cause of their choice. It violates the competition laws and trade practice legislation of numerous states. It arbitrarily singles out an organization that has

not committed any illegal act in any country and cuts it off from its financial lifeline in every country.
[...]

In the US, our publishing is protected by the First Amendment, as has been repeatedly demonstrated by a wide variety of respected legal experts on the US Constitution. In January 2011 the U.S. Secretary of the Treasury, Timothy C. Geithner, announced that there were no grounds to blacklist WikiLeaks. There are no judgements, or even charges, against WikiLeaks or its staff anywhere in the world.

The blockade was an immediate reaction to the “cablegates” release, where an enormous amount of classified USA diplomatic documents had been published by Wikileaks. This episode did not please many powerful people in USA (arguably, Wikileaks has hit its military-industrial complex in many ways). Though the Wikileaks organization received much appreciation from all over the world, also in the form of monetary donations. While the media wave of cablegates was reverberating through the world’s screens, international transaction monopolies like Maestro and Visa blocked Wikileaks from receiving donations, without a legal mandate, nor a courtcase order. Wikileaks also had its registered Internet domains obscured, with the exception of the one registered in Switzerland.

Hackers believe the world can be changed and, while understanding the importance for code and shared protocols, they are determined to play on *neutral* grounds, which is also a condition for change to happen. Some readers may judge hackers as naïve for believing that there can actually be *network neutrality*, most system analysts, even in the financial sector, have recognised the presence of long-tail errors. Those familiar with the principles enunciated in Taleb’s Black-Swan will agree that it is impossible to establish neutrality within a tainted system, but, for the hacker community at large, the Wikileaks financial blockade was a radically new moment of fundamental betrayal. Thus it was a crucial momentum for the growth of Bitcoin: several hackers adopted it right in those days, feeling it was, rationally, liberally, the next thing to do. The growth of Bitcoin started then, as visible in *Figure 1* it was 5 months previous to the first Forbes article that popularized it.

8 Glory

Glory, in theology as much as in politics, is what takes the place of the inconceivable void that is the idleness of power; nevertheless, is this very inconceivable emptiness that nourishes and feeds the power (or, better said, what the apparatus of power transforms in nourishment)

Giorgio Agamben

Every form of currency, since the very beginning of its earliest forms, has dealt with the grammar of power. It is the establishment of a sovereign and its glory that justifies the shared trust into a symbolic form of value circulation. The investment of power into currency, especially when its not backed by mineral values, is codified in mystery and glory.

Bitcoin is not exempted from such dynamics: it innovates the way the digital becomes tangible, a role with highly disruptive potential. Hence, even when choosing the iconography for its own currency, the Bitcoin community shows a political rupture.

The intriguing mystery of the identity of its disappearing author Satoshi Nakamoto, might seem a detail, but not for our analysis: it is of central importance to the Bitcoin myth and that of future crypto-currencies. Bitcoin has no single monetary authority, but a shared pact and the underlying rationality of a mathematical algorithm - the intangible dream of neutrality. Being deflationary, Bitcoins exist within a finite range of possibilities, a quantity of value that is increasingly difficult to mine. No one can create more Bitcoins than those established to be created in the first place, to the great horror of modern economists that regard fiat currency as a necessary tool to move within the troubled waters of contemporaneity, with good reason indeed. But there is no hierarchy in Bitcoin: meaning literally that there is no sacred origin (ἱεραρχία), no written fate, no single ruler, no second thought on its essence.

Bitcoin promises to be the neutral medium for an economy based on participation, not the edict of a king, a central bank, or their authorized intermediaries - nevertheless, it must be said, Bitcoin did create new riches, those who believed earlier than others in the promise of this algorithm. The rupture offered by this new perspective on money is not dealing with equality or welfare, it might not benefit society or help us get out of the crisis: it is a protest for network neutrality.

Such a medium, we must also admit, will likely incarnate the market freedom of the Austrian school of economics. The European Central Bank has produced an analysis of the Bitcoin scheme in October 2012 reciting:

The theoretical roots of Bitcoin can be found in the Austrian school of economics and its criticism of the current fiat money system and interventions undertaken by governments and other agencies, which, in their view, result in exacerbated business cycles and massive inflation.

This insight should be handled carefully: it might overstate on the ambitions of Bitcoin, which first and foremost is a successful implementation of a system for value transactions in the digital domain, whose success is due to the biopolitical dynamics we are exploring in this article. Nevertheless, the interpretation of its ethos in fieri is not far from reality. It is paradoxical how, in a time in which we face the failure of most Austrian economic theories, we are confronted with narratives that mystify and popularize them on the wave of technical innovation and functional transformation. But this is a reductionist way to describe Bitcoin and it strictly depends from the adoption of universal categories: I am convinced such a method of analysis can't lead the quest for comprehension we are engaging here. So let's take a step back from this dead end and look into Bitcoin's symbology.

If we look back in the history of icons used to mint money, we'll find a long stream of symbols of leadership: heads or bodies of humans or animals that address or signify the power of scientists, rulers, educators, judges or that of a nation-state. Many are the symbols of hierarchy that govern the minting and authentication of the currency, as well symbols of wealth and geographical maps. I'll refrain now from engaging an analysis of such symbols used in the past, but observe that Bitcoin has and will have a different symbology to glorify it.

The iconography of Bitcoin reflects the shared values of the community behind it. If there would be a person representative of it, this would be its mysterious creator Satoshi Nakamoto, but the fact that he doesn't really exist makes things much more interesting. One of the early symbols of Bitcoin was alpaca, for instance the mockup presented here comes from an old forum's thread and in its own way it is meant to celebrate the first artisans that ever sold their creations on the Bitcoin market.

As an experiment, in a previous article for the Bitcoin community I've suggested the use of the empty throne as a bridge symbol across classical, modern and post-human iconography. The image of an empty prepared throne (ἐτοιμασία τοῦ θρόνου) is an icon found in the Old Testament and in books comprising the Upanishad, a sacred icon whose value “..is never so powerful as when the throne is empty”, commented once archaeologist Charles Picard. The empty throne was used on minted currency in the Augustan era and sculpted exemplars of it are found in Knossos and Rome.

But the response of the Bitcoin community to such an old symbol of power, despite the fact it could represent the absence of Satoshi Nakamoto, has been negative. Someone commented that “perhaps a broken empty throne would be even better, symbolizing the breaking of the old power”, someone else suggested that “a physical Bitcoin should have a mirror in the middle. Bitcoin is all about the individual” and again another suggestion “Bitcoin is mercurial – it's quicksilver. It's the fool of the tarot and a touchstone. It turns base electrons into gold. It subverts and debases all norms and conventions. The fool is the perfect symbol for bitcoin”. Many also acclaimed the use of the Guy Fawkes mask, already adopted by Anonymous, from the V for Vendetta comics and movie.

The glory behind Bitcoin is mostly shrouded in mystery, revolt against tyrannical injustice, the reclamation of individual rights, power distribution and the disintermediation and self-determination. But also, I strongly argue, by the transverse presence of a community feeling and the joyous consciousness that a powerful process is unfolding in history: those participating have the possibility to express themselves in their diversity, rather than the uniformed, sterile and omnipresent corporate language of economics.

After the phase in which the Multitude has built its body inside the language, the next opening cycle of conflicts will see the Multitude engaged in the construction of its body beyond language. Christian Marazzi



Figure 3



Figure 4: Protestors weaving a Bitcoin banner in Occupy Amsterdam, July 2012

9 Popularity

By now should be clear that such a process of subjectivation as the one we are describing is not the simple emergence of a new innovative technology, it is not just a *λόγος* on *τέχνη*, it goes well beyond. The enormous popularization of Bitcoin is proof that the dimensions of this process of subjectivation are multiple and cannot be comprehended by adopting a single narrative, and even less so by using the categories of economic analysis.

The popularity of Bitcoin as of today is enormous and still growing: this is a result of the biopolitical progression described above and its inscription inside a particular context, it is not a quality of Bitcoin alone. Bitcoin is rooted in the protest movements that accompanied the financial crisis through 2009 until now, namely the Occupy movement. While there can be reason to conceal this fact for those who hail the unconditioned and instrumental success of Bitcoin, it is important to account this historically in order to understand what might happen in the future.

The cultural scene around Bitcoin is shaped around new values that, despite their many pitfalls, incarnate the rebellion against “The System”. In the last Bitcoin conference in Europe we have clearly seen that those people closest to it are definitely interested in the larger picture: they are conscious that a systemic critique is the underpinning of Bitcoin existence, to the point that the next conference title changed from being focused simply on Bitcoin to being called the “unSystem” conference with among the speakers Anonymous, Occupy London, Voina¹² and Birgitta Jónsdóttir¹³.

Being popular also means to be branched, forked, replicated, cloned, recombined and ultimately appropriated

¹²a Russian street-art group well known for their provocative and politically charged works of performance art.

¹³Member of the Constitutional Assembly of the Icelandic Parliament and former member of Wikileaks.

by the people: a popular icon will feed the mind of popular culture without consuming itself, but confusing its authenticity in the existence of new popular instances. This is already happening to Bitcoin with very interesting consequences. Considering that its popularity is mostly among the hacker (or, should we say, young cyborgs?) community, the branching of Bitcoin is giving birth to many valid technical implementations, that are both capable of functioning on large scale, and explore novel approaches to currency and networking.

Among the first forks of Bitcoin were ironic implementations of it: like Cosby coin featuring the popular TV star Bill Cosby with a computer, or Carrots - just carrots, or Weed which was a currency matched to the value of its developer's favourite Thai beer.

But there are also serious forks of Bitcoin, both alternative or complementary to it, and we can expect more in future: NameCoin (whose functionality is to register new network domains) or Litecoin (which can be mined on the same machines mining Bitcoins, without interference) are just some valid examples.

A particularly interesting one is Freicoin¹⁴ which grafts on ideas by Silvio Gesell for a monetary system with zero interest on credit: the value of currency “decays”, meaning that as time goes by it loses value. Freicoin cannot work as the storage of value, a common practice among Bitcoin users, therefore it circulates faster. By implementing this feature, referred to as “demurrage”, this is one of the most promising forks of Bitcoin today, at least in theory.

With my own pet project in the Bitcoin galaxy, something called Freecoin¹⁵, I've started documenting the phenomenon of forking Bitcoin since its early days and advocated within the community for the “configurability of the genesis code” and in general to leverage the possibilities of customisation for the technology underlying Bitcoin. It is my belief that, while Bitcoin represents a unique political rupture with the old establishment governing money, it is not the ultimate solution to it.

The need for digital currencies based on triple-signed receipts cannot be simply satisfied by Bitcoin. Nevertheless, strengthened by the popularity and all consequences we have explored here, Bitcoin might stand on the longer term as a fixed reference for future implementations: it is realistic to predict that its value will only grow in future.

10 Conclusion

The time has come to explain the title of this article, namely, that Bitcoin is breaking the Taboo on Money. For many years we have taken money for granted, without even questioning its engineering, without analysing accountancy in systemic terms. We have used it and we have been used by it. To paraphrase Georg Simmel, we have made ourselves “indirect beings”, the intermediaries between money and the creation and satisfaction of our own desires.

Just like a taboo that is so close to us to make us turn the other way, we have avoided questioning what makes money exist. In the past 50 and more years people have quietly accepted the transformation of money into something more abstract, far from everyone's hands, in fact becoming just a number in the databases of banks, a gesture of interaction with computers that know more than we do about our possessions. While being the “root of all evil” for some, it has become close to a religion for others, but in both cases money has been too important to be questioned and its evolution too natural to be interfered with by the masses. It is a system that permeates most if not all societal interactions, at least in the Western world, so we assume it to be neutral and, in any cases, we will never question its existence.

Most political analyses study the dynamics related to the distribution of money, its relation to labour, accumulation, use value and exchange values. Universals have governed the entire discourse around monetary engineering

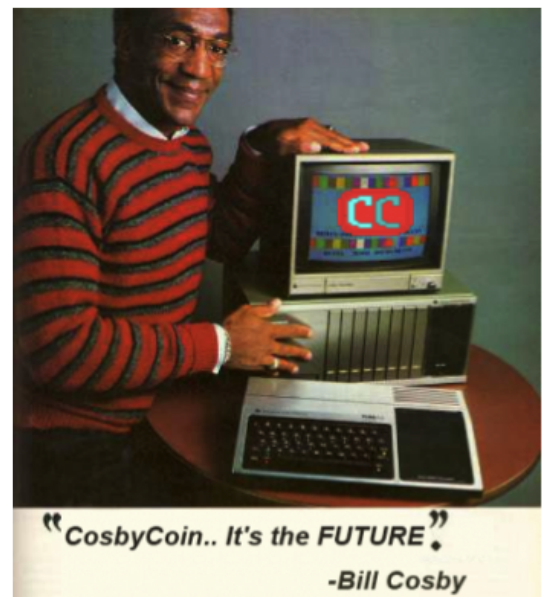


Figure 5: an ironical example of Bitcoin fork

¹⁴“Freicoin: a peer-to-peer digital currency delivering freedom from usury” <http://freico.in>

¹⁵“Freecoin is not a currency, but a suite to create P2P currencies” <http://freecoin.ch>

and mathematical models have been the method to explain its aspects. As a glaring exception to this, there are sociological analyses such as that made by Max Weber that evaluated the relationship between ethics and money across historical mutations of society. Yet, to this day, only few dared to look closer into currency systems and their biopolitical implications, without wearing the protective goggles of historically established universals: this has been a self-imposed taboo for many researchers and practitioners, to dissect this medium, just like a dead body that we are not allowed to study.

Now that money seems to be either dead or dying, it is the time to dare this dissection. It might be the case that, by trespassing this taboo, we will find out ways to change things on a larger scale, especially considering the long due line of innovation in the field of accountancy that has still to be applied.

Ultimately, there are proofs to the rupture I'm pointing out here, in the wake of many new currencies born after Bitcoin: with all irony and irreverence intended. The gates were left open by the mystery man: Satoshi the fool, Satoshi the saint, trespassed the line in front of everyone. There is no longer a taboo on money. Bitcoin is not really about the loss of power of a few governments, but about the possibility for many more people to experiment with the building of new constituencies.

11 Contributor details

Denis Roio, also known by his hacker nickname Jaromil, is an artist, activist and software developer at Dyne.org. His creations are recommended by the FSF and redistributed by several GNU/Linux and BSD operating systems worldwide, while he is also an active contributor to media theory discourses. Jaromil publishes conceptual art in digital form since the year 2000, has lead R&D activities in the Netherlands Media Art Institute for 6 years, was honored with the Vilém Flusser Award in 2009 and awarded a fellowship in the 40 under 40 program for young European leaders in 2012. He is currently writing his Ph.D. as candidate of the Planetary Collegium M-Node at NABA in Milano.




Figure 6: Portrait courtesy of Robert Lloyd

12 References

- Simmel, G., 1900, “Philosophie des Geldes”, DigBib.org
- Foucault, M., 1979, “Cours au Collège de France 1978-1979”, Feltrinelli
- Levy, S., 1994, “E-Money”, Wired USA, issue 2.12
- Lietaer, B., 2001, “The Future of Money”, Random House
- Flusser, V., 2002, “Writings”, Minnesota Univ. press
- Marazzi, C., et al., 2003, “La Moneta nell Impero”, Ombre Corte
- Ascott, R., 2003, “Telematic Embrace”, Univ. California press
- Grigg, I., 2005, “Triple Entry Accounting”, Systemics Inc.
- Agamben, G., 2007, “Il Regno e La Gloria”, Neri Pozza
- Nakamoto, S., 2009, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Bitcoin website
- Negri and Hardt, 2010, “Commonwealth”, Harvard Univ. press
- E.C.B, 2012, “Virtual Currency Schemes”, European Central Bank
- Sachy, M., 2012, “The empowering potential of complementary currencies and alternative payment systems”, Silent University Tate Modern

VITALIK BUTERIN ON THE HARD LESSONS OF ETHEREUM'S FIRST FIVE YEARS

 breakermag.com/vitalik-buterin-on-the-hard-lessons-of-ethereums-first-five-years/

November 12, 2018

BY BRIAN PATRICK EHA

It may be that no one can truly understand what Vitalik Buterin has been through in the five years since writing, at age 19, the white paper describing the Ethereum protocol. As he worked with a group of collaborators to flesh out his design, he came to be seen as not only the inventor of Ethereum but something like its high priest, invested with no formal authority yet wielding tremendous soft power. Even critics say he has borne the responsibility with a maturity beyond his years.

The first major attempt to go beyond bitcoin, the Ethereum network now boasts thousands of developers, and its cryptocurrency, ether, has a market capitalization of more than \$21 billion, which almost certainly makes Buterin one of the wealthiest people in history to have no discernible ego. The New Yorker called him “[indifferently rich](#),” and indeed it is difficult to imagine a humbler or more unprepossessing centimillionaire. In March, when the price of ether was about \$377 (it's now hovering around \$209), Forbes pegged Buterin's net worth at between \$100 million and \$200 million. The success of Ethereum—the network that launched 1,000 coins—has made Buterin not only rich but famous. (William Shatner recently [gave him a thumbs-up](#).) Yet in an age dominated by hard-charging CEOs and the winner-take-all strategies of Uber and Amazon, Buterin seems to be motivated by higher ideals. His peripatetic lifestyle, spending

short stints in one country after another, permits little in the way of material possessions. Just as he depends on the kindness of friends for his temporary abodes, so he seems not to have an unkind bone in his own body. His sincerity is touching. Zooko Wilcox, the founder of Zcash, says Buterin [once told him](#), in the early years of bitcoin, “This is the first technology I’ve ever loved that loves me back.”

Yet if the once painfully shy Buterin has played a crucial role in building the sort of community to which he might wish to belong, it is now an ecosystem ambivalent about his continued prominence. I saw the Vitalik Effect firsthand recently at Devcon, the annual Ethereum developer conference that took place in Prague this year. On the first day, a group of attendees spotted Buterin, who was scheduled to give a [keynote address](#) the following morning, standing nearby—unprotected, as it were. They began wondering aloud why more people weren’t approaching him, as though Ethereum’s creator were a rock star who should be mobbed by groupies.

“It’s easy to overestimate the extent to which everyone thinks the way that you do.”

“Maybe they’re respecting his space,” one mused.

“No,” said another, “I think it’s because they’re afraid.”

They clearly yearned to go over and introduce themselves, but were at a loss for how they might hold Buterin’s interest. “What would we say to him? We’re application layer [devs]! ‘Thanks for your protocol, we really like it, we think it’s great’?”

They had reached an impasse. But one developer was working up the nerve. “If you dare me,” he said, “I’ll go up and talk to him.”

“I don’t want to dare you,” his friend replied.

In the end, a few of them did troop over and say hi, but only one member of the group had the guts—or the temerity—to

shake Buterin's hand.

That is more than I manage. When I meet Buterin, shortly after his keynote, his hands are full—a mobile phone, a mug of tea—and so he can extend only a single long finger, E.T.-like, by way of greeting. He is tall and almost shockingly lean, and while we talk he sits slightly hunched, often looking down while he ponders a question. When he does lift his gaze to meet mine, his blue eyes radiate warmth; once you have earned his eye contact you want to earn it again. He toys absently with the string of his tea bag while he speaks. Our brief conversation moves from his efforts to reduce his own importance in the Ethereum ecosystem to the leadership mistake he shares with Donald Trump.



People have called you a philosopher-king—and a while back, when there was a hoax that you'd died, the price of ether plummeted. Are you troubled by the community's continued reliance on you?

If the community does continue to rely on me, then I think that would definitely be a problem. The whole point of decentralization is that you can make a system where you don't need to know which specific people are involved in it

and that they're trustworthy in order to be able to participate in it. So if the *de facto* assumption for Ethereum's continued existence is that I do certain specific things, then that's a big risk to anyone in the Ethereum ecosystem—and obviously a large loss of freedom for myself.

At the same time, though, the extent to which I am a critical node in some sense is definitely much lower than it was a year ago. If you look even at some of the Twitter responses from yesterday, people were talking about how it's kind of clear that the community is relying on each other much more. That's something that we have been very deliberately working toward for the last year. So even something like, for example, the Ethereum Foundation's grant program, and [also] how we went with this multi-client approach to implementing Serenity and sharding. One of the goals there was to make it so that the work isn't just concentrated in a small group of people. You have all these different teams in different places all over the world trying to keep building.

The head of the Python team at the Ethereum Foundation talked today about “onboarding the next one million developers.” Is that the strategy to reduce your prominence—not to shrink your own role but just to bring more and more people on?

Bringing more and more people on is definitely the biggest part of it. If you bring more and more people on, it's hard to retain the same level of prominence unless you're in a position where you're actively managing all of them.

What would be the timeline for that? After Ethereum 2.0, [Serenity](#), is implemented?

It's just something that's going to naturally happen over time.

The slide you showed of the Hindenburg disaster to illustrate the [DAO hack](#) was funny. And it made me think about how you led the effort to slow down the attacker

and roll back the effects of his actions. Aren't there some advantages to being what Satoshi once was for bitcoin and what Linus Torvalds has been for Linux—"Benevolent Dictator for Life"?

There definitely are. It is a good thing for a development community to be smaller and more concentrated especially in the earlier stages, where there are lots of decisions to make. Designing big protocols by large committee is something that just doesn't work. But when the system stabilizes and we're talking less about huge fundamental revamps and more about ongoing marginal tweaks, then I think that's the point where the [decentralized] model starts both working more and making more sense as the right way to do it.

"Designing big protocols by large committee is something that just doesn't work."

One of the earliest ideas with blockchain was that it means you don't have to trust people; you can just trust math. Maybe that was true for bitcoin early on, but when it comes to things like [super-quadratic sharding](#), cross-shard transactions, SNARKs, and so on—for those who can't read code or verify the validity of these concepts, are they not forced once more to accept the decisions and judgements of a sort of priestly class?

There's definitely a balance there. Even in bitcoin, for example, [the cryptographic hash function] [SHA-256](#)—you might think of it as one thing, because it's one word and you never peek into the blocks. But really it's an insanely complicated thing with a pedigree of decades of academic research that just completely destroyed the security of a whole bunch of alternatives. On the other hand, this is part of the reason why I'm not a big fan of super-quadratic sharding at this point. We're just doing quadratic sharding. I do feel that [implementing the proof-of-stake system] Casper

is necessary to give Ethereum its higher level of security and efficiency; sharding is necessary to bring it up to the level of scalability that we need. But you do have to be very hawkish about protocol simplicity. And there are areas where I'm trying hard to come up with ways to push the protocol's complexity down.

One example is that there's this Merkle-tree structure in the current Ethereum chain, and it's this fairly complicated thing—basically it's a way of storing the data about all of the accounts in the system. I've been thinking a lot about how to cut the complexity of that by maybe a factor of five. But we'll see. Reducing the number of lines of code that you need to worry about is important.



Are there any other considerations?

There's also conceptual simplicity. But even there you have to think a bit more carefully. Because, for example, the bitcoin protocol seems simple, but the analysis in many ways is not simple. For example, people thought [from 2009 to 2013] that the bitcoin security [threshold] was 50 percent. But then Emin Gün Sirer and Ittay Eyal wrote the "[selfish mining](#)" paper and, oh, my God, now it's between zero and 33 percent, depending on your assumptions about the network, and here's a patch that the bitcoin core devs never implemented that will make it 25 percent. [Editor's note: In their 2013 paper, Sirer and Eyal proposed a fix to the

bitcoin protocol that was intended to raise the network's security threshold — the amount of total computational power in the network one would have to control in order to double-spend bitcoins or obtain more than one's fair share of mining rewards — to 25 percent.] So now you have to [consider] your attitudes about the possibility of collusion in the mining network, and your opinions about how the peer-to-peer network works, and a bunch of other things. Whereas [Ethereum's] proof-of-stake algorithm, we've definitely put more work into it. And in some respects the analysis [of its security] will be simpler. There's also just a much larger community that's doing the analysis.

"At some point I realized that you can't resolve all conflicts by just getting the two people to sit down and have a conversation with each other and hug each other."

So it's a little easier to trust because it's not just five people telling you to take it on faith or something?

Yeah, yeah. I definitely keep an eye out for solutions that seem like [they require] taking five people on faith, and I try hard to avoid them.

The fifth anniversary of your Ethereum white paper is coming up in November. Your father [recently said](#) that you were "innocent and unprepared" when you co-founded Ethereum and that you "had to learn a lot of tough lessons about people." What's the hardest lesson you've had to learn?

One is that it's easy to overestimate the extent to which everyone thinks the way that you do. Back in 2014 I thought, at least, that I was in the space because I believed in decentralization, believed in making open, public things for the world, believed in censorship-resistant mutual platforms, and all of that. There were a bunch of debates which had to do with the fact that the other people on the [Ethereum]

team just basically wanted to make a huge pile of money. Not all of them, but some. At some point I realized that you can't resolve all conflicts by just getting the two people to sit down and have a conversation with each other and hug each other. That resolves it for one hour, but then they go back to their rooms, and if the underlying issues aren't addressed then it's not changed.

You learned that dialogue has a place, but it can't solve everything?

Yeah, exactly. The other big one is that a lot of people were nice to me, and I thought they were nice to me because they were nice, but really they were nice to me because they perceived I was powerful. One of the mistakes I made as a leader at that time is, actually, the same mistake I noticed Donald Trump making a while ago. If you remember the time when he was really in favor of blowing up Obamacare, and then Barack came over the White House, they talked for one and a half hours, and then right after that, Trump said, "Oh, my God, I never believed healthcare could be so complicated." But then, of course, after that he wasn't particularly [in favor of] trying to stop blowing up Obamacare. The trait that I think about here is: agreeing with the last person you talked to. It's actually very easy to do that if you don't have experience. It did take me about a year or so to figure out how to move past that.

This interview has been edited for length and clarity.

Main image [Trevor Jones](#).

Name of Core

CARMINE PILL

Political Breakdown

UTOPIANIST, ARTISTS, CRITICAL ENGAGEMENT, EXPERIMENTAL
DADA, ALWAYS BOTH

Common Beliefs

CRITICAL OPTIMISM. THE REVOLUTION IS NOT AN APPLE
THAT FALLS WHEN ITS RIPE..YOU HAVE TO MAKE IT

Social Constructs

TRIAL AND ERROR, AESTHETICS AS ASSETS, ROAMING PARTY
LINES, INFORM TO DEFORM, PASSIONATELY ENGAGED

Coders

GLEN WEYL, RUTH CATLOW, BEN VICKERS, JONAS LUND,
ZTOHOVEN

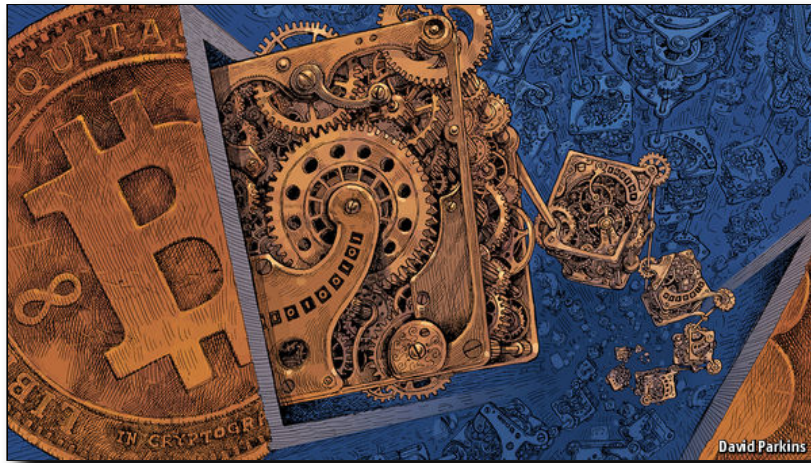
Coin

MONERO, ETHEREUM, JLT, HOLO, AUGUR, GOLEM,
DOGECOIN, CRYPTOKITTIES

BLOCKCHAINS - THE GREAT CHAIN OF BEING SURE ABOUT THINGS

■ economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the cryptocurrency



PRINT EDITION | BRIEFING

Oct 31st 2015

WHEN the Honduran police came to evict her in 2009 Mariana Catalina Izaguirre had lived in her lowly house for three decades. Unlike many of her neighbours in Tegucigalpa, the country's capital, she even had an official title to the land on which it stood. But the records at the country's Property Institute showed another person registered as its owner, too—and that person convinced a judge to sign an eviction order. By the time the legal confusion was finally sorted out, Ms Izaguirre's house had been demolished.

It is the sort of thing that happens every day in places where land registries are badly kept, mismanaged and/or corrupt—which is to say across much of the world. This lack of secure property rights is an endemic source of insecurity and injustice. It also makes it harder to use a house or a piece of land as collateral, stymying investment and job creation.

Such problems seem worlds away from bitcoin, a currency based on clever cryptography which has a devoted following among mostly well-off, often anti-government and sometimes criminal geeks. But the cryptographic technology that underlies bitcoin, called the “blockchain”, has applications well beyond cash and currency. It offers a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned. It is a way of making and preserving truths.

That is why politicians seeking to clean up the Property Institute in Honduras have asked Factom, an American startup, to provide a prototype of a blockchain-based land registry. Interest in the idea has also been expressed in Greece, which has no proper land registry and where only 7% of the territory is adequately mapped.

A PLACE IN THE PAST

Other applications for blockchain and similar “distributed ledgers” range from thwarting diamond thieves to streamlining stockmarkets: the NASDAQ exchange will soon start using a blockchain-based system to record trades in privately held companies. The Bank of England, not known for technological flights of fancy, seems electrified: distributed ledgers, it concluded in a research note late last year, are a “significant innovation” that could have “far-reaching implications” in the financial industry.

The politically minded see the blockchain reaching further than that. When co-operatives and left-wingers gathered for

this year's OuiShare Fest in Paris to discuss ways that grass-roots organisations could undermine giant repositories of data like Facebook, the blockchain made it into almost every speech. Libertarians dream of a world where more and more state regulations are replaced with private contracts between individuals—contracts which blockchain-based programming would make self-enforcing.

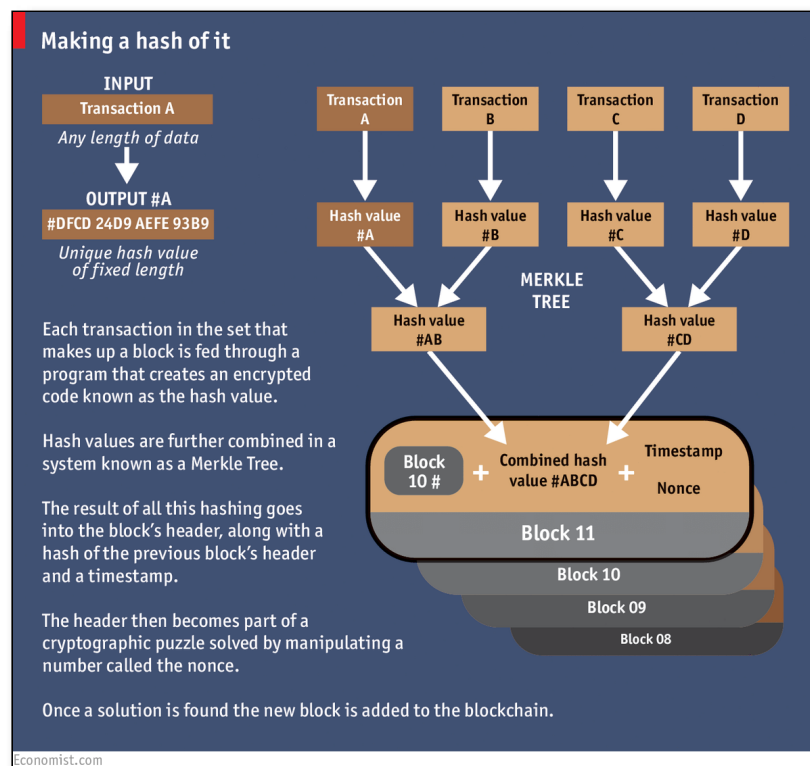
The blockchain began life in the mind of Satoshi Nakamoto, the brilliant, pseudonymous and so far unidentified creator of bitcoin—a “purely peer-to-peer version of electronic cash”, as he put it in a paper published in 2008. To work as cash, bitcoin had to be able to change hands without being diverted into the wrong account and to be incapable of being spent twice by the same person. To fulfil Mr Nakamoto's dream of a decentralised system the avoidance of such abuses had to be achieved without recourse to any trusted third party, such as the banks which stand behind conventional payment systems.

It is the blockchain that replaces this trusted third party. A database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers—bitcoin's “nodes”—around the world and is publicly available. But for all its openness it is also trustworthy and secure. This is guaranteed by the mixture of mathematical subtlety and computational brute force built into its “consensus mechanism”—the process by which the nodes agree on how to update the blockchain in the light of bitcoin transfers from one person to another.

Let us say that Alice wants to pay Bob for services rendered. Both have bitcoin “wallets”—software which accesses the blockchain rather as a browser accesses the web, but does not identify the user to the system. The transaction starts with Alice's wallet proposing that the blockchain be changed

so as to show Alice's wallet a little emptier and Bob's a little fuller.

The network goes through a number of steps to confirm this change. As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether Alice actually has the bitcoin she now wants to spend. If everything looks kosher, specialised nodes called miners will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain.



This entails repeatedly feeding the data through a cryptographic “hash” function which boils the block down into a string of digits of a given length (see diagram). Like a lot of cryptography, this hashing is a one-way street. It is easy to go from the data to their hash; impossible to go from the hash back to the data. But though the hash does not contain the data, it is still unique to them. Change what goes into the block in any way—alter a transaction by a single digit—and the hash would be different.

RUNNING IN THE SHADOWS

That hash is put, along with some other data, into the header of the proposed block. This header then becomes the basis for an exacting mathematical puzzle which involves using the hash function yet again. This puzzle can only be solved by trial and error. Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that's the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. The hash of the header becomes the new block's identifying string, and that block is now part of the ledger. Alice's payment to Bob, and all the other transactions the block contains, are confirmed.

This puzzle stage introduces three things that add hugely to bitcoin's security. One is chance. You cannot predict which miner will solve a puzzle, and so you cannot predict who will get to update the blockchain at any given time, except in so far as it has to be one of the hard working miners, not some random interloper. This makes cheating hard.

The second addition is history. Each new header contains a hash of the previous block's header, which in turn contains a hash of the header before that, and so on and so on all the way back to the beginning. It is this concatenation that makes the blocks into a chain. Starting from all the data in the ledger it is trivial to reproduce the header for the latest block. Make a change anywhere, though—even back in one of the earliest blocks—and that changed block's header will come out different. This means that so will the next block's, and all the subsequent ones. The ledger will no longer match the latest block's identifier, and will be rejected.

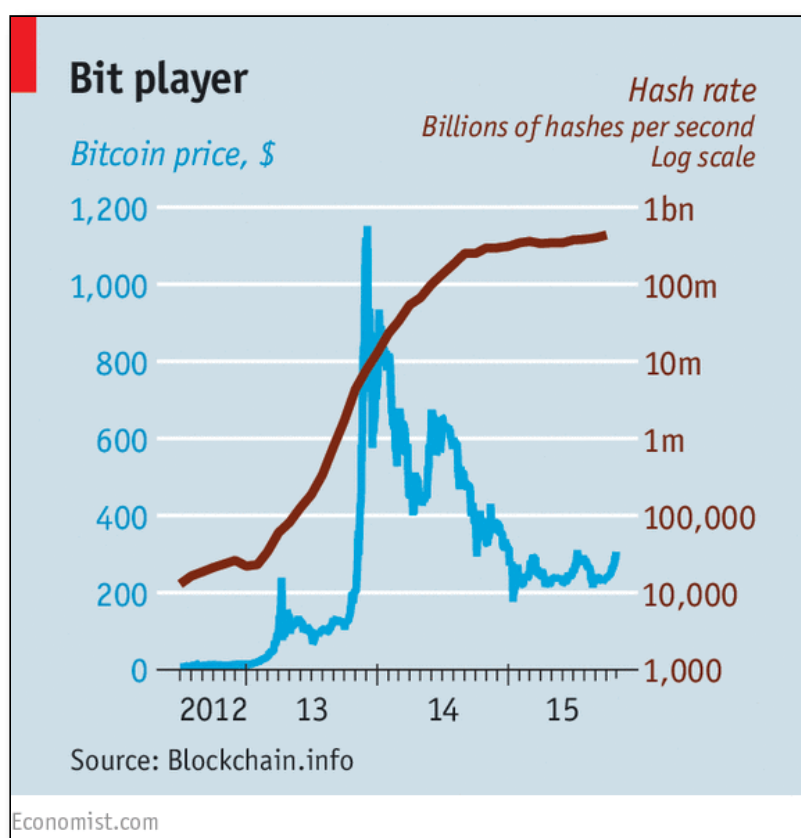
Is there a way round this? Imagine that Alice changes her mind about paying Bob and tries to rewrite history so that her bitcoin stays in her wallet. If she were a competent miner she could solve the requisite puzzle and produce a new

version of the blockchain. But in the time it took her to do so, the rest of the network would have lengthened the original blockchain. And nodes always work on the longest version of the blockchain there is. This rule stops the occasions when two miners find the solution almost simultaneously from causing anything more than a temporary fork in the chain. It also stops cheating. To force the system to accept her new version Alice would need to lengthen it faster than the rest of the system was lengthening the original. Short of controlling more than half the computers—known in the jargon as a “51% attack”—that should not be possible.

DREAMS ARE SOMETIMES CATCHING

Leaving aside the difficulties of trying to subvert the network, there is a deeper question: why bother to be part of it at all? Because the third thing the puzzle-solving step adds is an incentive. Forging a new block creates new bitcoin. The winning miner earns 25 bitcoin, worth about \$7,500 at current prices.

All this cleverness does not, in itself, make bitcoin a particularly attractive currency. Its value is unstable and unpredictable (see chart), and the total amount in circulation is deliberately limited. But the blockchain mechanism works very well. According to blockchain.info, a website that tracks such things, on an average day more than 120,000 transactions are added to the blockchain, representing about \$75m exchanged. There are now 380,000 blocks; the ledger weighs in at nearly 45 gigabytes.



Most of the data in the blockchain are about bitcoin. But they do not have to be. Mr Nakamoto has built what geeks call an “open platform”—a distributed system the workings of which are open to examination and elaboration. The paragon of such platforms is the internet itself; other examples include operating systems like Android or Windows. Applications that depend on basic features of the blockchain can thus be developed without asking anybody for permission or paying anyone for the privilege. “The internet finally has a public data base,” says Chris Dixon of Andreessen Horowitz, a venture-capital firm which has financed several bitcoin start-ups, including Coinbase, which provides wallets, and 21, which makes bitcoin-mining hardware for the masses.

For now blockchain-based offerings fall in three buckets. The first takes advantage of the fact that any type of asset can be transferred using the blockchain. One of the startups betting on this idea is Colu. It has developed a mechanism to “dye” very small bitcoin transactions (called “bitcoin dust”)

by adding extra data to them so that they can represent bonds, shares or units of precious metals.

Protecting land titles is an example of the second bucket: applications that use the blockchain as a truth machine. Bitcoin transactions can be combined with snippets of additional information which then also become embedded in the ledger. It can thus be a registry of anything worth tracking closely. Everledger uses the blockchain to protect luxury goods; for example it will stick on to the blockchain data about a stone's distinguishing attributes, providing unchallengeable proof of its identity should it be stolen. Onename stores personal information in a way that is meant to do away with the need for passwords; CoinSpark acts as a notary. Note, though, that for these applications, unlike for pure bitcoin transactions, a certain amount of trust is required; you have to believe the intermediary will store the data accurately.

It is the third bucket that contains the most ambitious applications: "smart contracts" that execute themselves automatically under the right circumstances. Bitcoin can be "programmed" so that it only becomes available under certain conditions. One use of this ability is to defer the payment miners get for solving a puzzle until 99 more blocks have been added—which provides another incentive to keep the blockchain in good shape.

Lighthouse, a project started by Mike Hearn, one of bitcoin's leading programmers, is a decentralised crowdfunding service that uses these principles. If enough money is pledged to a project it all goes through; if the target is never reached, none does. Mr Hearn says his scheme will both be cheaper than non-bitcoin competitors and also more independent, as governments will be unable to pull the plug on a project they don't like.

ENERGY IS CONTAGIOUS

The advent of distributed ledgers opens up an “entirely new quadrant of possibilities”, in the words of Albert Wenger of USV, a New York venture firm that has invested in startups such as OpenBazaar, a middleman-free peer-to-peer marketplace. But for all that the blockchain is open and exciting, sceptics argue that its security may yet be fallible and its procedures may not scale. What works for bitcoin and a few niche applications may be unable to support thousands of different services with millions of users.

Though Mr Nakamoto’s subtle design has so far proved impregnable, academic researchers have identified tactics that might allow a sneaky and well financed miner to compromise the block chain without direct control of 51% of it. And getting control of an appreciable fraction of the network’s resources looks less unlikely than it used to. Once the purview of hobbyists, bitcoin mining is now dominated by large “pools”, in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap.

Another worry is the impact on the environment. With no other way to establish the bona fides of miners, the bitcoin architecture forces them to do a lot of hard computing; this “proof of work”, without which there can be no reward, insures that all concerned have skin in the game. But it adds up to a lot of otherwise pointless computing. According to blockchain.info the network’s miners are now trying 450 thousand trillion solutions per second. And every calculation takes energy.

Because miners keep details of their hardware secret, nobody really knows how much power the network consumes. If everyone were using the most efficient hardware, its annual electricity usage might be about two terawatt-hours—a bit more than the amount used by the 150,000 inhabitants of King’s County in California’s Central

Valley. Make really pessimistic assumptions about the miners' efficiency, though, and you can get the figure up to 40 terawatt-hours, almost two-thirds of what the 10m people in Los Angeles County get through. That surely overstates the problem; still, the more widely people use bitcoin, the worse the waste could get.

Yet for all this profligacy bitcoin remains limited. Because Mr Nakamoto decided to cap the size of a block at one megabyte, or about 1,400 transactions, it can handle only around seven transactions per second, compared to the 1,736 a second Visa handles in America. Blocks could be made bigger; but bigger blocks would take longer to propagate through the network, worsening the risks of forking.

Earlier platforms have surmounted similar problems. When millions went online after the invention of the web browser in the 1990s pundits predicted the internet would grind to a standstill: *eppur si muove*. Similarly, the bitcoin system is not standing still. Specialised mining computers can be very energy efficient, and less energy-hungry alternatives to the proof-of-work mechanism have been proposed. Developers are also working on an add-on called "Lightning" which would handle large numbers of smaller transactions outside the blockchain. Faster connections will let bigger blocks propagate as quickly as small ones used to.

The problem is not so much a lack of fixes. It is that the network's "bitcoin improvement process" makes it hard to choose one. Change requires community-wide agreement, and these are not people to whom consensus comes easily. Consider the civil war being waged over the size of blocks. One camp frets that quickly increasing the block size will lead to further concentration in the mining industry and turn bitcoin into more of a conventional payment processor. The other side argues that the system could crash as early as next year if nothing is done, with transactions taking hours.

A BREAK IN THE BATTLE

Mr Hearn and Gavin Andresen, another bitcoin grandee, are leaders of the big-block camp. They have called on mining firms to install a new version of bitcoin which supports a much bigger block size. Some miners who do, though, appear to be suffering cyber-attacks. And in what seems a concerted effort to show the need for, or the dangers of, such an upgrade, the system is being driven to its limits by vast numbers of tiny transactions.

This has all given new momentum to efforts to build an alternative to the bitcoin blockchain, one that might be optimised for the storing of distributed ledgers rather than for the running of a cryptocurrency. MultiChain, a build-your-own-blockchain platform offered by Coin Sciences, another startup, demonstrates what is possible. As well as offering the wherewithal to build a public blockchain like bitcoin's, it can also be used to build private chains open only to vetted users. If all the users start off trusted the need for mining and proof-of-work is reduced or eliminated, and a currency attached to the ledger becomes an optional extra.

The first industry to adopt such sons of blockchain may well be the one whose failings originally inspired Mr Nakamoto: finance. In recent months there has been a rush of bankerly enthusiasm for private blockchains as a way of keeping tamper-proof ledgers. One of the reasons, irony of ironies, is that this technology born of anti-government libertarianism could make it easier for the banks to comply with regulatory requirements on knowing their customers and anti-money-laundering rules. But there is a deeper appeal.

Industrial historians point out that new powers often become available long before the processes that best use them are developed. When electric motors were first developed they were deployed like the big hulking steam engines that came before them. It took decades for manufacturers to see that lots of decentralised electric motors could reorganise every

aspect of the way they made things. In its report on digital currencies, the Bank of England sees something similar afoot in the financial sector. Thanks to cheap computing financial firms have digitised their inner workings; but they have not yet changed their organisations to match. Payment systems are mostly still centralised: transfers are cleared through the central bank. When financial firms do business with each other, the hard work of synchronising their internal ledgers can take several days, which ties up capital and increases risk.

Distributed ledgers that settle transactions in minutes or seconds could go a long way to solving such problems and fulfilling the greater promise of digitised banking. They could also save banks a lot of money: according to Santander, a bank, by 2022 such ledgers could cut the industry's bills by up to \$20 billion a year. Vendors still need to prove that they could deal with the far-higher-than-bitcoin transaction rates that would be involved; but big banks are already pushing for standards to shape the emerging technology. One of them, UBS, has proposed the creation of a standard "settlement coin". The first order of business for R3 CEV, a blockchain startup in which UBS has invested alongside Goldman Sachs, JPMorgan and 22 other banks, is to develop a standardised architecture for private ledgers.

The banks' problems are not unique. All sorts of companies and public bodies suffer from hard-to-maintain and often incompatible databases and the high transaction costs of getting them to talk to each other. This is the problem Ethereum, arguably the most ambitious distributed-ledger project, wants to solve. The brainchild of Vitalik Buterin, a 21-year-old Canadian programming prodigy, Ethereum's distributed ledger can deal with more data than bitcoin's can. And it comes with a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their

owners dividends if profits reach a certain level. Such cleverness, Mr Buterin hopes, will allow the formation of “decentralised autonomous organisations”—virtual companies that are basically just sets of rules running on Ethereum’s blockchain.



One of the areas where such ideas could have radical effects is in the “internet of things”—a network of billions of previously mute everyday objects such as fridges, doorstops and lawn sprinklers. A recent report from IBM entitled “Device Democracy” argues that it would be impossible to keep track of and manage these billions of devices centrally, and unwise to try; such attempts would make them vulnerable to hacking attacks and government surveillance. Distributed registers seem a good alternative.

The sort of programmability Ethereum offers does not just allow people’s property to be tracked and registered. It allows it to be used in new sorts of ways. Thus a car-key embedded in the Ethereum blockchain could be sold or rented out in all manner of rule-based ways, enabling new peer-to-peer schemes for renting or sharing cars. Further out, some talk of using the technology to make by-then-self-driving cars self-owning, to boot. Such vehicles could stash away some of the digital money they make from renting out their keys to pay for fuel, repairs and parking spaces, all according to preprogrammed rules.

WHAT WOULD ROUSSEAU HAVE SAID?

Unsurprisingly, some think such schemes overly ambitious. Ethereum's first ("genesis") block was only mined in August and, though there is a little ecosystem of start-ups clustered around it, Mr Buterin admitted in a recent blog post that it is somewhat short of cash. But the details of which particular blockchains end up flourishing matter much less than the broad enthusiasm for distributed ledgers that is leading both start-ups and giant incumbents to examine their potential. Despite society's inexhaustible ability to laugh at accountants, the workings of ledgers really do matter.

Today's world is deeply dependent on double-entry book-keeping. Its standardised system of recording debits and credits is central to any attempt to understand a company's financial position. Whether modern capitalism absolutely required such book-keeping in order to develop, as Werner Sombart, a German sociologist, claimed in the early 20th century, is open to question. Though the system began among the merchants of renaissance Italy, which offers an interesting coincidence of timing, it spread round the world much more slowly than capitalism did, becoming widely used only in the late 19th century. But there is no question that the technique is of fundamental importance not just as a record of what a company does, but as a way of defining what one can be.

Ledgers that no longer need to be maintained by a company—or a government—may in time spur new changes in how companies and governments work, in what is expected of them and in what can be done without them. A realisation that systems without centralised record-keeping can be just as trustworthy as those that have them may bring radical change.

Such ideas can expect some eye-rolling—blockchains are still a novelty applicable only in a few niches, and the doubts as to how far they can spread and scale up may prove well

founded. They can also expect resistance. Some of bitcoin's critics have always seen it as the latest techy attempt to spread a "Californian ideology" which promises salvation through technology-induced decentralisation while ignoring and obfuscating the realities of power—and happily concentrating vast wealth in the hands of an elite. The idea of making trust a matter of coding, rather than of democratic politics, legitimacy and accountability, is not necessarily an appealing or empowering one.

At the same time, a world with record-keeping mathematically immune to manipulation would have many benefits. Evicted Ms Izaguirre would be better off; so would many others in many other settings. If blockchains have a fundamental paradox, it is this: by offering a way of setting the past and present in cryptographic stone, they could make the future a very different place.

IF YOU DON'T HAVE BREAD, EAT ART!: CONTEMPORARY ART AND DERIVATIVE FASCISMS

e-flux.com/journal/76/69732/if-you-don-t-have-bread-eat-art-contemporary-art-and-derivative-fascisms/

JOURNAL #76 - OCTOBER 2016

HITO STEYERL



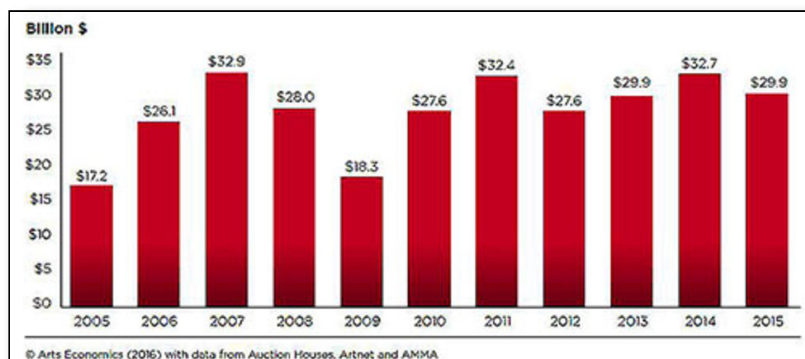
Christie's auctioneers vend a Mark Rothko painting.

Is art a currency? Investor Stefan Simchowicz thinks so. He wrote with uncompromising clarity about the post-Brexit era: "Art will effectively continue its structural function as an alternative currency that hedges against inflation and currency depreciation." 1 Have silver paintings become a proxy gold standard? 2 How did it come to this? During the ongoing crisis, investors were showered with tax money,

which then went into freeport collections, tower mansions, and shell companies. Quantitative easing eroded currency stability and depleted common resources, entrenching a precarious service economy with dismal wages, if any, eternal gigs, eternal debt, permanent doubt, and now increasing violence. This destabilization is one reason the value of art looks more stable than the prospects of many national GDPs. In the EU this takes place against a backdrop of mass evictions, austerity, arson attacks, Daesh run amok, and Deutsche scams. Results include child poverty, debt blackmail, rigged economies, and the fascist scapegoating of others for widely self-inflicted failed policies. Art is an “alternative currency” of this historical moment. 3 It seems to trade against a lot of misery.

Meanwhile, reactionary extremism intensifies in many places. I won’t bore you with specifics. There’s always another attack, election, coup, or someone who ups the ante in terms of violence, misogyny, snuff, or infamy. Derivative fascisms 4 continue to grow, wherever disenfranchised middle classes fear (and face) global competition—and choose to both punch down and suck up to reactionary oligarchies. 5 Ever more self-tribalized formations pop up that prefer not to abolish neoliberal competition—but instead eliminate competitors personally. Derivative fascisms try to fuse all-out free trade economics with (for example) white nationalism [6] by promoting survival of the fittest for everyone except themselves. Authoritarian neoliberalism segues into just authoritarianism.

A permanent fog of war is fanned by permanent fakes on Facebook. Already deregulated ideas of truth are destabilized even further. Emergency rules. Critique is a troll fest. Crisis commodified as entertainment. The age of neoliberal globalization seems exhausted and a period of contraction, fragmentation, and autocratic rule has set in.



The growth of the global auction market from 2005 to 2015, according to data from Auction House, ArtNet, and AMMA.

ALTERNATIVE CURRENCY

Art markets seem not overly concerned. In times in which financial institutions and even whole political entities may just dissolve into fluffy glitter, investment in art seems somehow more real. Moreover, as alternative currency, art seems to fulfill what Ethereum and Bitcoin have hitherto only promised. 6 Rather than money issued by a nation and administrated by central banks, art is a networked, decentralized, widespread system of value. 7 It gains stability because it calibrates credit or disgrace across competing institutions or cliques. There are markets, collectors, museums, publications, and the academy asynchronously registering (or mostly failing to do so) exhibitions, scandals, likes and prices. As with cryptocurrencies, there is no central institution to guarantee value; instead there is a jumble of sponsors, censors, bloggers, developers, producers, hipsters, handlers, patrons, privateers, collectors, and way more confusing characters. Value arises from gossip- *cum* -spin and insider information. Fraudsters and con artists mix helter-skelter with pontificating professors, anxious gallerists, and couch-surfing students. This informal ecology is eminently hackable, but since everyone does it, it sometimes evens out—even though at highly manipulated levels. It is at once highly malleable and inert, sublime, dopey, opaque, bizarre, and blatant: a game in which the most transcendental

phenomena are on collectors' waiting lists. Further down the food chain, media art, like Bitcoin, tries to manage the contradictions of digital scarcity by limiting the illimitable. But for all its pretense to technological infallibility, Bitcoin is potentially just as dependent on group power as art-market values are dependent on consent, collusion, and coincidence. What looks like incorruptible tech in practice hinges on people's actions. As to the encryption part in art: art is often encrypted to the point of sometimes being undecryptable. Encryption is routinely applied, even or especially if there is no meaning whatsoever. Art is encryption as such, regardless of the existence of a message with a multitude of conflicting and often useless keys. 9 Its reputational economy is randomly quantified, ranked by bullshit algorithms that convert artists and academics into ranked positions, but it also includes more traditionally clannish social hierarchies. It is a fully ridiculous, crooked, and toothless congregation and yet, like civilization as a whole, art would be a great idea.

In practice though, art industries trigger trickle-up effects which are then flushed sideways into tax havens. Art's economies divert investments from sustainable job creation, education, and research and externalize social cost and risk. They bleach neighborhoods, underpay, overrate, and peddle excruciating baloney.

This does not only apply to art's investor and manager classes. The lifestyles of many art workers also support a corporate technological (and antisocial) infrastructure that whisks off profits into fiscal banana republics. Apple, Google, Uber, Airbnb, Ryanair, Facebook, and other hipster providers pay hardly any taxes in Ireland, Jersey, or other semisecret jurisdictions. They don't contribute to local services like schools or hospitals and their idea of sharing is to make sure they get their share.

But let's face it—in relation to the scale of other industries, the art sector is just a blip. Contemporary art is just a hash for all that's opaque, unintelligible, and unfair, for top-down class war and all-out inequality. It's the tip of an iceberg acting as a spear.



"The online art market has continued to grow strongly (up 24 percent to \$3.27 billion) despite the global art market slowing in 2015," states the foreword of this art insurer's report.

DEGENERATE ART

Predictably, this leads to resentment and outright anger. Art is increasingly labeled as a decadent, rootless, out-of-touch, cosmopolitan urban elite activity. In one sense, this is a perfectly honest and partly pertinent description. 10

Contemporary art belongs to a time in which everything goes and nothing goes anywhere, a time of stagnant escalation, of serial novelty as deadlock. Many are itching for major changes, some because the system is pointless, harmful, 1 percent-ish, and exclusive, and many more because they finally want in.

On the other hand, talk of “rootless cosmopolitans” is clearly reminiscent of both Nazi and Stalinist propaganda, who relished in branding dissenting intellectuals as “parasites” within “healthy national bodies.” In both regimes this kind of jargon was used to get rid of minority intelligentsia, formal experiments and progressive agendas; not to improve access for locals or improve or broaden the appeal of art. The “anti-elitist” discourse in culture is at present mainly deployed by conservative elites, who hope to deflect attention from their own economic privileges by relaunching of stereotypes of “degenerate art.”

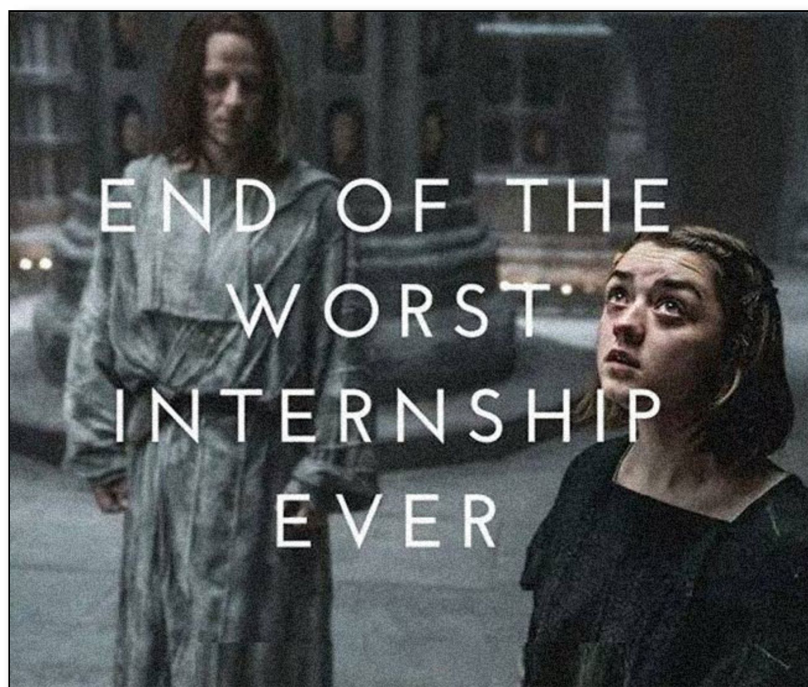
So if you are hoping for new opportunities with the authoritarians, you might find yourself disappointed.

Authoritarian right-wing regimes will not get rid of art-fair VIP lists or make art more relevant or accessible to different groups of people. In no way will they abolish elites or even art. They will only accelerate inequalities, beyond the fiscal-material to the existential-material. This transformation is not about accountability, criteria, access, or transparency. It will not prevent tax fraud, doctored markets, the Daesh antiquities trade, or systemic underpay. It will be more of the same, just much worse: less pay for workers, less exchange, fewer perspectives, less circulation, and even less regulation, if such a thing is even possible. Inconvenient art will fly out the window—anything non-flat, non-huge, or remotely complex or challenging. Intellectual perspectives, expanded canons, nontraditional histories will be axed—anything that requires an investment of time and effort instead of conspicuous money. Public support swapped for

Instagram metrics. Art fully floated on some kind of Arsedaq. More fairs, longer yachts for more violent assholes, oil paintings of booty blondes, abstract stock-chart calligraphy. Yummy organic superfoods. Accelerationist designer breeding. Personalized one-on-one performances for tax evaders. Male masters, more male masters, and repeat. Art will take its place next to big-game hunting, armed paragliding, and adventure slumming.

Yay for expensive craft and anything vacuous that works in a chain-hotel lobby. Plastiglomerate marble, welded by corporate characters banging on about natural selection. Kits for biological “self-improvement.” Crapstraction, algostraction, personalized installations incorporating Krav Maga lessons. Religious nailpaint will slay in all seasons, especially with a Louis Vuitton logo. Hedge-fund mandalas. Modest fashion. Immodest fashion. Nativist mumbo jumbo. Genetically engineered caviar in well-behaved ethnic pottery. Conceptual plastic surgery. Racial plastic surgery. Bespoke ivory gun handles. Murals on border walls. Good luck with this. You will be my mortal enemy.

Just like institutional critique was overtaken by a neoliberal Right that went ahead and simply abolished art institutions, the critique of contemporary art and claims for an exit from this paradigm are dwarfed by their reactionary counterparts. The reactionary exit—or acceleration of stagnation—is already well underway. Algorithmic and analogue market manipulation, alongside the defunding, dismantling, and hollowing-out of the public and post-public sector, 11 transforms what sometimes worked as a forum for shared ideas, judgment, and experimentation into HNWI interior design. Art will be firewalled within isolationist unlinked canons, which can easily be marketed as national, religious, and fully biased histories.



Game of Thrones lends itself to serving as a metaphor for fanstastic precarity.

AN ALTERNATIVE ALTERNATIVE CURRENCY?

Now what? Where does one go from here?

Let's put the next paragraph into brackets. It just indicates a hypothetical possibility.

If art is an alternative currency, its circulation also outlines an operational infrastructure. Could these structures be repossessed to work differently? How much value would the alternative currency of art lose if its most corrupt aspects were to be regulated or restructured to benefit art's larger communities? How about even a minimum of rules in the market—gallery contracts, resale-time minimums, artist fees, 12 remunerated internships? Introducing blockchain public records for the production, transaction, and locating of artworks in order to reign in tax fraud and money laundering? 13 Declining the most mortifying sponsor and patron relationships instead of artwashing fossil extraction, weapons manufacturing, and banks bailed out with former cultural funding? How about asking for fees on resales similar to those asked on photocopies to pay for art workers'

health insurance? Or on any offshore art-related transaction? Could art as alternative currency not only circulate within existing systems but even launch not-yet-existing economies (publics, institutions, markets, parallel art worlds, etc.)?

But to expect any kind of progressive transformation to happen by itself—just because the infrastructure or technology exists—would be like expecting the internet to create socialism or automation to evenly benefit all humankind. The internet spawned Uber and Amazon, not the Paris Commune. The results may be called “the sharing economy,” but this mostly means that the poor share with the rich, not vice versa. Should any less unilateral sharing be suggested, the bulk of capital will decamp immediately. 14 One of the first steps towards parallel art sectors would thus be to organize even partial sustainability in the absence of bubble liquidity and barely limited amounts of free labor. Whatever emerges will be a new version of art-affiliated autonomy

In contrast to the modernist autonomy of art schemes, this autonomy is not solitary, unlinked, or isolated. Nor will it come about by some fantasy of progress in-built into technology. On the contrary it can only emerge through both a conscious effort and exchange among diverse entities. It’s an autonomy that works through circulation, transformation, and alchemy. The links it could build on exist as weak links (aka, air-kiss links) and reshaping them would need to happen within a compromised mess of contradictory activities. But simultaneously people can try to synch with the art-related undercommons 15 by building partial networked autonomy via all means necessary. If art is a currency, can it be an undercurrent? Could it work like an Unter, not an Uber?

How to do this? People are used to perceiving the art world as sponsored by states, foundations, patrons, and

corporations. But the contrary applies at least equally well. Throughout history it has been artists and artworkers, more than any other actors, who have subsidized art production. 16 Most do so by concocting mixed-income schemes in which, simply speaking, some form of wage labor (or other income) funds art-making. But more generally, everyone involved also contributes in all sorts of other ways to art's circulation, thus making it stronger as currency. Even artists who live "off their work" subsidize the market by way of enormous commissions in relation to other industries. But why should one sponsor VIP prepreviews, bespoke museum extensions without any means to fill them, art-fair arms races, institutional franchises built under penal-colony conditions, and other baffling bubbles? This bloated, entitled, fully superfluous, embarrassing, and most of all politically toxic overhead is subsidized by means of free labor and life time, but also by paying attention to blingstraction and circulating its spinoffs, thus creating reach and legitimacy. Even the majority of artists that cannot afford saying no to any offer of income could save time not doing this. 17 Refusing sponsorship of this sort might be the first step towards shaking the unsustainable and mortifying dependency on speculative operations that indirectly increase authoritarian violence and division. Spend free time assisting colleagues, 18 not working for free for bank foundations. Don't "share" corporate crap on monopolist platforms. Ask yourself: Do you want global capitalism with a fascist face? Do you want to artwash more insane weather, insane leaders, poisonous and rising water, crumbling infrastructure, and brand-new walls? How can people genuinely share what they need? 19 How much speed is necessary? How can artistic (and art-related) autonomy evolve from haughty sovereignty to modest networked devolution? 20 How can platform cooperatives contribute to this? Can art institutions follow the lead of new municipalist networks and alliances of "rebel cities"? 21 In the face of

derivative fascisms, can local forms of life be reimagined beyond blood, soil, nation, and corporation, as networks of neighborhoods, publics, layered audiences? 22 Can art keep local imaginaries curious, open-minded, and spirited? How to make tangible the idea that belonging is in becoming—not in having been? 23 What is art's scale, perspective, and challenge in de-growing constituencies? Can one transform art's currency into art's confluence? Replace speculation with overflow? 24

Art's organizing role in the value-process—long overlooked, downplayed, worshipped, or fucked—is at last becoming clear enough to approach, if not rationally, than perhaps realistically. Art as alternative currency shows that art sectors already constitute a maze of overlapping systems in which good-old gossip, greed, lofty ideals, inebriation, and ruthless competition form countless networked cliques. The core of its value is generated less by transaction than by endless negotiation, via gossip, criticism, hearsay, haggling, heckling, peer reviews, small talk, and shade. The result is a solid tangle of feudal loyalties and glowing enmity, rejected love and fervent envy, pooling striving, longing, and vital energies. In short, the value is not in the product but in the network; not in gaming or predicting the market 25 but in creating exchange. 26 Most importantly, art is one of the few exchanges that derivative fascists don't control—yet.

But as a reserve system for dumb, mean, and greedy money, art's social value (auto)deconstructs and turns into a shell operation that ultimately just shields more empty shells and amplifies fragmentation and division. Similarly, arts venues are already shifting into bonded warehouses and overdesigned bank vaults inside gilded, gated compounds designed by seemingly the same three architects worldwide.

It's easy to imagine what the motto for art as the reserve currency of a fully rigged system might be. Just envision a posh PR lieutenant policing the entrance of a big art fair,

gingerly declaring to anyone pushed aside, displaced, exploited, and ignored: “If you don’t have bread, just eat art!”

×

Thank you to Sven Lütticken, Anton Vidokle, and Stephen Squibb for very helpful comments.

Hito Steyerl is a filmmaker and writer who lives in Berlin.

© 2016 e-flux and the author

RAVE CULTURE IS MAKING ITS MOVE ONTO THE BLOCKCHAIN

■ [wired.co.uk/article/rave-culture-on-the-blockchain](https://www.wired.co.uk/article/rave-culture-on-the-blockchain)

BEN VICKERS



Señor Salme

In one sense, the rave scene has always been encrypted. In its heyday, when news of illicit parties spread by word of mouth, you just needed to know the right people. But new technologies are adding another layer to this.

Throughout the last year, rumours of a crypto-enabled rave revival have been rife on the dark net and in closely guarded members-only forums, with some referring to these gatherings more publicly as crypto-raves, trustless raves or the "decentralised autonomous rave scene". This underground phenomenon has been driven by creative tech, in the form of the blockchain. Technologist and artist Mat Dryhurst has seen this first hand. "Like most good things, it emerged slowly and organically," he says. "The first time I went to a crypto rave, I got a text message from a friend who was given a few invites, received my own unique keys and was given an invite of my own to share."

The keys he's referring to can take different forms: PGP-signed messages stored on [public blockchains](#) ; or decentralised tokens distributed by DAOs (decentralised autonomous organisations), with each token representing a single ticket, in line with the recent explosion of ICOs and the tokenisation of everything that has come to the world of cryptocurrencies.

"One needs a number of 'block confirmations' to have passed to ensure access," explains Amnesia Scanner, a Berlin-based collective of designers and musicians who have been anonymously contracted to play at some of these decentralised autonomous raves. "Once you're in, you'll often be given access to a decentralised application that uses a hybrid of proof-of-stake and proof-of-work, that secures the scene," they say. Instead of peer-to-peer, it's friend-to-friend.

The blockchain is secure and anonymous and, by using it, party organisers can keep their identity hidden and automate usual organisational overheads, while ensuring that the event is open only to people that they trust.

"We know of gatherings broadcast on insecure networks such as Facebook being targeted by the police, or worse still, right-wing factions who are intent on doxing and harassing partygoers," Dryhurst says.

These events have undoubtedly been inspired by a growing worldwide interest in [cryptography and digital privacy](#) , but they have their roots in the concept of the "temporary autonomous zone", a term that was coined in an influential 1991 book of the same title by anarchist and arch-hermetist Hakim Bey, and which would go on to influence events such as Burning Man.

Because of their autonomous nature, there's no single type of music or scene represented at these events, although so far it's mostly been dance music such as techno and jungle. "The common element is an emphasis on privacy and

community that I think augments whatever music is being presented," Dryhurst says.

The blockchain isn't the only technology that is being experimented with at these events. Electronic duo Amnesia Scanner has witnessed AR and VR apps that employ hypnotic techniques to induce altered states that drug the user. The pair say that there are rumours about a German decentralised autonomous rave scene where participants ingest sleep medication and force themselves to stay awake.

The scene is growing in places such as the San Francisco Bay Area, Moscow and Berlin, but its greatest potential could be outside big cities, at the periphery of electronic music culture. The technology in use here could also unlock possibilities in music and wider culture more generally. "The magic of blockchains and smart contracts for me is the ability to encode ideology into the things that you create," says Dryhurst. "This could be groundbreaking for music as a medium. Rather than being limited to implying ideology through stylistic gestures and poetry, we are now able to execute ideology."

Establishing automated systems of trust through the blockchain could support an explosion in ad-hoc gatherings - not just raves, but theatre, live-action role-playing games, parties and protest movements, all equipped to evade oppression and stagnation.

A Quasi Proto Preface

What this book is about, what is inside, and why we did it

The blockchain is janus-faced. On one side its traits of transparency and decentralization promise much in terms of fairness and accountability, but on the other its monetary roots born as a financial payment system, albeit grounded in open-source software, mean its implementations are often stridently capitalistic. Furthermore, those involved in its development seem to oscillate between radical ethical standpoints and reductionist technological determinism. The blockchain engenders what has been called a ‘digital metalism’¹ with the ability, like a modern philosopher’s stone, to transmute life through a distributed ledger. That such a pecuniary minded technology is being touted as a new technology to underpin a newfangled internet, compels an exploration of both its current state and how it may be rethought.

A Performative Map

En masse, this whole collection operates as performative explainer of sorts, with the book containing multiple entry and exit points on the subject through which an understanding, unique to each reader, of both present incarnations and possible futures may emerge.

Jump to Ruth Catlow’s introduction for some essentials, and further technical elucidations within essays by Martín Nadal and César Escudero Andaluz, Rob Myers and Rachel O’Dwyer.

The book’s contributors represent the best of a transdisciplinary and enquiring spirit – required to understand and rethink the blockchain – and come from a wide variety of backgrounds, to kludge, critique and refunction their way through the terrain. We hope this inventive character makes what can be an obscure or off-putting field, which is principally controlled by developers and venture capitalists, a more live and open space.

Many works perform a quasi DIY dissection and montaging of the blockchain, acting as a subversive mapping of its individual parts, functions, and wider infrastructure. Such approaches respond to how this technology, if indeed it is to become a powerful tool of organizing

and mediating life, necessitates a need to make claims upon and intervene in it. Within the book, the diverse ecology of blockchains, smart contracts and cryptocurrency, are dynamically deployed and engaged with as new subjects of enquiry, new methods for organizing, and new mediums for art.

Finbook

Embodying this spirit, exploiting the blockchain as subject, method, and medium, we are excited to be able to include FinBook, which both enables an interactive experience of a proto-blockchain technology and intervenes within the book itself, linking articles to a financial trading portfolio. We encourage you to use the QR codes to access an online portal where you can rate the chapters in this book by assigning them value tokens. Additionally, FinBots operating inside the FinBook interface will themselves be assigning and trading these value tokens, in a speculative pastiche of the kinds of ways cultural value might combine with modes of financial trading under a blockchain-based cultural regime.

Art & the Blockchain Hybridity

It is interesting to note how FinBook and other artist projects within this book, which employ hybrid versions of blockchain technology or revel in its speculative unknowns, are representative of both the blockchain's nascent state and complexity, and the degree to which the blockchain is, or is not, being employed and translated more broadly. Many in the business world for example are adopting what might be called a blockchain-lite by opting for 'federated' and private incarnations, rather than its fully decentralized and transparent form, and favouring more and more the term Distributed Ledger Technology.² As Vitalik Buterin, founder of Ethereum, has stated: 'the concept of one blockchain to rule them all – a unique blockchain carrying a unique digital currency and used for all distributed-ledger applications – is obsolete'.³ But we should add – it's still early days.

In the course of editing the collection over the last year, we have observed the ebb and flow of the hype that surrounds the blockchain, and its struggle to implement more concrete manifestations. There continues to be huge disagreement and uncertainty regarding its future viability and adoption. In this environment, initiatives emerging from commons and open source communities such as Hyperledger⁴

and Dyne's Freecoin,⁵ create new territory in parallel (and compete ideologically and economically) with multi-billion dollar, massively global and 'closed' enterprises such as the Enterprise Ethereum Alliance of companies including JP Morgan and Microsoft.⁶ This wild west-style context is amplified by hackers, who are an unknown quantity with much to gain potentially by exploiting weaknesses in untested code, and the vulnerability (perhaps unsuitability) of current technical infrastructure. As @VladZamfir an active developer within the blockchain community tweeted at 4:40 AM – 4 Mar 2017: 'Ethereum isn't safe or scalable. It is immature experimental tech. Don't rely on it for mission critical apps unless absolutely necessary!' In the meantime, speculation is rife and this is reflected in many of the entries in this book. There is a curious equivalence between art's speculative abilities, to play with fact, fiction, and abstraction, and the blockchain's own chimeric character. Both art and the blockchain grapple with the instability of authorship and authenticity: where does agency lie, who is Satoshi? Inversely, it is intriguing to witness some in the blockchain fraternity rethinking their own character and narratives through an artistic lens. As @matthew_d_green tweeted at 10:40 PM, 13 Jul 2017, in reference to the latest potential Bitcoin fork: '...it seems like they are trapped in some horrible Sartre play where everyone has to use the word "decentralized" to mean different things.'

Perhaps he is referring to Sartre's play *No Exit*, known for the line, 'L'enfer, c'est les autres' translated as 'Hell is other people' or 'Hell is [the] others.' Which does perhaps offer some articulation of the blockchain's infernal infatuation with proof over trust. Or maybe he is referring to Sartre's *The Condemned of Altona*, which gives voice to his famous notion that 'Man is condemned to be free.' To which we might add, but only if cryptographically anonymized, traceable, and immutably codified. The blockchain does seem to be in a perpetual state of existential crisis. As @DMOberhaus wrote at 9:32 PM, 13 Jul 2017: 'An ICO (Ethereum Token) called 'FUCK' raised \$30k in 30 minutes because nothing matters anymore.' Or consider the transformation of Dogecoin from in-joke cryptocurrency to in-demand digital asset, with a capitalization of \$340 million in June 2017.⁷

The Book of the Block

What is clear throughout this book is that what the blockchain *is*, is very different to what it *means*, and this gap is only expanding as the

blockchain becomes perceptible to an ever wider group of people. Artists operate within this gap, sometimes drawing together technics and implications into coherent, perceptible objects, and sometimes extrapolating new speculative trajectories from the technical possibilities or suggestive ether of decentralized ledgers. The first half of this book includes documentation and discussion of a range of such interventions: from key speculative works such as Primavera De Filippi's *Plantoid*, and Paul Seidler, Paul Kolling and Max Hampshire's *Terra0*, to the more playful, perhaps even nostalgic, *Bittercoin* by Martín Nadal & César Escudero Andaluz. Also in this section the reader will find works by artists who have sought to document the world of meanings, possibilities and implementations in contemporary practices around the blockchain. These include visual-poetics such as Ami Clarke's text-based work, documentary formats including Peter Gomes' transcription, and Pablo Velasco's engagement with workshop discussions taking place at the Institute of Network Cultures, Amsterdam, and provocations such as *Satoshi Oath* by Jaya Klara Brekke and Elias Haase, PWR studio's development of their *Textblock* white paper, and work by Simon Denny presented here with an accompanying interview. The form of these presentations is deliberately diverse, and to a large degree dictated by the artists themselves. We hope that the reader will agree that the experiments with form throughout the book is appropriate to the system of ideas taking place across it.

In a following section, we are please to include a number of new creative works responding to the book as a site for experiencing what the blockchain means and how it feels. In the case of speculative fictions by Cecilia Wee, Rob Myers and artist collective Surfatial, potential future blockchain worlds can be glimpsed and are played out in variously terrifying and humorous ways. Poems by Theodoros Chiotis and Edward Picot respond to PWR's *Textblock* concept, and combine the theoretical implications of blockchain technology with the formal constraints and corruptions it implies. The blockchain appearing this way is not just a tool or structure for data to be stored, but also an affective presence – one that experimental literary practices are well placed to present in their concentrated forms. Illustration is another useful tool for envisaging feeling as form. The cover of this book features a newly commissioned illustration by Juhee Hahn that delineates the fine lines between cooperation, codification and control that the blockchain straddles.

The sequence of essays in the concluding theory section of the book begins with a fiery essay by Hito Steyerl, originally published in *e-flux journal*. In this essay, in effect diagnosing the conditions for art

production in the era that blockchains threaten to intervene, Steyerl articulates two of the major concerns of the book: art as currency and art as socio-political arena. Demonstrating how art's seemingly unshakable marketability is accompanied by an unsustainable crisis point in working conditions for artists.

Crisis points are of course the perfect moments to perceive the edges of any system. Blockchain technology's most notable crisis was the DAO hack of 17th June 2016, in which a highly effective attack was performed on the Ethereum blockchain, allowing for millions of dollars' worth of its investors' money to be syphoned off. As Ben Vickers documents in his essay, this crisis led to a fascinating split within the Ethereum communities, around the pragmatic requirement to intervene in a supposedly – ideologically – autonomous system, and the need to preserve this autonomy. Vickers' text allegorizes the Ethereum hack and resulting fork as an historical event, lived and responded to in real-time by people – investors and coders – with differing perspectives. The event is one in which the autonomy, collaborative and distributed ethos of the blockchain comes into conflict with one another and leads to radically unexpected events. The Ethereum hack is considered by Vickers to be of political and social importance akin to the beginnings of the Occupy movement, or the collapse of experiments with the first real-time predictive computer systems during the Chilean communist era – although the actual political allegiances at work in Ethereum are at best obscure.

Following Vickers' essay, and the conflict internal to Ethereum and other development communities, Rob Myers' develops a discussion of the political atmosphere surrounding the Blockchain's evolution. He engages specifically with the ideology of libertarians, anarcho-capitalists and syndico-anarchists who at various moments have been accused (or credited) with moulding and shaping blockchain technology to their interests. Myers' essay offers a granular survey of the link between perspectives on terms such as 'justice', 'agency' and 'truth', and how they play out in actual blockchain environments, blogs and chat-rooms. Myers' involvement in the often esoteric cultures of alt-currencies in particular lays the ground-work both for his own fiction *Bad Shibe*, included in this collection, and for other artists interested in the political aesthetics of blockchain implementation.

Max Dovey takes up the link between libertarianism and anti-statism in his examination of blockchain marriages. He observes that the ostensibly benign and personal act of declaring everlasting love and affiliation to your partner on the blockchain is better understood as a

highly charged symbolic act – as it explores and promotes the potential of blockchain to circumvent civic infrastructure. Dovey notes that the highest profile blockchain weddings have been performed by people with clear commercial investments in the blockchain. For Dovey, the rhetoric around the resurrection of the original (or ‘classic’) Ethereum after its forking, has interesting resonances with marriage, and the ‘proto-patriotism’ of some of its users.

Each of these essays, and in particular their reference to the Ethereum fork, will help to orient the reader in terms of the diversity of applications, ideological investment, and forms of socio-political rhetoric around the blockchain. Following this series of contributions, we are pleased to include a number of essays that directly address the ways in which blockchain technology is being, and may be used to inform conditions for the production and dissemination of art. Most frequently these essays engage with the way in which blockchain technology might accelerate, reify, or reverse the seismic transformations in working conditions, intellectual property, and sales, inaugurated by the ‘digital revolution’. Martin Zeilinger for example makes the point that the move towards ephemerality in digital environments was first made by conceptual artists in the 1960s. For Zeilinger, the ease with which conceptualism, originally a critique of art markets and institutions, was folded back into these apparatuses is cause for thought for blockchain enthusiasts.

Mark Waugh reports on the variety of projects DACS (Design and Artists Copyright Society) are involved in, exploring how blockchain technology might help to manage and document the ownership of art objects. Helen Kaplinsky offers a note of caution to these important and timely investigations. For Kaplinsky there is a historical dimension to this tension around the object – that of Colonialism and the museum. Citing a variety of notable contemporary blockchain projects which explore intellectual property and commercial rights – from the IP management tool Ascribe to Imogen Heap’s collaborative album project *Mycelium* – Kaplinsky notes that the decentralization and transparency of these forms of art ownership, although a move away from the often shadowy operations of centralized networks in online ‘Platform Capitalism’, threaten to replicate and further embed the self-disciplining nature of historical institutional control apparatuses such as the museum.

Like Kaplinsky, Rachel O’Dwyer traces different forms of digital editioning by organizations such as Ascribe, and alternative forms of payment and distribution experimented with by musicians – focusing

on what existing internet-based systems and platforms might suggest about future blockchain implementation. In a critique which has echoes of the conflict around Ethereum, O'Dwyer suggests that the purported decentralization and equality promised by blockchain technology will surely be as deeply indebted to administering organizations as internet-based ones, and the ideology of these organizations are rarely shared by the artists who might use them. O'Dwyer also argues that the blockchain is in fact a poor substitute for some internet and digital-based forms of data protection such as digital rights management.

In a substantively different form of enquiry, Bjørn Magnhildøen proposes that core concepts from phenomenology: 'being' and 'time', also have a different relation, and are in fact conflated, in the context of the blockchain. Magnhildøen, uses this observation to create a new category, of 'being@time', and calls for artworks that take place within it. Acting in a continuum, this suggests that after the dematerialization of the art object, via conceptual art, perhaps now we might, through the blockchain, deconceptualize the artwork. Embracing the inevitable anachronism and paradox of such a gesture, a (presently) active call for works for an exhibition responding to this situation can be found in his chapter.

Given the reputation of avant-garde music practitioners to embrace new technologies more quickly than other creative fields, it seems appropriate to end this collection with Holly Herndon and Mat Dryhurst. In an interview with Marc Garrett, the artists discuss how the distributed and, therefore, multiple and collaborative space of the blockchain lends itself to the kinds of ensemble practice that have grown in avant-garde music, design, and new media circles. Herndon and Dryhurst's is an optimistic and well informed position, which reflects on the positive forms of transformation that need to, and can, take place in the wake of digital-era changes in cultural production and distribution.

Blockchain Publishing, Language and Actors

Since our inception, Torque has been interested in the relationship between language, mind and technology, and in particular the self-reflexive and intra-active opportunities publishing on these themes offers. Our first books sought to gather leading thinkers in the areas of literature, media, art, neuroscience, and philosophy to explore what the contemporary conditions are for reading and writing;

often developing content through public forums such as gallery interventions, workshops and symposia. We consider the present volume to be an important addition to this sequence of publications and processes. For us, *Artists Re:Thinking the Blockchain* not only documents the fascinating range of practices and provocations around this almost mythical technology, but also offers at several points important observations around the challenges and opportunities facing publishers like ourselves and how we can relate to the public via new technologies.

As individuals involved in publishing we were initially intrigued by the potential for the blockchain to facilitate online micro payments (of say less than a pound) that traditionally have been too costly to flourish online, and which may offer new opportunities for funding special interest publications and generate new forms of interaction between readers and text. But in a return to the blockchain's janus-faced character the roll out of micropayments also has the potential to enable companies to charge for every micro gesture and activity online, from sending an email to search queries.⁸

As we encounter it though this book, the blockchain's technological rumblings affect the world way beyond markets and trade; for example, by influencing the language that people will have to adopt to work in this new medium. This was evident in the recent 'second biggest cryptocurrency hack ever'⁹, again orchestrated on the Ethereum chain, in July 2017, just as this introduction is being composed. Writing in the aftermath of this hack, software engineer Haseeb Qureshi noted that the language that Ethereum's 'smart contracts' are written in will need to be radically different from the existing languages that web developers are used to working with. Qureshi calls for a new language that has security built in.

Also, as Adam Greenfield has articulated, we need to be mindful of who the 'incumbent actors' are on this scene of new linguistic form and cryptographic code acts, who are directing its evolution.¹⁰ The assumptions that blockchain evangelists and technologists make about society, basing its functioning on property, contracts and markets, make what Greenfield describes as 'a market where there was none before' and often ignore qualities of the most powerful social movements, egalitarian organizations, and relationships, both human and non-human, that operate above and beyond this.¹¹ Greenfield writes: 'We want to believe in the possibilities of a technology that claims to give people powerful new tools for collective action, unsupervised by the state.' As always, we need to look and engage

way beyond the technosolution, and be mindful of the blockchain operating as ‘a solution looking for a problem.’¹²

Blockchain actors are deeply enmeshed in the conjuring and creation of a libertarian ‘sociotechnical imaginary’¹³ where a desire for abstraction and cutting out the middle man is often challenged by the grubby realities of life. Bitcoin for example is proving much more like other forms of money than perhaps those in its coterie like to admit. As Nigel Dodds writes, in practice: ‘the currency has generated a thriving community around its political ideals, relies on a high degree of social organization in order to be produced, has a discernible social structure, and is characterized by asymmetries of wealth and power that not dissimilar from the mainstream financial system. Unwittingly, then, Bitcoin serves as a powerful demonstration of the relational character of money.’¹⁴ This conflict between the dream and reality of the blockchain creates peculiar effects where ‘abstracting technologies remove themselves from the realm of action by configuring quasi-characters and quasi-events in a quasi-plot. Blockchain technology and monetary technologies that are built on it organize not so much humans and direct interactions between them, but rather quasi-characters and quasi-events.’¹⁵ This derivative abstraction necessitates a reductive ‘technological dependency’, where just as Greenfield suggests we want to believe in new tools, so those promoting the blockchain dream of a kind of hyper –bureaucracy,¹⁶ or Esperanto protocol, seeking to overcome the way that paperwork ‘makes everyone, no matter how powerful they may be in reality, feel so powerless.’¹⁷ Time will tell whether the blockchain simply replaces one type of bureaucracy and middle man, for another, and the degree to which it has to erode what counts as life in the process. After all, much that we value costs nothing, requires no documentation, incentive, or contract, and leaves little trace.

It is perhaps in the post-human space away from ‘the money’ that the blockchain and smart contracts have the most original things to offer: as a way get ‘outside ourselves’ and push beyond our own anthropocentric views and vested interests, as articulated deftly in *Terra0* the self governing forest, featured in this book. Here the otherness of technology and smart contracts, works with that of plant-based systems to form a more-than-human assemblage, treading a fascinating line between decolonizing nature and technosolutionism. Once more though, this hugely potent line of thought has to be tempered by an acknowledgement of lessons learned during the industrial and digital revolutions. The irony of *Terra0*, won’t be lost on the commentators who note that ‘proof-of-work’ currencies such

as Bitcoin exact a significant ecological price through their method of creating artificial scarcity.¹⁸ But then, even these calls must be weighed against convincing contemporary commentary actively calling for a more swift move towards cryptogovernance to stave off the worst environmental and social inequities of capitalism.¹⁹ We hope projects such as *Terra0* documented in this book will contribute to the ability and will of people to engage in these nascent but urgent conversations and modes of action.

Conclusion / Thanks

As well as being the third major interdisciplinary collection from Torque Editions, this book is the second in a sequence of publications produced by Furtherfield, following on from their notable 2010 book *Artist Re: Thinking Games* produced in collaboration with FACT. Ruth Catlow and Marc Garrett have a unique and vital approach to exploring the relations between technology and art production. This approach is deeply political while avoiding partisanship, and also deeply democratic, open, and with a clear ethical vision. We thank them for the range of artists and thinkers that they've gathered for this publication, to which we have added, and the generosity and good humour that has typified all our communications on what has been a long journey from conception to execution. We would also like to thank Mark Simmonds, the designer of this book, for his commitment to experimentation and attention to detail and Roger McKinley at FACT, Arts Council England and Culture Capital Exchange for funding support. To readers, we firstly thank those who supported our first Crowdfunder for this book around 18 months ago, who have been not only generous, but patient also, and of course all the artists and writers who have contributed and engaged so richly in the project and wider subject. Finally, on the issue of timeliness, we are aware that the print edition of this book will long outlast many of the myths currently in circulation about blockchain tech: we hope that readers will embrace the inevitable anachronisms in such an enterprise.

Notes

1 Maurer, B., T. C. Nelms, L. Swartz. 'When perhaps the real problem is money itself: the practical materiality of bitcoin,' *Social Semiotics* 23:2, 2013, pp. 261–277.

2 Motroc, Gabriela. 'Is blockchain the land of milk and honey? 9 experts share their concerns.' *Jaxenter*, June 28, 2017, <http://jaxenter.com/blockchain-interview-series-part-2-135174>. Accessed 05.07.2017.

3 'One blockchain to rule them all?' *The Economist*, Apr 20th 2016, <http://economist.com/news/science-and-technology/21697197-week-we-discuss-how->

- keep-drones-away-manned-aircraft-and-talk. Accessed 03.05.2017
- 4 Hyperledger, 2017, <http://hyperledger.org>. Accessed 01.05.2017.
- 5 Freecoin, 2017, <http://freecoin.dyne.org>. Accessed 01.05.2017.
- 6 'Business Giants to Announce Creation of a Computing System Based on Ethereum.' *New York Times*, Feb 27 2017, <http://www.nytimes.com/2017/02/27/business/dealbook/ethereum-alliance-business-banking-security>. Accessed 02.03.2017.
- 7 See Rob Myers' contributions for further explication of Dogecoin.
- 8 Morozov, Evgeny. 'Tech titans are busy privatising our data.' *The Guardian*, 24 April 2017, <http://theguardian.com/commentisfree/2016/apr/24/the-new-feudalism-silicon-valley-overlords-advertising-necessary-evil>. Accessed 05.02.2017
- 9 Qureshi, Haseed. 'A hacker stole \$31M of Ether—how it happened, and what it means for Ethereum.' *medium.com*, 20 July 2017, <http://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce>. Accessed 25.07.2017.
- 10 Greenfield, Adam. *Radical Technologies: The Design of Everyday Life*. London: Verso, 2017.
- 11 *Ibid.*
- 12 Bloomberg, Jason. 'Six Reasons Why We Need Blockchain Skeptics.' *Forbes*, July 30 2017, <http://forbes.com/sites/jasonbloomberg/2017/07/30/six-reasons-why-we-need-blockchain-skeptics>. Accessed 01.08.2017.
- 13 Jasanoff, Sheila and Sang-Hyun Kim (eds.). *Dreamscapes of Modernity – Sociotechnical Imaginaries and the Fabrication Of Power*. University of Chicago Press, 2015.
- 14 Dodd, Nigel. 'The Social Life of Bitcoin.' *Theory, Culture & Society*, 2017, ISSN 0263-2764 (In Press), p. 1.
- 15 Reijers, Wessel, and Mark Coeckelbergh. 'The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies.' *Philosophy and Technology*, 31 Oct 2016, p. 15.
- 16 See for example two blockchain evangelists: Vinay Gupta, 'The Promise of the Blockchain', *Vimeo*, 25 Feb 2016, <http://vimeo.com/161183966> and Melanie Swan's 'Institute for Blockchain Studies', <http://blockchainstudies.org>
- 17 Kafka, Ben. *The Demon of Writing: Powers and Failures of Paperwork*. Zone Books, 2012, p. 17.
- 18 'Bitcoins are a waste of energy – literally.' *ABC News*, 05 Oct 2015, <http://abc.net.au/news/2015-10-06/quiggin-bitcoins-are-a-waste-of-energy/6827940>. Accessed 01.05.2017.
- 19 Chapron, Guillaume. 'The environment needs cryptogovernance.' *Nature | Comment*, 22 May 2017, <http://nature.com/news/the-environment-needs-cryptogovernance-1.22023>. Accessed 20.05.2017.

Artists Re:Thinking the Blockchain Introduction

We want to stimulate a conversation with you about what arts brings to blockchain developments and vice versa. To discuss the implications and potentials for the arts of the blockchain.¹

We know that the blockchain is an important and powerful new technology but ‘we don’t know what a blockchain can do yet.’²

You will find here starbursts of joy about the potential extensions of creative collaboration offered by blockchain technologies.³ But it is also darkly poetic that another energy-ravenous financial technology should emerge just as we watch the tipping point of manmade global-warming recede to the distant horizon in our rear view mirrors. So this is not a marketing campaign, but a discussion of ‘what is’. In spite of the, as yet, unresolved technical obstacles of scalability and environmental cost blockchain technologies are here to stay. They are overtaking the WWW as the next big network technology for speculation and disruption. Investors recognize their potential for authentication of identity and matter, more efficient and secure financial transactions and distribution of digital assets; communications so secure as to facilitate voting; and as a coordinating technology for the billions of devices connected to the Internet.⁴ They currently attract huge investment from finance, technology and government sectors⁵ in anticipation of the fourth industrial revolution of decentralized, super-automation and hyperconnectivity.

Powerful technologies develop to reflect the interests and values of those who develop them, but impact the everyday lives of us all. The World Economic Forum predicts that these developments will be accompanied by a significant increase in global inequity.⁶ This vision of the future disenfranchises and demotes the role played by an ever increasing number of humans (and no doubt other life forms too) in the business of determining what makes a good life. It has been shown that ‘strategies for economic, technical and social innovation that fixate on establishing ever more efficient and productive systems of control and growth, deployed by fewer, more centralized agents [are] both unjust and environmentally unsustainable. Humanity needs new strategies for social and material renewal and to develop more diverse and lively ecologies of ideas, occupations and values.’⁷

Our efforts to publish this book represent our assertion that artists have a crucial part to play here. As Gene Youngblood says: 'Radicals don't predict they build.'⁸ So we must aim for more variety in background and outlook among the people involved in the building of blockchains and the imaginaries that underpin them.

Artists have worked with computing and communication infrastructures for as long as they have been in existence. They have consciously crafted particular social relations with their platforms or artwares. When artists approach new technologies a number of things happen: by making connections that are neither necessarily utilitarian nor profitable, they explore potential for diverse human interest and experience; they discover expressive and communicative potentials of its tools, devices, systems and cultures; they make difficult concepts more feelable, legible and fascinating.⁹ They have also already had central roles in projects such as D-Cent¹⁰ and FairCoop,¹¹ the blockchain-based tools for enhanced democracy.

Artists are good at mediating abstractions for our perceptions through play, open exploration and supposition. They can tolerate, even relish, extended encounters with difference, contradiction, muddle and slippage between symbolic and material possibilities without rushing to usefulness or simplicity. They have a kitbag of methods and processes for revealing the practical affordances and animal spirits of a subject, medium or technology. They know that a way to get to know something that doesn't yet exist is to collaborate with its possibilities and to do something/anything with it or about it. And by doing so they materialize and shape what it will be, allowing many other people to access, approach, and reach out to it with different parts of themselves.

The contributors to this book are developing and sharing a situational awareness of a technology that is notoriously hard to conceptualize. The difficulty of understanding how the blockchain works, and why it is significant, may partly be due to the fact that the majority of us are still mystified by the working of both money and markets. Perhaps the most important and hard-to-grasp characteristics of the blockchain is the way it puts finance, or its mechanisms, at the heart of every action in the digital domain. This also means, as Rob Myers writes, that 'AltCoins, cryptotokens, smart contracts and DAOs are tools that artists can use to explore new ways of social organization and artistic production. The ideology and technology of the blockchain and the materials of art history (especially the history of conceptual art) can provide useful resources for mutual experiment and critique.'¹²

The remainder of this introduction is in two parts. The first offers some simple blockchain orientation. The second part sets out to tell the story of how we got to this point and to share with you our plans and intentions for the future. Perhaps with this information you will want to get involved. We hope so.

[The blockchain is...]

00:15	00:20	Irra Ariella Khi Co-founder and CEO Vchain Technology	The blockchain is a new way of building our information technology. In a way that's truly never been done before.
00:21	00:25	Ben Vickers Curator of Digital, Serpentine Galleries Co-founder, unMonastery	The blockchain is my darkest nightmare.
00:26	00:35	Jaime Sevilla Developer, Researcher GHAYA #hackforgood	The blockchain is a way of coordinating computers all over the world in a way that they have always the same information.
00:36	00:41	Research Fellow, Associate Director – Centre for Crypto- currency Research, Imperial College	The internet was about the exchange of information. Blockchain is about exchange of assets and exchange of value.
00:42	00:51	Sam Davies, Digital Catapult	Because of the Blockchain in the future there's going to be less reliance on central points of authority, to handle data and to handle transactions and the rules around how that data's used.
00:52	00:59	Dr. Catherine Mulligan	Blockchain is that final crest on the tsunami of digital technologies that will really challenge fundamentally the way that we structure society.
01:00	01:10	Vinay Gupta Resilience Guru Hexayurt	It really is a generic technology like the web you could build almost any kind of workable system on top of it, it can enhance almost any political model. So what we're going to get depends on what we choose.
01:13	01:20	Elias Haase Developer, Thinker, Beekeeper Founder, B9lab	With this technology especially you are chiseling away on a new kind of society.
01:21	01:30	Irra Ariella Khi	In terms of relating to each other, the number one thing as human beings we use is trust. Blockchain allows us to replace trust with proof.

The blockchain is the underlying technology for the first global digital currency, Bitcoin, and was first described in 2008 in a white paper by the pseudonymous Satoshi Nakamoto. This coincided with (and some suggest was a direct response to)¹⁴ the financial crash which saw the banks bailed out by government with taxpayers' money. Since 2013 it has been developed to facilitate not only the decentralized creation, tracking and exchange of digital money but also smart contracts – 'unstoppable applications',¹⁵ deployed by humans and then enacted without further human interference.

Its proponents claim that the global deployment of smart contracts via this new protocol will change everything forever. And depending on the kind of person you are, and the kind of access you have to knowledge, tools and resources you will find this exciting, exasperating, foolish, terrifying, the latest hype swing, or just plain not-your-business. If you are old enough it will remind you of the clamour surrounding the emergence of the World Wide Web. In terms of its ecology of tools and infrastructures, the blockchain is at the same stage of development as the WWW in the early 90s. It's not surprising therefore that many people find blockchain hard to understand.

A good way into this is to realize that the history of computing is tied up with the history of database management.¹⁶ Which I will now simplify like this...

- ❑ **A computer is a machine that stores information in a database and a collection of software to manipulate and move that information around.**
- ❑ **The Internet is a network of computers (and their databases).**
- ❑ **In 1991 the Web gave us a way to access the information on the network of computer databases around the world.**
- ❑ **In the early noughties peer to peer technologies enabled file sharing on a global scale.**
- ❑ **1999 ubiquitous computing and mobile technologies allowed computers to 'live among us in the world'.**
- ❑ **In 2008 the Bitcoin digital currency was launched – a secure, anonymous and transparent, way to record all transactions to a decentralized global database.**

□ **In 2013 people realized that Bitcoin is underpinned by the blockchain protocol that can be used to distribute and enact smart contracts (and smart contracts are pieces of software that can manipulate and move around information, and now digital assets).**¹⁷

[Cryptocurrency is...]

A cryptocurrency is digital, but it can be used and exchanged electronically like other currencies. After they are unleashed on the world cryptocurrencies are not controlled by a central authority like countries or central banks. Instead, their value and use as an exchange medium is reached by consensus between its users using blockchain technology. In cryptocurrency, trust in people and institutions is replaced by trust in the fairness of market forces and the mathematics of cryptography which prevent counterfeiting and maintain its security.

The value of a cryptocurrency is set by market supply and demand, just as with gold or silver. Hard metals derive their value from scarcity and the difficulty of extraction, with cryptocurrencies the only difficulty is computational, the only scarcity by design. In a system called proof-of-work¹⁸ miners' machines run software that uses processing power and lots of energy to compete for coins. To mine new coins, these computers periodically gather up a 'block' of new transactions from across the network and then race to solve a difficult mathematical puzzle for that block. The winner is said to have successfully mined the block, granting them ownership of the freshly minted coins and any transaction fees paid by users.

This new block incorporates a reference to the previously mined block (represented by its 'cryptographic hash' ID number), and joins a sequential, unmovable chain of blocks. The security and stability of a blockchain is maintained because all users hold a record of every transaction made. Because each new block takes so much computational power to mine, it very quickly becomes prohibitively expensive to hack the currency. In this way it solves the double spend problem, answering the question: 'how do I prove, without the mediation of a central authority, that the payment I have received can be honoured, in order that I may release my asset to the payee?'

The initial advertised benefits of cryptocurrencies (there are lots of altcoins now all with slightly different features) included the

lack of interference by states and banks, the ‘trusted third parties’ in Nakamoto’s white paper; the low cost of payment processing (compared with wire transfers); and the ability of its underpinning blockchain technology to provide infrastructure connecting transactional apparatus to secure votes and share holdings. Because of the anonymity of transfers, Bitcoin is also said to have facilitated money laundering, the trading of illicit goods and nefarious services such as assassination markets.¹⁹

[A smart contract is...]

02:58	03:10	Rob Myers Artist, Writer, Hacker	A smart contract is a piece of code now on the Blockchain which performs the function of a legal contract without the interference of a possible corruptible human agency.
03:11	03:21	Elias Haase	In a way, code is law. We don't control it, we can't alter it once it's been implemented and it will do what it's been built to do.
03:22	03:28	Jaya Klara Brekke Digital Strategy, Design, Research and Curating Durham University	When you're looking at money you're looking at governance, you're looking at law. You know that's not trivial stuff. That's not just something you can reinvent within a few lines of code.
03:29	03:41	Dr. Catherine Mulligan	The redefinition of society will happen in smart contracts and these kind of places unless the law courts are actively ensuring that people aren't getting disenfranchised
03:42	04:02	Pavlo Tanasyuk CEO BlockVerify	Information systems they are fundamentally social, and when we think about a bank or certain organization we have to understand that it's not only technologies we have to be able to be aware of but also this social interaction of people and we have to understand how we can map that into the system.

– Excerpts from *The Blockchain: Change Everything Forever*, (2016)²⁰

Since 2013 blockchain-based platforms like Ethereum have been under development to enable software programmes known as ‘smart contracts’ to enact decisions and to distribute capital on a blockchain network, according to agreed terms, without human user verification; with the responsibility for doing so embodied in their programming rather than in written or spoken legal contracts. The resulting Decentralized Autonomous Organizations, and Applications (DAOs and DAPPs), can automate the administration of company business and act like computer viruses with wallets in their pockets.

Vitalik Buterin the coder and co-founder of Ethereum describes the

second wave of development, after digital currencies, as a ‘universal programmable blockchain’ packaged up for anyone to use for finance, p2p commerce, ‘distributed governance and human collaboration as a whole’ offering the ‘ability to create technologies that are decentralized, removing middle men’.²¹

And so it follows that blockchain technology promises to facilitate the automation, monetization, manipulation (through smart contracts) and marketization of every transaction across a decentralized global database.

While the Web is the Internet of information and communication, the blockchain is the Internet of Money.²²

Smart contracts have ambiguous legal status. While the law’s defaults technically apply, until very recently²³ they have flown under the radar of government regulation. While this is one of the main attractions to people whose political complexion we might describe as anarcho-capitalist and who ask ‘what has regulation ever done for us?’,²⁴ there is growing concern about the impact of these technologies. As Dr. Catherine Mulligan puts it ‘the worry is that society is being restructured by a small unrepresentative group of technocrats while it’s something that everyone needs to participate in – the discussion about society and economy, and also governance, how we rule ourselves.’²⁵

[Blockchains and the arts... warm up]

It’s normal that Furtherfield should pay attention to the blockchain. It is an emerging network technology and we are an arts led community who work with networked media and pay attention to how network technologies are changing reality. As Marc Garrett, Furtherfield’s co-director has written: ‘The meaning of art is in perpetual flux, and we examine its changing relationship with the human condition... Neo-liberalism’s panoptic encroachment on everyday life has informed Furtherfield’s own motives and strategies and, in contrast with most galleries and institutions that engage with art, we have stayed alert to its influence as part of a shared dialogue.’²⁶

Like many people we started experimenting in the Furtherfield office, with mining bitcoins in the late noughties, but not with any real focus. It was difficult and boring, it wasn’t art and it didn’t make any sense. We have since trashed those old computers with their wallets installed (these would be worth tens of thousands of ££££s now).

Over the following years artist and hacker Rob Myers, a long-time Furtherfield contributor and advisor, wrote a series of articles and made a series of software-artworks that explored algorithms, accelerationism, art in the era of smart contracts, and the relationship between conceptual art and cryptocurrency. In 2014 he shared with us a draft for a paper called *DAOWO – DAO it With Others*²⁷ which set the scene for our work with the blockchain. It proposed to combine DAOs with *DIWO (Do It With Others)*²⁸ – arts-led methods and actions for critical and collaborative production and a commons for arts in the network age. It pointed at the many internal ethical contradictions of the rhetoric surrounding blockchain developments, all of which resonated very strongly with me, as a recovering WWW-utopian.

It was at this point that philosophical fascination coincided with an increasingly urgent need to build a more resilient future arts economy to sustain Furtherfield's communities and platforms. Art is, after all, practical philosophy and as media art pioneer Shu Lea Cheang has noted: 'Money, value, monetary exchange... These concepts have long been excluded from the field of new media, as if the Internet and Net Art were emancipated from these issues, living not on love and fresh water but on silicon and bits, living in a utopia of collective intelligence detached from economic constraints.'²⁹ Accordingly, we were gripped by the idea that interventions into established currency systems by citizens, artists and cultural workers could provide a source for new thinking and potentially create an ecology of value and values in which arts and artists would play a central role.

This prompted further investigation and we started to take inspiration from, and to connect up with, the work other people and programmes such as the the activist hedge fund *Robin Hood Cooperative*,³⁰ *Digital Futures: Money No Object*³¹ with Rachel Falconer at the White Building and Irini Papadimitriou at the V&A in London; *MoneyLab*³² at the Institute of Network Cultures, Amsterdam; and the experimental Art Reserve Bank³³ where you can change your money into a new reserve currency created by artists. We continued to be informed by our friends at the Foundation for Peer to Peer Alternatives³⁴ which proposes theories and methods for a transition to a global commons; and by our *Reading the Commons* group led by Tim Waterman, Research Associate in Landscape Commons, at Furtherfield. Most crucially it was activated by 20 years of art and conversation between hundreds of artists, techies, activists, thinkers and doers with diverse perspectives, who participate from around the world on the Furtherfield website³⁵ and the Netbehaviour email discussion list.

[Dance!]

Furtherfield launched the *Art Data Money* programme in Autumn 2015 with the intention of drawing an active international community of artists, technologists and activists to look at the opportunities for increased collaboration and sustainability in the arts offered by big data and the blockchain. We invited them to join us online and at our 2 venues, a gallery and lab space in the heart of Finsbury Park in North London to build a commons for arts in the network age for a programme of:

- ❑ **Art Shows where finance, cryptocurrencies and data are made tangible through critically engaging, feelable artworks for everyone.**
- ❑ **Labs using hacking, play, and artistic techniques to take apart existing financial structures; algorithms and data flows to discover how they work and create new more participatory models.**
- ❑ **Debates involving an alliance of diverse partners to generate new conversations, networks, and ways of organising value exchanges across traditional divides.**³⁶

In 2015 we curated an exhibition at Furtherfield Gallery and a toured an offshoot exhibition around the UK with Digital Catapult. *The Human Face of Crypto Economies* (2015)³⁷ and its accompanying lab series featured work by Dani Admiss, Émilie Brout and Maxime Marion, Shu Lea Cheang, Sarah T Gold, Jennifer Lyn Morone, Rob Myers, The Museum of Contemporary Commodities (MoCC), Brett Scott at the London School of Financial Arts, and Cecilia Wee. The work sought to demystify money and cryptocurrencies, to discover in whose interest data is gathered and circulated, and at how we might produce, exchange and value things differently in the age of big data and the blockchain. This work garnered a broad spectrum of attention, review and discussion from across the art, blockchain and fintech worlds. In 2016 we received a small research collaboration grant from The Culture Capital Exchange, to work with Sam Skinner of Torque to explore the possibilities for experimental publishing on the blockchain.

2016 also saw the start of a partnership between myself and Ben

Vickers of UnMonastery and Serpentine Galleries that brought focus to our shared ambition for more social engagement, and activist organization, and a desire to interrogate and address more closely the possibilities offered by the blockchain for cooperation and collaboration within the art world.

In April 2016 we convened a two day event to explore the potential for the arts of the blockchain. The first day's workshop at Furtherfield Commons brought together a range of artists and developers, researchers and activists to map the fast emerging field. Much of the work of participants in that workshop is represented in this book. Jaya Klara Brekke and Elias Haase crystalize the ethical challenge to developers in the form of *The Satoshi Oath*, setting out one of the clearest analyses I have seen of the worrying and dangerous absence of scaffolding for social responsibility in engineering and enterprise cultures. Curator and theorist Helen Kaplinsky points out the current trend in arts-focused blockchain startups such as Ascribe, Monegraph and Verisart (that focus on IP tracking for digital art and provenance of artworks) to replicate the Victorian conception of art, represented by the operations and capital flows within existing museum and gallery systems, in the service of the artworld oligopoly. She also discusses *Ampliative Art*, an early art DAO mapped out by Spanish artist-academic Adrian Onco who was also present. Artist and researcher, Kei Kreutler drew connections between artist manifestos and organizational constitutions that may inscribe the solidarity-generating (or otherwise) values of arts collectives into DAOs. Max Dovey, over from the Institute for Network Cultures, brought his experience of programming the *MoneyLab* conference and his recent participation in a blockchain bodystorming workshop with Chris Speed and the Design Informatics team at the University of Edinburgh, in which their *Geocoin* prototype app provided the catalyst for the devising of a temporary, location-based Bitcoin marriage system as an exploration of informal contracts. This is the starting point for his article in this book about the consequences of the blockchain's immutability rule and the dangers of irreversible contracts. Also present was Sam Skinner, co-director, with Nathan Jones, of the experimental publishers Torque, with whom we collaborated on this very book!

The second day's event was of a different nature. Hosted by the Austrian Cultural Forum, we invited art and technology world-players, thinkers and policy makers to gather together, in order to share our findings and invite them to rise to the challenge of engaging with this critical moment in history, stating in no uncertain terms:

‘blockchain technologies are set to shape the next century.’

We offered a short introduction to the affordances of the technology and then presented our view on the potential impact of the blockchain and arts together, informed by the previous day’s discussions:

- ❑ **New funding models – Renegotiation of the economic and social value of art.**
- ❑ **Lowering the cost for organising – DAOs could remodel collaboration.**
- ❑ **Automated solidarity for artists and new kinds of audiences, patrons and participants.**
- ❑ **Unanticipated futures – New imaginaries for how we act in the world.**
- ❑ **Redefine ‘Authorship’ – Incentives for fractional, progressive ownership & collective production of art and livelihoods.**
- ❑ **Opening up black box technologies – to diversify engagement**

This event provided the context for thinking together and learning quickly without a preset artistic, commercial, or ideological agenda. What emerged was a cautious interest in the ‘potential for blockchain to devolve mechanisms and processes for funding for artists, as well as allowing various players in the arts ecosystem – artists, collectors, viewers, curators, and others – to define how they want to interact, with the possibility that sharing and artwork almost merge, or at least become as two sides of the same coin.’³⁸ This event was notable for its presentation of the technology as inherently ambiguous, in contrast to critiques of it as both literal fascism,³⁹ and ‘to the original libertarian or revolutionary claims made for Bitcoin, the evolution of the technology today seems to offer as many risks of a dystopian future as emancipatory opportunities.’⁴⁰ There was also a level of perplexity in the audience and a desire voiced for making the subject more accessible, while still critical. I’m sure that someone said that a book may aid this!

We followed this up with the creation of the short film *The Blockchain: Change Everything Forever* directed by film maker Peter Gomes (2016), in collaboration with Digital Catapult, London, which set

out to broaden the range of people involved in its future by bringing together leading thinkers, computer scientists, entrepreneurs, artists and activists. It asked ‘What can a blockchain do? Who builds this new reality? How will we rule ourselves? and How will the future be different because of the blockchain?’⁴¹ We deliberately selected contributors across the spectrum – from fierce critics to evangelists, and we made an art film. This film has been described as ‘the most critical film yet to be made about the blockchain’⁴² (there is a LOT of blockchain video marketing out there). It has been watched online by over 13,000 people and viewed at art exhibitions, screenings and blockchain conferences and festivals around the world.

Since this time we have been building our understanding and range of approaches to working with blockchains. At MoneyLab 2016 Vickers and I ran a *Live Action Role Play* for 35 people called *Role Play Your Way to Budgetary Blockchain Bliss*. It took the hackathon as a scenario and made concrete the inequities often at play at the start of any real world enterprise. Pablo Velasco’s account in this book captures the methods and spirit of the event. This activity was a precursor to a series of smart contract role-play and design activities for people of all backgrounds and disciplines where participants will write social relations into code as a basis for debate. From Autumn 2017 we will partner with Goethe-Institut on a series of *DAOWO* workshops to build capacity in the arts for working with and understanding blockchain, as part of a European collaboration project *State Machines: Art, Work, and Identity in an Age of Planetary-Scale Computation*.

Our recent exhibition at Furtherfield Gallery *NEWWORLD ORDER*⁴³ invited visitors to imagine a world in which responsibility for many aspects of life (reproduction, decision-making, organization, nurture, stewardship) are mechanised and automated. Transferred, once and for all, from natural and social systems into a secure, networked, digital ledger of transactions and computer-executed contracts. Envisioning a future world of world-making machines, markets and natural processes, free from interference by states and other human institutions. These included two blockchain-based artworks, both presented in this book: O’khaos’ self-replicating metal flower *Plantoid*, a new hybrid life-form that evolves on the blockchain, and *terra0* the augmented forest that owns itself and sells its own assets on the blockchain. It also presented the crypto based sci-fi story *Bad Shibe* by Rob Myers with illustrations by Lina Theodorou, reprinted here, which is a pathos-rich meditation on the emergence of ideologies propounded and executed by an elite of technical experts who are also free market believers. The installation by xfx (*a.k.a.* Ami Clarke), also

represented in this book, included a video as data capture, showing glimpses of the material parts of an Ether mining rig. It conveys the energy used and the sweat equity of a DIY cryptocurrency prospector with finely tuned financial calculations and a (not so free) money mining system. This exhibition will tour in 2018 to Aksioma, Slovenia and Drugo More, Rijeka as part of the *State Machines* programme.

All of this work is also helping to prepare the ground for moving a part of Furtherfield onto the blockchain in the context of Platforming Finsbury Park, a 4 year initiative in which we plan to transform Finsbury Park in Haringey, North London, into a canvas for adventurous, world-class digital art, and into a site for fieldwork in human and machine imagination. Our intention is to think through, with researchers of all stripes, the ways in which artists, participants and audiences might create, value and circulate previously unimagined artforms to interact with beliefs, decisions and intentions. The three most interesting design problems we anticipate are: how to ensure that any cultural value generated benefits diverse local communities; how to value strangeness, difference and mystique (without which we might ask, what value is art?) and; how to negotiate the bridge between users of local physical spaces and international digital networks.

We do not underestimate the work to be done here but look to the work of socially, artistically, and design minded organizations and projects already underway: Ascribe, Aragon, Art is Open Source, Backfeed, Colony, Constant, Deckspace, Faircoin, Freecoin, Metahaven, Robin Hood Cooperative, Upstage.

The artists working with the early WWW created software to craft experiences and relationships, pre-empting by 10 years, developments in the social web. Audiences for Net Art⁴⁴ became participants in and co-creators of distributed online artworks, making really strong user interfaces to engage people. The new social relations were integral to the aesthetics and message of their work. Many recent technology developments offer promise and potential as artistic media, for cultural contexts, and for expanding expressive potentials and dramatic interventions. As a new network protocol the adoption and formation of new forms of the blockchain has the potential to provide the organising principles for the deployment and use of other emerging technologies and tech cultures, IoT, VR, AR, AI, and Biotech.

If we have learned anything in our twenty years of effort to produce artworks and art contexts to stimulate and diversify debate around life since-Net it is that decentralized infrastructure does not equate

to decentralized resource or power, or at least not for any length of time. Blockchain technology ‘isn’t inherently emancipatory, just as it isn’t inherently repressive. The blockchain can be used to support pretty much any political outlook.’⁴⁵ This is a point worth pressing on and is best understood by work going on around cultures of the commons. These promote constructive experimentation through peer learning, nuanced openness, access to knowledge, tools and contexts that extend freedoms of expression, association and collaboration. But this is also accompanied by the understanding that it’s not enough for radicals just to build. Their visions must also incorporate processes of maintenance and stewardship in order to negotiate ongoing prosperity in contexts, increasingly uncertain, chaotic and unpredictable conditions, or else see their communities or cultural commons harvested, hoovered and alienated by recentralizing forces. It is for this reason that artists’ engagement with the art and politics of infrastructure – through discussions of power, law, governance, cooperation, creative collaboration, cultural stewardship, legacy and expression – are a running theme through this book.

One of our intentions in creating this book is to offer a set of differently crafted lenses through which to spy a territory, some of which exists only in our imaginations. By reading it and by playing its marketized contributions through the FinBook platform that is threaded through it, you will discover more about the origins, concepts, uses and users of blockchain technologies at work now, and to make your own mind up about what a future with the blockchain will be. Our understanding is that, as with the early days of the WWW, we have an opportunity to build our own contexts for cultural production. We should be ambitious and aspire to construct an ethical perspective on the networked society that Gene Youngblood describes as an ‘ecosocial nervous system’ operating across ‘translocal social heterotopias’.⁴⁶

In order to achieve this we must involve more diverse people in the process of making the game rather than increasing the number of people who are just to be played!

[Acknowledgements and thanks]

Marc Garrett, for being a critically engaging badass, and a dedicated partner in adventures of the networked imagination. The unstoppable creative experimentalists Nathan Jones and Sam Skinner of Torque publishing. Peter Gomes, Kei Kreutler, Rob Myers, and Ben Vickers for high art and high geek insight and inspiration and

crypto-solidarity. For generous, accessible and engaging writing and acting about crypto-things and why they are important Vinay Gupta, Dr. Catherine Mulligan, Brett Scott and Melanie Swan. My fellow blockchain-curious Londoners: Rachel Baker, Lara Blazic, Alexie Blinov, Ami Clarke, Neil Cummings, David Cross, Lisa Haskell, Helen Kaplinsky, Amit Rai, Lucy Sollitt, James Stevens, Mark Waugh, Cecilia Wee, Martin Zeilinger and; internationally: Shu lea Cheang, Max Dovey, Dr. Rachel O'Dwyer, Dr. Primavera De Filippi, Holly Herndon, Alexandre Monin, Cornelia Sollfrank, Hito Steyerl and terra0.

For inspiration: Ampliative Arts, Art is Open Source, Ascribe, Aragon, BigchainDB, Carroll/Fletcher Gallery, Colony, DAOWO, D-Cent, Facecoin, Faircoin, Foundation for P2P Alternatives, Entropical, iMAL, Institute of Network Cultures, London School of Financial Arts, Network Disruption Lab, Netbehaviour discussion list, Monograph, O'khaos, Plantoid, Robin Hood Cooperative, MoneyLab, Spiralseed, Torque, unMonastery, Upstage.

Partners and funders of this work include: The energetic and endlessly enquiring team from the Design Informatics Dept at the University of Edinburgh University headed up by Dr. Chris Speed, with Rory Gianni, Bettina Nissen, and Shaun Oosthuizen. Arts Council England, Computer Arts Society, Digital Catapult, FACT, Goethe-Institut, Haringey Council, London, Ravensbourne, Southbank Centre, The Culture Capital Exchange, The Creative Europe Programme of the European Union and the State Machines network: Aksioma, Drugo More, Institute of Network Cultures and NeMe.

Finally, heartfelt thanks to all Furtherfielders. You know who you are!

Notes

1 Opening statement at *Potentials for the Arts of the Blockchain* at Austrian Cultural Forum, April 2016. Convened by Furtherfield and Ben Vickers.

2 Artist and researcher, Kei Kreutler in *The Blockchain: Change Everything Forever*, A Furtherfield film by Pete Gomes, 2016.

3 See the interview by Marc Garrett with Holly Herndon and Mat Dryhurst in this book.

4 *How Many Things are Currently Connected to The 'Internet of Things' (IoT)?* <http://forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot>

5 \$1.4bn investment in blockchain start-ups in last 9 months of 2016, says PwC expert John Kennedy, *Silicon Republic*, November 2016, <http://linkis.com/Ayjj>

6 UBS White Paper for the World Economic Forum, Annual Meeting 2016, *Extreme Automation and Connectivity: The Global, Regional, and Investment Implications of the Fourth Industrial Revolution*.

7 Catlow, Ruth. 'WE WON'T FLY FOR ART: MEDIA ART ECOLOGIES.' *Culture Machine*, Vol 13, 2012, <http://culturemachine.net/index.php/cm/article/download/475/493>

- 8 Gene Youngblood in Third Space Network convened by Randall Packer, 2017, <http://thirdspacenet.com/gene-youngblood>
- 9 See also: Catlow, Ruth. *Art and the Blockchain, Digital Catapult*, 2016, <http://digitalcatapultcentre.org.uk/art-and-the-blockchain>
- 10 <http://dcentproject.eu>
- 11 <http://fair.coop/faircoin>
- 12 Myers, Rob. 'Conceptual Art, Cryptocurrency and Beyond.' *Furtherfield*, 2014, <http://furtherfield.org/features/conceptual-art-cryptocurrency-and-beyond>.
- 13 *The Blockchain: Change Everything Forever*, 2016.
- 14 http://en.bitcoin.it/wiki/Genesis_block
- 15 <http://www.ethereum.org>
- 16 Gupta, Vinay. 'Programmable Blockchains in Context: Ethereum's Future.' *Conensys*, 2015, <http://media.consensys.net/programmable-blockchains-in-context-ethereum-s-future-cd8451eb421e>
- 17 This elaborates on a slide presented at the Austrian Cultural Forum, April 2016 in an event convened by Furtherfield and Ben Vickers in which we invited arts and policy makers to join us to explore the potential for blockchain and the arts.
- 18 Proof-of-work is the system used by Bitcoin and other major cryptocurrencies at time of writing. However other systems are now being developed to address energy use. Ethereum is working on proof-of-stake and, to discourage hoarding and currency speculation, Faircoin now implements proof-of-cooperation.
- 19 This long explanation is reprinted mostly verbatim from my *Afterword for Bad Shibe*, 2017. I'm pleased to say that this glorious Dogecoin-inspired sci-fi novella by Rob Myers is reprinted here along with illustrations by Lina Theodorou.
- 20 *The Blockchain: Change Everything Forever*, 2016.
- 21 'Vitalik Buterin explains Ethereum.' *YouTube*, <http://youtube.com/watch?v=TDGq4aeevgY>.
- 22 Antonopoulos, A.M. *The Internet of Money*. Createspace Independent, 2016.
- 23 *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities* issued by U.S. Securities and Exchange Commission, Washington D.C., July 25, 2017, <http://sec.gov/news/press-release/2017-131>.
- 24 Asked in all seriousness by Vinay Gupta, in one of his informative, entertaining and terrifying podcasts.
- 25 Dr. Catherine Mulligan, in *The Blockchain: Change Everything Forever*, 2016.
- 26 Garrett, Marc. 'Furtherfield and Contemporary Art Culture – Where are We Now.' *Furtherfield*, 2015, <http://furtherfield.org/features/articles/furtherfield-and-contemporary-art-culture-where-we-are-now>.
- 27 <http://furtherfield.org/artdatamoney/includes/files/daowo.pdf>
- 28 <http://furtherfield.org/projects/diwo-do-it-others-resource>
- 29 Cheang, Shu Lea and Annick Rivoire. 'We Grow Money, We Eat Money, We Shit Money.' *MCD*, #76, 2015, <http://www.digitalmcd.com/la-version-anglaise-du-mcd76-est-disponible>.
- 30 <http://bollier.org/blog/robin-hood-coop-activist-hedge-fund>
- 31 <http://furtherfield.org/programmes/event/digital-futures-money-no-object-prototyping-session>
- 32 <http://networkcultures.org/moneylab>
- 33 <http://artreservebank.com>

- 34 <http://p2pfoundation.net>
- 35 <http://furtherfield.org>
- 36 <http://furtherfield.org/artdatamoney>
- 37 <http://furtherfield.org/programmes/exhibition/human-face-cryptoeconomies>
- 38 Chakrabarti, U. Kanad. 'From Bearer Bonds to the Blockchain: Artistic Perspectives on Digital Money.' *Eatthe hipster*, 2016, <http://eatthehipster.org/2016/05/01/blockchains-potential-in-the-arts>
- 39 Columbia, David. *The Politics of Bitcoin, Software as Right-Wing Extremism*. University of Minnesota Press, 2016.
- 40 *Ibid.*
- 41 Made in collaboration with London's Digital Catapult <http://furtherfield.org/projects/blockchain>.
- 42 In conversation with Pablo de Soto of Hackitectura.
- 43 <http://furtherfield.org/programmes/exhibition/new-world-order>
- 44 In her 2011 book *Nettitudes – Let's Talk Net Art*, Josephine Bosma describes Net Art as 'art based on Internet cultures, which revolve around technology, games, social networks, commerce and politics.'
- 45 Chakrabarti, U. Kanad. 'From Bearer Bonds to the Blockchain: Artistic Perspectives on Digital Money.'
- 46 Gene Youngblood in Third Space Network convened by Randall Packer, 2017, <http://thirdspacenetnetwork.com/gene-youngblood>.