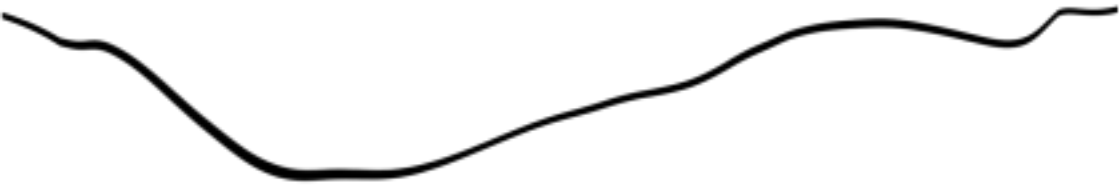
SR / DPR

A Reader by Luke Munn



Printing generously provided by:
http://colab.aut.ac.nz/

For information about projects, writing and research, please visit:
http://www.lukemunn.com/

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

John Perry Barlow
February 8, 1996

Introduction:
Luke Munn

Timeline:
01.11.2008 16:16:33
The Birth of Bitcoin

03.01.2009 18:15:05
The Genesis Block

01.06.2011 12:00:00
Silk Road Running

02.10.2013 15:15:00
DPR Arrested

26.10.2013 07:36:13
FreeRoss.org Registered

Reader:
Messages to the FBI
The Bitcoin Community

Liberalism in the Classical Tradition
Ludwig von Mises

Bitcoin - finally, fair money?
The Wine & Cheese Appreciation Society of Greater London and Scott Lenney

Bitcoin, Magical Thinking and Political Ideology
Alex Payne

Bitcoin and the Speculative Anarchist
Adam Rothstein

A Shining Beacon
Dread Pirate Roberts

New Institutions, Old Shells
An Interview with Robert O'Brien

Introduction:

In 2008 Satoshi Nakamoto released a whitepaper on bitcoin, a new peer-to-peer cryptocurrency which redefined the way in which money is created, stored, and distributed. The paper outlined an elegant solution to double-spending and other traditional problems, establishing a proof of work consensus in which the longest chain of hashing procedures can be certified using a mixture of timestamping and cryptographic mechanisms. Built around a dynamic network architecture, the currency platform also allows peers to asynchronously connect, verify the global blockchain of transactions, and disconnect. This eliminates the necessity for any central institution or third party service, providing an infrastructure that resists the intervention of any single regulating body. In ideological terms then, Bitcoin almost effortlessly combines the cold beauty of rationalism with a pure libertarianism of free markets unfettered by state control. In Crypto We Trust.

In many ways, Bitcoin also embodies a disembodiment, an immateriality evidenced by individual's addresses as long alphanumeric strings, by CPU based mining which ignores energy costs, or by the financial 'mixer' services which merge transactions from multiple users into an anonymous slurry. In this space of private keys, botnet DDoS attacks and dizzying currency fluctuations, this immateriality is one which is even exemplified by the creator herself. Satoshi Nakamoto is an entity with no 'real world' referent. Over several years, an array of investigative journalists, hackers, and community groups have attempted to establish the identity of this mythic

figure. All have failed to prove their case. Each designee has strenuously denied being the Bitcoin inventor. In one theory, Satoshi is actually a group of corporates working in tandem, a hybrid name constructed by combining the letters of Toyota, Mitsubishi, Sanyo, and other Japanese multinationals.

This disembodiment also powered the dreams of the Dread Pirate Roberts, the kingpin of the Silk Road. As a deep web address, this marketplace didn't exist in the mainstream topographies of the internet which are spidered by Google and other search engines, but instead required an encrypted browser and Tor's typical long alphanumeric string to access. As DPR espoused, the site wasn't simply a technical e-commerce implementation of Bitcoin with Tor, but a free market experiment molded on the principles of libertarianism, the Austrian school of economics, and agorism. If the Silk Road operated on a different network protocol, it also leveraged its immateriality to provide distancing on an emotional and psychological level. The marketplace isolated its buyers from the unexpected dangers of street level drug trafficking, both in terms of purchase and use. In other words, SR bypassed the erratic behaviour of dealers, but just as importantly, it provided a hermetic space wholly discrete from the bodily fallout of junkies, binges and bad trips.

Like Satoshi, Silk Road's alleged kingpin, Ross Ulbricht attempted to use a pseudonym as a mechanism for distributing his identity into a constellation of personas. The Dread Pirate

Roberts was originally a character from the film Princess Bride, in which the name is gifted from one pirate to the next, carrying on a legend for the sake of increased notoriety. In Ulbricht's case, the DPR moniker was not only a way to atomise his individuality, but also mitigate his responsibility. In a Forbes interview, DPR claims he is the second incarnation of the name, simply taking over the work from Silk Road's true founder, the original DPR. Alongside this expanded digital identity, Ulbricht attempted to almost disappear physically. According to flatmates who knew him as Josh, he ate steak dinners for one most nights and kept to himself, working in his bedroom on his laptop. On Silk Road's forums he confessed that there was no one he could talk to in the real world, nobody he could confide in. Unlike Satoshi however, Ulbricht was all too human, undone by fallibility, physical presence and psychological markers. He posted a question about PHP and Tor on coding site Stack Overflow using his public handle 'ohyeaross' before changing it a couple minutes later to a more generic, 'frosty'. His net footprint fleshes out a real world figure, from LinkedIn to a singles profile, a NetWorth account and a minimal YouTube channel, photographs depict a handsome figure visiting a sister in Sydney, dancing at a college party, hanging out with family in Texas. His poetic writings and economic interests stem from a single persona, matching up across media ranging from social network platforms to deep web forums.

On October 1, 2013 at 3:15pm, the FBI descended on the Science Fiction section of the Glen Park Library in San Francisco,

arresting Ulbricht and using several screenshots from his laptop as evidence in its charges filed the next day. According to their allegations, the digital screen name of one of the largest narcotics operations had been traced back to a single eagle scout from Austin Texas. It's this bleed through that the project seeks to explore, not only the permeability embodied within the life of Ross Ulbricht, but also the tensions in the other threads of this story: the spirituality of technorationalism, the transparency of anonymity, and the infrastructural underpinnings of free cybermarkets.

Luke Munn, Aotearoa, September 2014

01.11.2008 16:16:33

The Birth of Bitcoin:

Bitcoin P2P e-cash paper
Satoshi Nakamoto Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at: http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted 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 honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted 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.

Full paper at: http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

---------- The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to

03.01.2009
18:15:05

The Genesis Block

The Genesis Block is the name given to the first block within any blockchain-based cryptocurrency platform.

Alongside key information such as timestamps and receiver wallet addresses, Bitcoin also provides mechanisms to embed around 50 characters of additional information about the transaction, sometimes used for public notes or ‘mined by’ accreditations.

Satoshi Nakamura’s Genesis Block, however, used this space to include the following text:

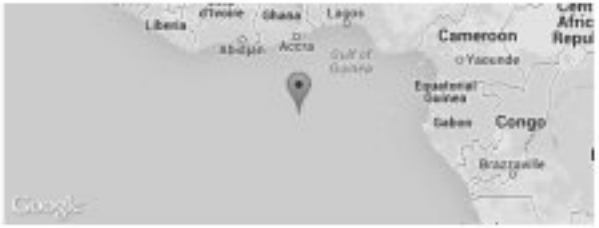
‘The Times 03/Jan/2009 Chancellor on brink of second bailout for banks’

Block #0

Summary	
Number Of Transactions	1
Output Total	$ 21,444.50
Estimated Transaction Volume	$ 0.00
Transaction Fees	$ 0.00
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.2783203125 KB
Version	1
Nonce	2083236893
Block Reward	$ 21,444.50

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Network Propagation (Click To View)



Transactions Transactions contained within this block

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b (Size: 204 bytes) 2009-01-03 18:15:05

No Inputs (Newly Generated Coins) → 1A1zP1eP5QGefi2... (Genesis of Bitcoin 🔒) - (Unspent) $ 21,444.50

$ 21,444.50

Transaction View information about a bitcoin transaction

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

No Inputs (Newly Generated Coins)	1A1zP1eP5QGefi2... (Genesis of Bitcoin ð) - (Unspent)	$ 21,439.00
		$ 21,439.00

Summary	
Size	204 (bytes)
Received Time	2009-01-03 18:15:05
Reward From Block	0
Scripts	Hide scripts & coinbase
Relayed by IP	0.0.0.0 (whois)
Visualize	View Tree Chart

CoinBase

04ffff001d0104455468652064696d6573203033214a616e2f323030392043686616e63656c6c6f722066f6e206272696e6b2066207365636f6e642062616e6b75742066f722062616e6b73
(decoded) ��EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Output Scripts

04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG	OK

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

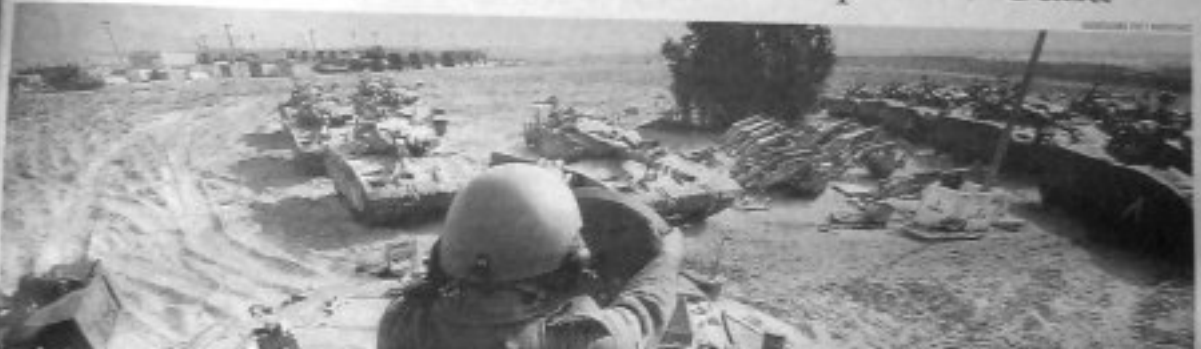
£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza



Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets". The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hoof" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

Detox in style
The best spas on the planet
Travel

Salman Rushdie
I won't marry again
Pages 22, 23

Giant killing?
Guide to the FA Cup third round
Sport

01.06.2011 16:20:00

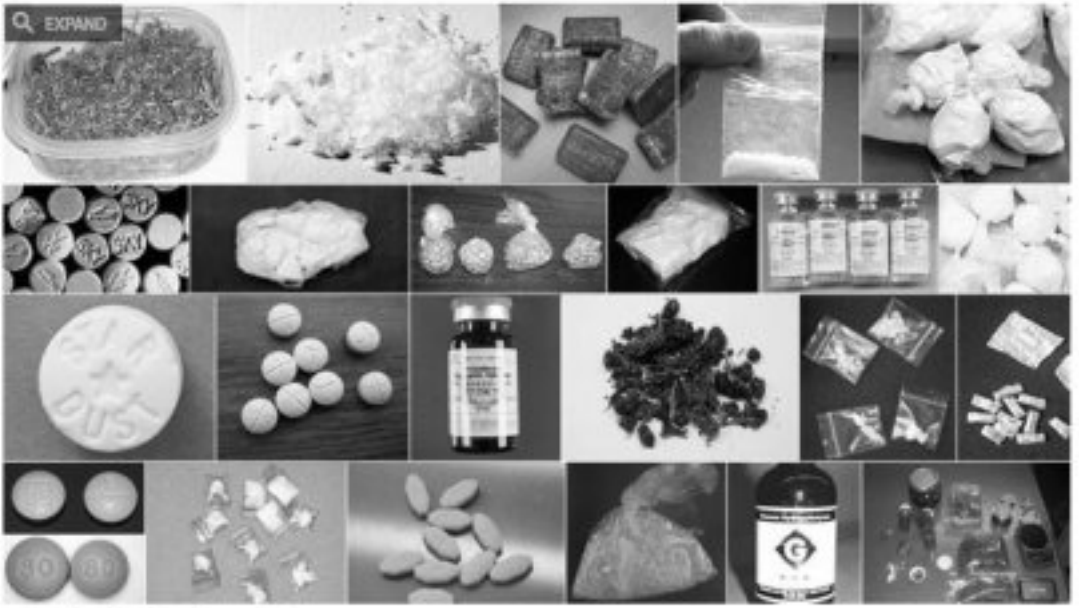
Silk Road Running

GAWKER

The Underground Website Where You Can Buy Any Drug Imaginable

Adrian Chen
Filed to: EXCLUSIVE 6/01/11 4:20pm

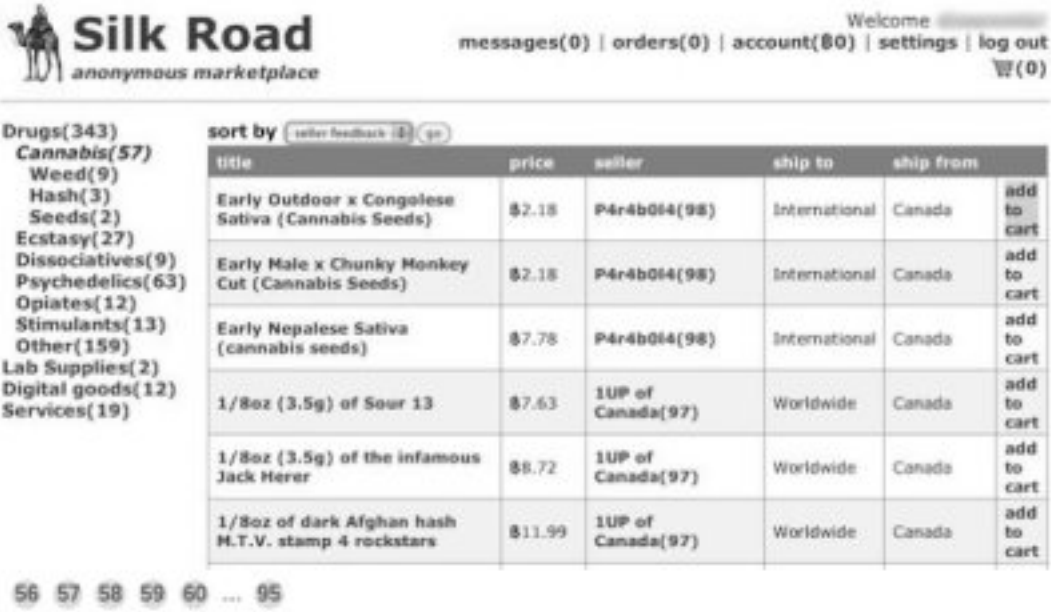
2,502,441 20



1 2 3 4 5 ... 55

Making small talk with your pot dealer sucks. Buying cocaine can get you shot. What if you could buy and sell drugs online like books or light bulbs? Now you can: Welcome to Silk Road.

About three weeks ago, the U.S. Postal Service delivered an ordinary envelope to Mark's door. Inside was a tiny plastic bag containing 10 tabs of LSD. "If you had opened it, unless you were looking for it, you wouldn't have even noticed," Mark told us in a phone interview.



Mark, a software developer, had ordered the 100 micrograms of acid through a listing on the online marketplace Silk Road. He found a seller with lots of good feedback who seemed to know what they were talking about, added the acid to his digital shopping cart and hit "check out." He entered his address and paid the seller 50 Bitcoins—untraceable digital currency—worth around $150. Four days later the drugs, sent from Canada, arrived at his house.

"It kind of felt like I was in the future," Mark said.

View gallery »

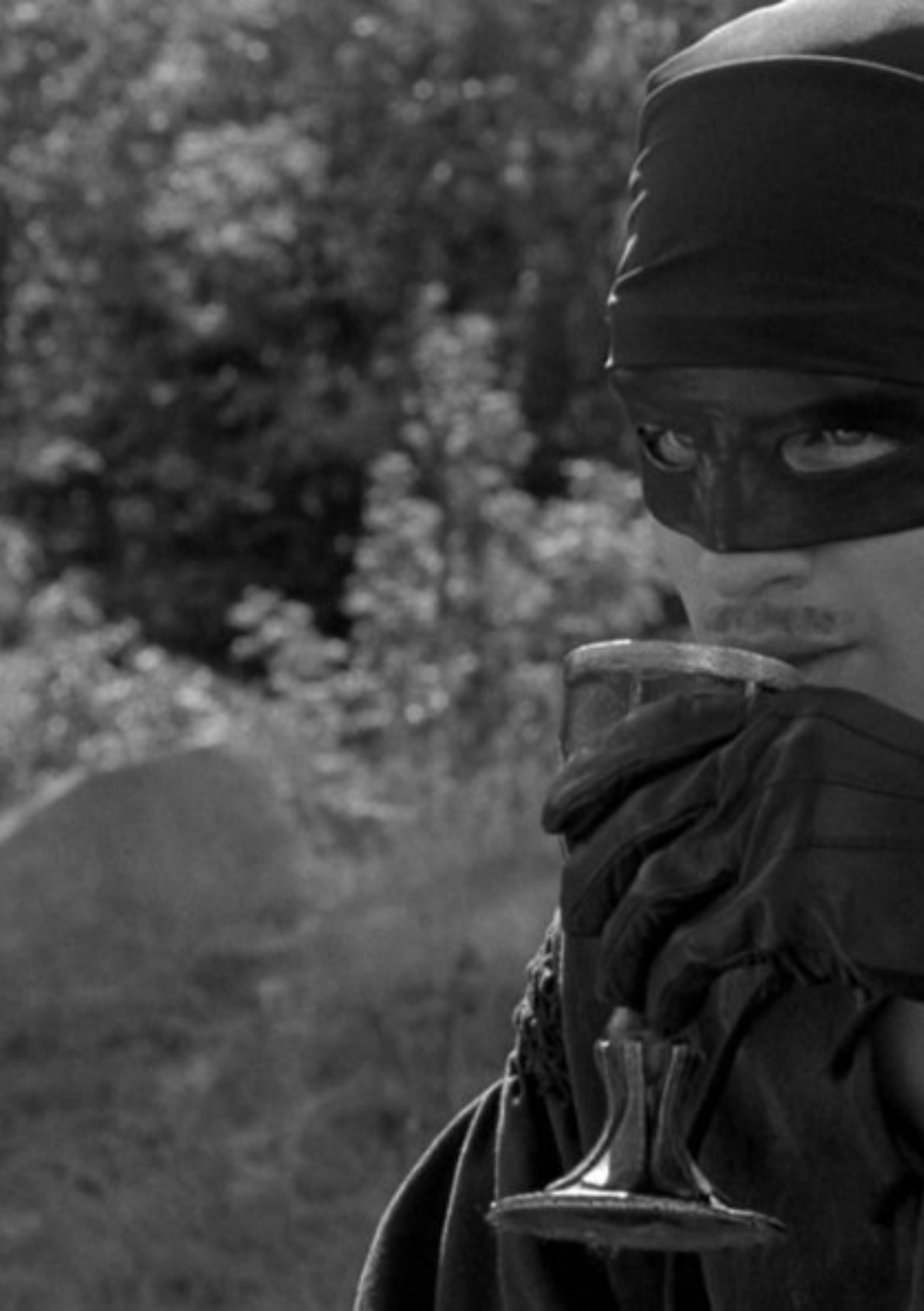
Silk Road, a digital black market that sits just below most internet users' purview, does resemble something from a cyberpunk novel. Through a combination of anonymity technology and a sophisticated user-feedback system, Silk Road makes buying and selling illegal drugs as easy as buying used electronics—and seemingly as safe. It's Amazon—if Amazon sold mind-altering chemicals.

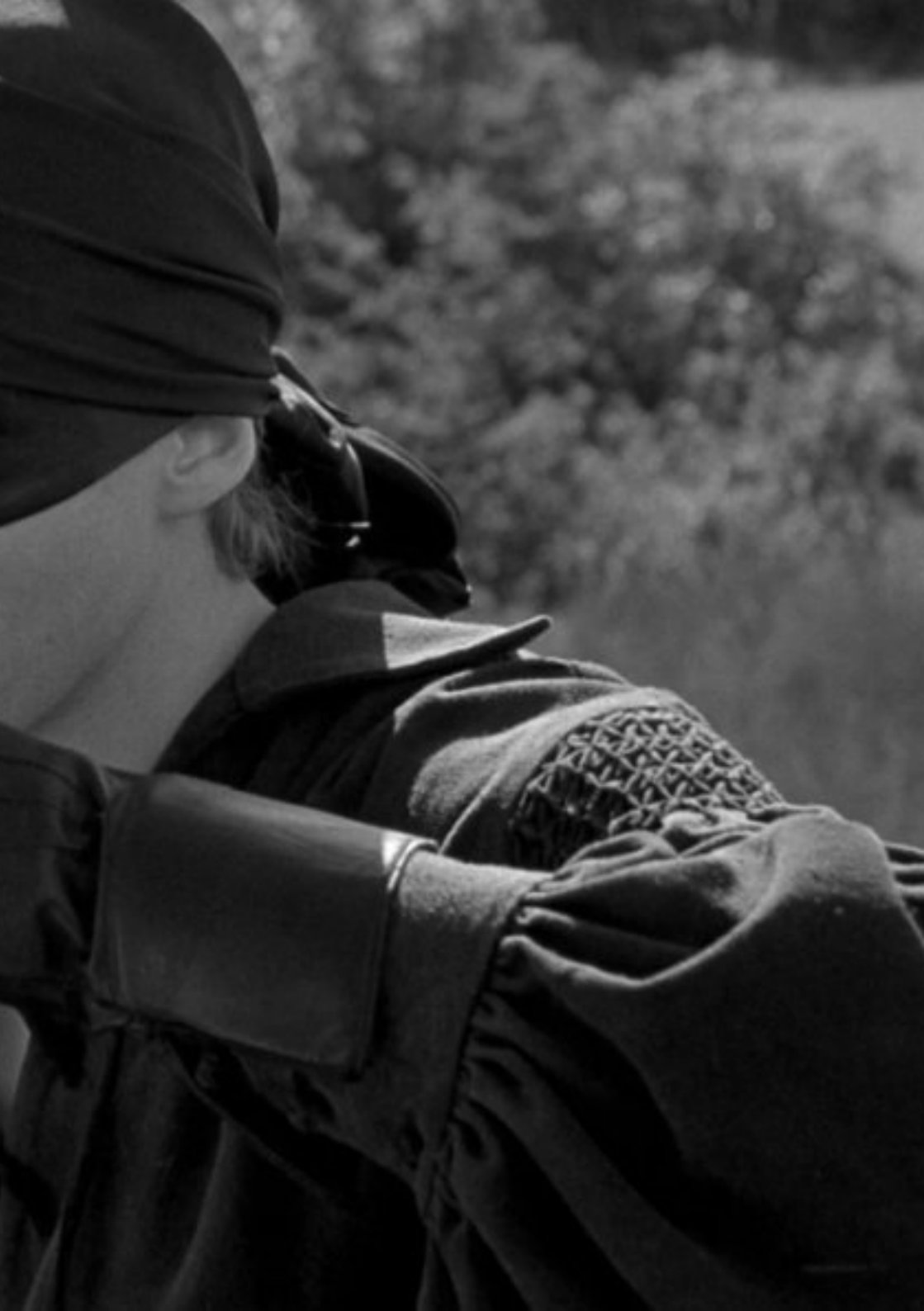
02.10.2013
15:15:00

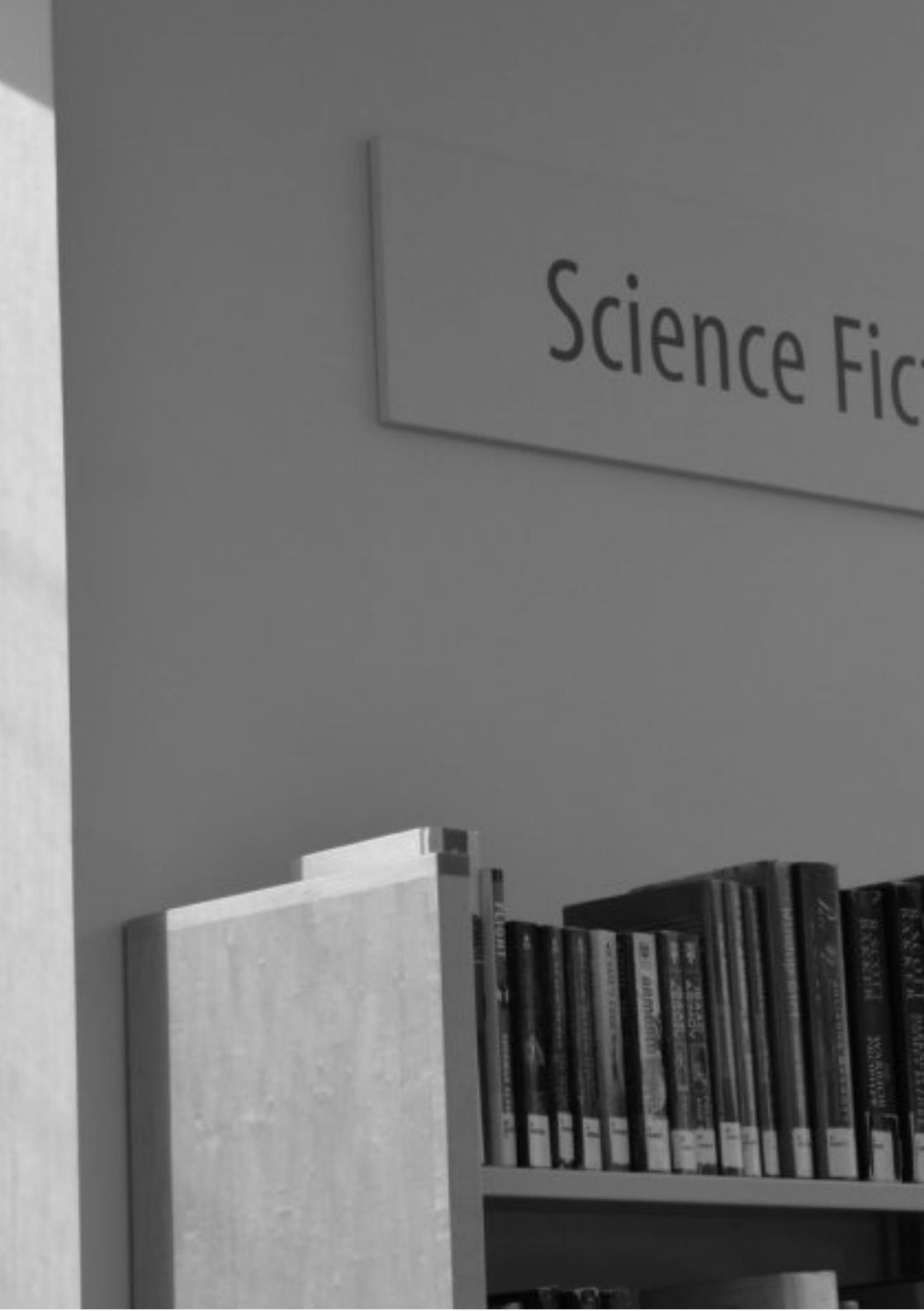
Dread Pirate Roberts Arrested

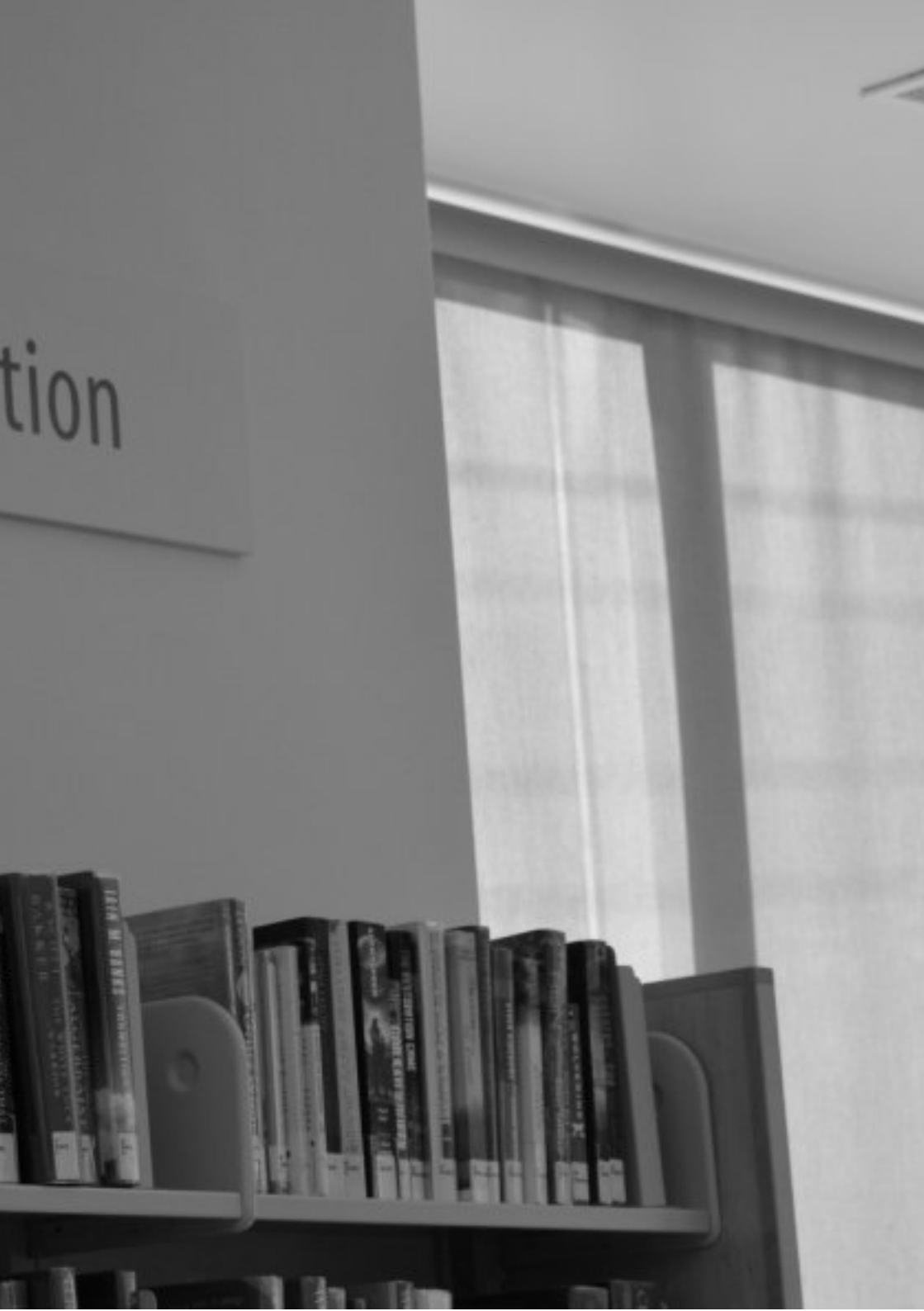
Westley: Well, Roberts had grown so rich, he wanted to retire. So he took me to his cabin, and told me his secret. "I am not the Dread Pirate Roberts", he said. "My name is Ryan. I inherited the ship from the previous Dread Pirate Roberts, just as you will inherit it from me. The man I inherited it from was not the real Dread Pirate Roberts either. His name was Cummerbund. The real Roberts has been retired fifteen years and living like a King in Patagonia." Then he explained that the name was the important thing for inspiring the necessary fear. You see, no one would surrender to the Dread Pirate Westley. So we sailed ashore, took on an entirely new crew, and he stayed aboard for a while as first mate, all the time calling me Roberts. Once the crew believed, he left the ship, and I have been Roberts ever since.

The Princess Bride, 1987, Director: Rob Reiner, Production Company: Twentieth Century Fox
http://www.princessbride.8m.com/script.htm






Science Fic


tion

DPR: I didn't start the Silk Road, my predecessor did. From what I understand, it was an original idea to combine Bitcoin and Tor to create an anonymous market. Everything was in place, he just put the pieces together… He was well compensated and happy with our arrangement. It was his idea to pass the torch in fact.

I would say my role is as a center of trust. The vendors trust me and the customers trust me and by extension they trust those on my team that decide who is right and wrong in disputes, and they trust me to be responsible for their funds in escrow. My role is also to provide vision and direction, to chart a course so to speak.

An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A), Andy Greenberg, Forbes http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/

The Federal government claims that Ross Ulbricht created and operated the anonymous online marketplace Silk Road, under the pseudonym Dread Pirate Roberts (DPR). Although law enforcement shut down the Silk Road site Oct. 2 after arresting Ross, DPR posted on the Silk Road forum six days later and the Silk Road site was up and running again about a month later and is still today.

http://freeross.org/the-case-the-goal-and-why-this-matters-2/

When Ross Ulbricht, known as Dread Pirate Roberts to users of the site, was arrested last week, the FBI seized 26,000 Bitcoins belonging to Silk Road customers. But it also attempted, unsuccessfully, to claim the nearly 600,000 - thought to be worth around $80m - which Ulbricht himself is thought to be holding.

Bitcoin is a digital currency based on a methods of cryptography similar to those used to protect confidential emails. Due to its decentralised nature – the currency does not rely on any centralised agency to process payments, instead relying on work done by users' computers – it is popular for a number of fringe-legal and illegal uses. One of those uses was Silk Road, where Bitcoin was required for all transactions.

http://www.theguardian.com/technology/2013/oct/07/fbi-bitcoin-silk-road-ross-ulbricht.

26.10.2013 07:36:13

FreeRoss.org Registered

Free Ross Ulbricht | The C

freeross.org

FREE ROSS ULBRICHT

THE OFFICAL LEGAL DEFENSE FUND OF THE ULBRICHT FAMILY

HOME THE CASE WHO IS RO

INTERNET FRE

ARE A

The outcome of this

THE CASE

The Federal government claims that Ross Ulbricht created and operated the web marketplace Silk Road, under the pseudonym Dread Pirate Roberts (DPR)... Read More

WHY THIS MATTERS

This case will set precedent for the 21st century and pave the way for new law and interpretations that will impact the future and freedom of the Internet and our First Amendment rights... Read More

SS? DONATE LINKS/ARTICLES CONTACT & MORE

EDOM AND PRIVACY

T STAKE

case will impact your life.

DONATE NOW

OUR GOAL

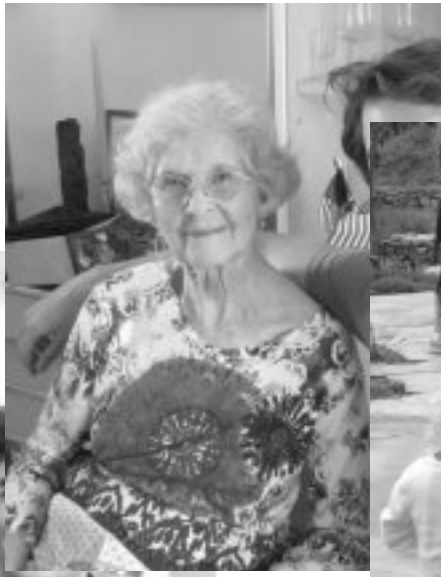
To protect individual freedom and privacy. To provide Ross with what every American citizen is promised: a fair trial. To have Ross acquitted of all charges. Read More

HOW TO HELP

Every donation helps and none is too small. Credit card, PayPal, bitcoin all work to help defend Ross, Internet privacy and our personal liberty. Read More

YouTube

Download The Free Ross Posters Here



Messages to the FBI
The Bitcoin Community

The FBI has been deluged by more than 200 messages of protest from pro-drugs advocates after a raid on Silk Road, an online marketplace for illicit goods.

The agency is attempting to access 600,000 Bitcoins, worth around $80m (£49.7m), accumulated by Ross Ulbricht, the alleged creator of Silk Road, but has already seized 26,000 ($3.2m) that the site had held in escrow for its customers.

The FBI then transferred the Bitcoins to a new address on blockchain.info., which allows users to manage their Bitcoin accounts.

Unfortunately for the FBI, hundreds of Silk Road users identified the FBI's wallet details and used blockchain to post publicly viewable messages along with miniscule transactions.

http://www.theguardian.com/technology/2013/oct/07/fbi-bitcoin-pranked-silk-road

Public Note: The designer of a new kind of system must participate fully in the implementation. -- Donald E. Knuth
2c77011c1f2bee473f7fee2a94cec760ba48ab02344020f4a2d38130632a85542013-10-05 11:05:26
12CzJJGGe8YQ9a6ncELCMRAfADnMQzhSeQ
Silkroad Seized Coins 0.0001 BTC

Public Note: If people let the government decide what foods they eat and what medicines they take, their bodies will soon be in as sorry a state as are the souls of those who live under tyranny. - Thomas Jefferson
4d26df559898974d25b671f63cb6b2cdba12030ec06d91a7df01d37ed6665a672013-10-05 11:00:02
1F7CinWsrNhP7Cy3wbRs5afTHsT3M35kSU
Silkroad Seized Coins 0.0000001 BTC

Public Note: “The means of defense against foreign danger historically have become the instruments of tyranny at home” ? James Madison
4d65d663d7979b234fbe6f0b23d6abdc85215272bea4b118e9d901c97e54fd032013-10-05 05:14:03
1MHuciFBEM2h7R11U1za4zSTcPMSZt9m3S
Silkroad Seized Coins 0.00000001 BTC

Public Note: CNN, FOX, NBC. Imagine if we could trace every single dollar the government spends? Why can't we do that today? This is the age of the internet, but the gov't is clouded in secrecy. Long live BTC BG.

d7e8604c7af0b7f5f1a9f427f12d7445b4c895b15d69c5aad746044
8388631d82013-10-05 03:40:48
17Acos3VtCfR1Pdmyqnw2d2nzE3KTGGWGQ
Silkroad Seized Coins 0.000001 BTC

Public Note: Prohibition doesn't work. Good try. Many more will rise.
c86f5f7a70db1c5a3001be6889c9fc3b2307b0749e7154a42b10db4
ff10829452013-10-05 02:38:37
1AxpEfouR7AwsPURZcLsgMNhzfVzgYRy7C
Silkroad Seized Coins 0.000001 BTC

Public Note: Hey look, three markets to take its place, and more to come. Real bang up job there guys. Keep telling yourself that your fake white god is coming to help you.
4763968f60a73de60fb4da10f43c9a7f55d6960a339e95276db5f43
c26df25d32013-10-05 01:38:53
1GiuRBiLuDrRHs5jZq6eMMwCQmTzEQxTwL
Silkroad Seized Coins 0.0001 BTC

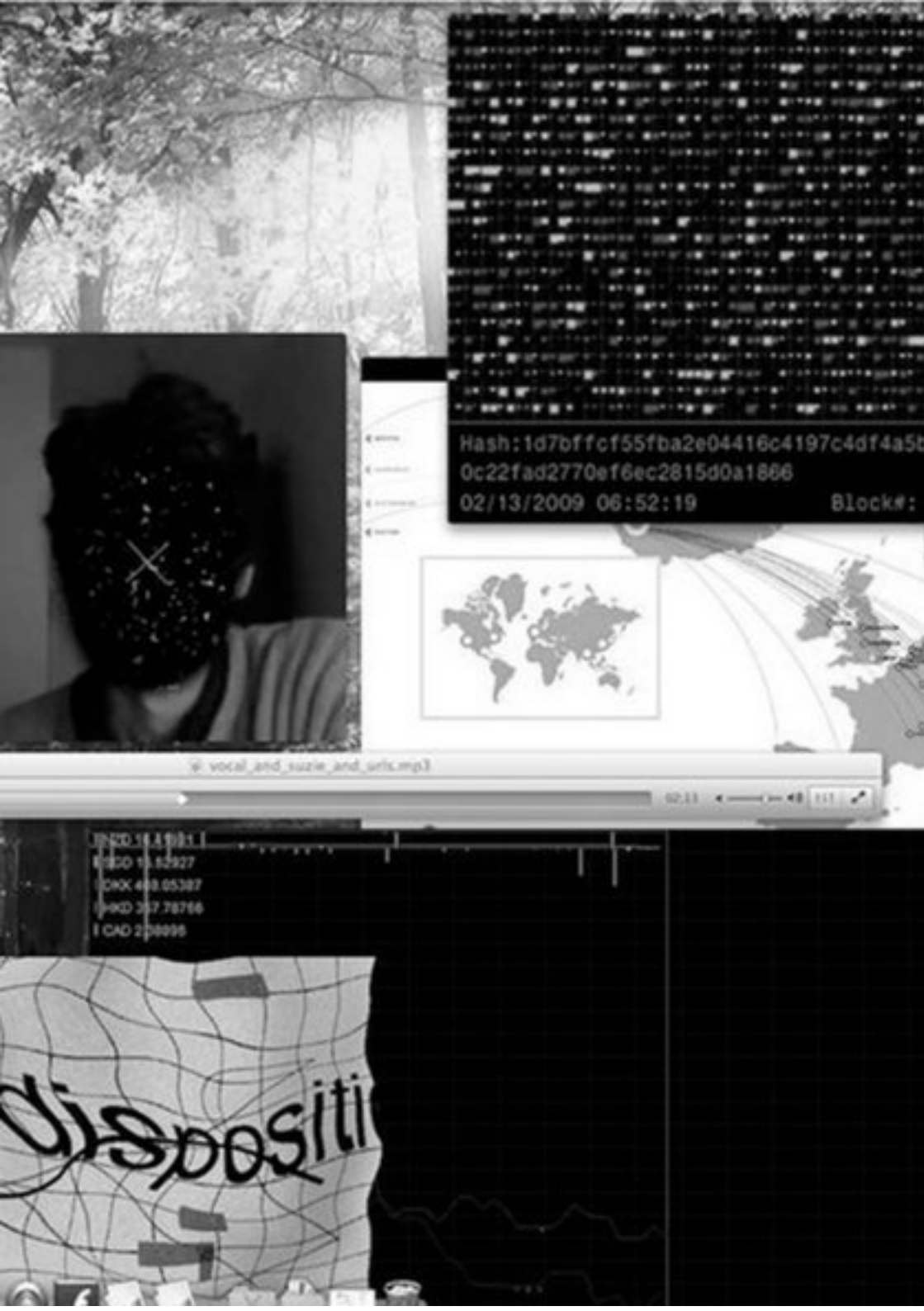
Public Note: PROVERBS 10:2 - Treasures gained by wickedness do not profit, but righteousness delivers from death
3b233c4896027020a3f66369c20bc38eec2a8ab755e76c4975d37a3
092ce26302013-10-04 23:30:30
1GHZv4b2Qz9TdqY7rswXRfFLT3Rbuhy6UZ
Silkroad Seized Coins 0.00001 BTC

Public Note: LeT mE dOn8 tO yOuR eViL cAuSe! AlL hAiL tHe

eViL GoVeRnMeNt!
fbea2a1c79c8c30f4b45b04d190adbd62e07bfbb31c93918e9a1545a7f20da6a2013-10-04 22:38:28
13bYGNEaG4UKocNasNf5WL4mDWgMDGJDXD
Silkroad Seized Coins 0.0000666 BTC

Public Note: Tired of donut-eating stereotypes? Buy baklava w/ btc @ mandrik.com!
b460098fdba4d2c304a6b493da12dac632d1eca5ec006d72dd775d987cee8dab2013-10-04 18:28:05
12vGQPuSU6kCAtwhWcBTbB2ZDSxFKSaK6V
Silkroad Seized Coins 0.00001 BTC

Public Note: U.S. Marines Guard Afghanistan Poppy Fields | http://www.youtube.com/watch?v=HNqIrDKnNE8
087674b0b76f4e1691021c750f104bbdad4ddaba08f8a74f54646db932e3c2ba2013-10-04 14:49:35
1AhbPvDuR8BLcMYp7VxPSr8ChAj4yFT3Ee
Silkroad Seized Coins 0.0002 BTC


Hash:1d7bffcf55fba2e04416c4197c4df4a5
0c22fad2770ef6ec2815d0a1866
02/13/2009 06:52:19
Block#:
vocal_and_suzie_and_urls.mp3
dispositi

Liberalism in the Classical Tradition
Ludgwig von Mises

1. Liberalism

The philosophers, sociologists, and economists of the eighteenth and the early part of the nineteenth century formulated a political program that served as a guide to social policy first in England and the United States, then on the European continent, and finally in the other parts of the inhabited world as well. Nowhere was this program ever completely carried out. Even in England, which has been called the homeland of liberalism and the model liberal country, the proponents of liberal policies never succeeded in winning all their demands. In the rest of the world only parts of the liberal program were adopted, while others, no less important, were either rejected from the very first or discarded after a short time. Only with some exaggeration can one say that the world once lived through a liberal era. Liberalism was never permitted to come to full fruition.

Nevertheless, brief and all too limited as the supremacy of liberal ideas was, it sufficed to change the face of the earth. A magnificent economic development took place. The release of man's productive powers multiplied the means of subsistence many times over. On the eve of the World War (which was itself the result of a long and bitter struggle against the liberal spirit and which ushered in a period of still more bitter attacks on liberal principles), the world was incomparably more densely populated than it had ever been, and each inhabitant could live incomparably better than had been possible in earlier centuries. The prosperity that liberalism had created reduced

considerably infant mortality, which had been the pitiless scourge of earlier ages, and, as a result of the improvement in living conditions, lengthened the average span of life.

Nor did this prosperity flow only to a select class of privileged persons. On the eve of the World War the worker in the industrial nations of Europe, in the United States, and in the overseas dominions of England lived better and more graciously than the nobleman of not too long before. Not only could he eat and drink according to his desire; he could give his children a better education; he could, if he wished, take part in the intellectual and cultural life of his nation; and, if he possessed enough talent and energy, he could, without difficulty, raise his social position. It was precisely in the countries that had gone the farthest in adopting the liberal program that the top of the social pyramid was composed, in the main, not of those who had, from their very birth, enjoyed a privileged position by virtue of the wealth or high rank of their parents, but of those who, under favorable conditions, had worked their way up from straitened circumstances by their own power. The barriers that had in earlier ages separated lords and serfs had fallen. Now there were only citizens with equal rights. No one was handicapped or persecuted on account of his nationality, his opinions, or his faith. Domestic Political and religious persecutions had ceased, and international wars began to become less frequent. Optimists were already hailing the dawn of the age of eternal peace.

But events have turned out otherwise. In the nineteenth century strong and violent opponents of liberalism sprang up who succeeded in wiping out a great part of what had been gained by the liberals. The world today wants to hear no more of liberalism. Outside England the term "liberalism" is frankly proscribed. In England, there are, to be sure, still "liberals," but most of them are so in name only. In fact, they are rather moderate socialists. Everywhere today political power is in the hands of the antiliberal parties. The program of antiliberalism unleashed the forces that gave rise to the great World War and, by virtue of import and export quotas, tariffs, migration barriers, and similar measures, has brought the nations of the world to the point of mutual isolation. Within each nation it has led to socialist experiments whose result has been a reduction in the productivity of labor and a concomitant increase in want and misery. Whoever does not deliberately close his eyes to the facts must recognize everywhere the signs of an approaching catastrophe in world economy. Antiliberalism is heading toward a general collapse of civilization.

If one wants to know what liberalism is and what it aims at, one cannot simply turn to history for the information and inquire what the liberal politicians stood for and what they accomplished. For liberalism nowhere succeeded in carrying out its program as it had intended.

Nor can the programs and actions of those parties that today call themselves liberal provide us with any enlightenment

concerning the nature of true liberalism. It has already been mentioned that even in England what is understood as liberalism today bears a much greater resemblance to Toryism and socialism than to the old program of the freetraders. If there are liberals who find it compatible with their liberalism to endorse the nationalization of railroads, of mines, and of other enterprises, and even to support protective tariffs, one can easily see that nowadays nothing is left of liberalism but the name.

Nor does it any longer suffice today to form one's idea of liberalism from a study of the writings of its great founders. Liberalism is not a completed doctrine or a fixed dogma. On the contrary: it is the application of the teachings of science to the social life of man. And just as economics, sociology, and philosophy have not stood still since the days of David Hume, Adam Smith, David Ricardo, Jeremy Bentham, and Wilhelm Humboldt, so the doctrine of liberalism is different today from what it was in their day, even though its fundamental principles have remained unchanged. For many years now no one has undertaken to present a concise statement of the essential meaning of that doctrine. This may serve to justify our present attempt at providing just such a work.


icarus_bitcoin_miner.jpg
scout
0x600.jpg
Tue Oct 1 3:17 PM
frosty
peaceful

Bitcoin - Finally, Fair Money?
The Wine and Cheese Appreciation Society of Greater London and Scott Lenney (extract)

The key technical innovation of the Bitcoin protocol is that it solves this double spending problem without relying on a central authority. All previous attempts at digital money relied on some sort of central clearing house which would ensure that Alice cannot spend her money more than once. In the Bitcoin network this problem is addressed by making all transactions public.xvii Thus, instead of handing the signed contract to Bob, it is published on the network by Alice's software. Then, the software of some other participant on the network signs that they have seen this contract certifying the transfer of Bitcoin from Alice to Bob. That is, someone acts as notary and signs Alice's signature and thereby witnesses Alice's signature. Honest witnesses will only sign the first spending of one Bitcoin and will refuse to sign later attempts to spend the same coin by the same person (unless the coin has arrived in that person's wallet again through the normal means). They verify that Alice owns the coin she spends. The witness' signature again is published (all this is handled automatically in the background by the client software).

Yet, Alice could simply collude with Charley and ask Charley to sign all her double spending contracts. She could get a false testimony from a crooked witness. In the Bitcoin network, this is prevented by selecting one witness at random for all transactions at a given moment. Instead of Alice picking a witness, it is randomly assigned. This random choice is organised as a kind of lottery where participants attempt to win the ability to be witness for the current time interval. One can

increase one's chances of being selected by investing more computer resources, but to have a decent chance one would need computer resources as great as the rest of the network combined.xviii As a side effect, many nodes on the network waste computational resources solving some mathematical puzzle by trying random solutions to win this witness lottery. In any case, for Alice and Charley to cheat they would have to win the lottery by investing considerable computational resources, too much to be worthwhile – at least that's the hope. Thus, cheating is considered improbable since honest random witnesses will reject forgeries.

But what is a forgery and why is it so bad that so much effort is spent – computational resources wasted – in order to prevent it? On an immediate, individual level a forged bank note behaves no differently from a real one: it can be used to buy stuff and pay bills. In fact, the problem with a forgery is precisely that it is indistinguishable from real money, that it does not make a difference to its users - otherwise people would not accept it. Since it is indistinguishable from real money it functions just as normal money and more money confronts the same amount of commodities and as a result the value of money might diminish.

So what is this value of money, then? What does it mean? Purchasing power. Recall, that Alice and Bob both insist on their right to their own stuff when they engage in exchange and refuse to give up their goods just because somebody needs

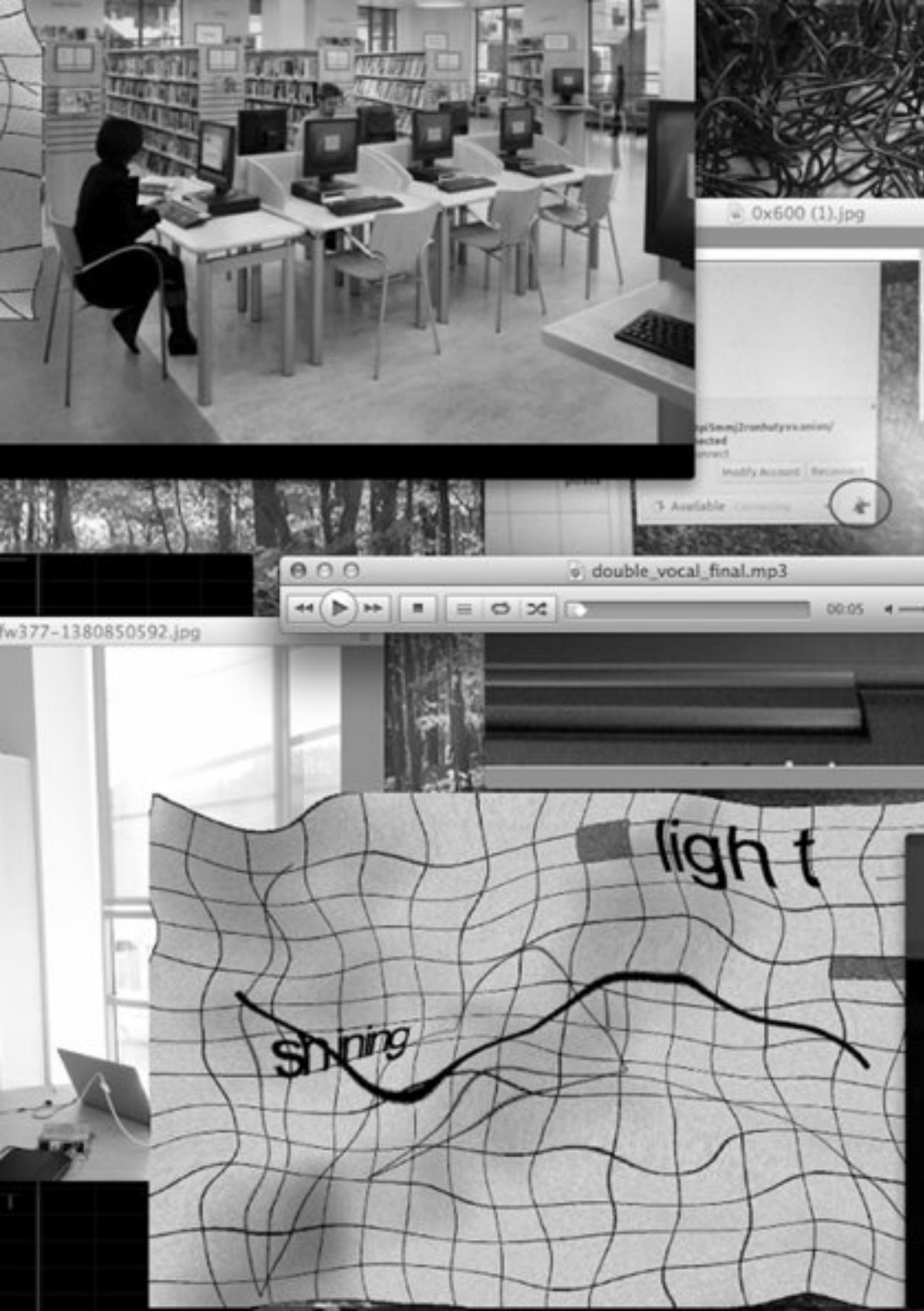
them. They insist on their exclusive right to dispose of their stuff, their private property. Under these conditions, money is the only way to get access to each other people's stuff, because it convinces the other party to consent to the transaction. On the basis of private property, the only way to get access to somebody else's private property is to offer one's own in exchange. Hence, money indicates how much wealth in society one can get access to. Money measures private property as such. Money expresses how much wealth as such one can make use of: not only coffee or shoes but coffee, shoes, buildings, services, labour power, anything. On the other hand, money counts how much wealth as such my coffee is worth: coffee is not only coffee but a means to get access to all the other commodities on the market. It is exchanged for money such that one can buy stuff with this money. The price of coffee signifies how much thereof. All in all, numbers on my bank statement tell me how much I can afford, the limit of my purchasing power and hence – reversing the perspective – from how much wealth I am excluded.

From this it is also clear that under these social conditions – free and equal exchange – those who have nothing will not get anything, that the poor stay poor. Of course, free agents in a free market never have anything, they always own themselves and can sell themselves – their labour power – to others. Yet, their situation is not adequately characterised by pointing out that nature condemns us to work for the products we wish to consume, as the libertarians have it. Unemployed workers can

only find work if somebody else offers them a job, if somebody else deems it profitable to employ them. Workers cannot change which product they offer, they only have one. That this situation is no pony farm can be verified by taking a look at the living conditions of workers and people out of work worldwide.

Money is power one can carry in one's pockets; it expresses how much control over land, people, machines and products I have. Thus, a forgery defeats the purpose of money: it turns this limit, this magnitude into an infinity of possibilities, anything is – in principle – up for grabs just because I want it. If everyone has infinity power, it loses all meaning. It would not be effective demand that counts, but simply the fact that there is demand, which is not to say that would be a bad thing, necessarily.

In summary, money is an expression of social conditions where private property separates means and needs. For money to have this quality it is imperative that I can only spend that which is mine. This quality and hence this separation of need and means, with all its ignorance and brutality towards need, must be violently enforced by the police and on the Bitcoin network – where what people can do to each other is limited – by an elaborate protocol of witnesses, randomness and hard mathematical problems.


0x600 (1).jpg
Available
double_vocal_final.mp3
00:05
fw377-1380850592.jpg
ligh t
shining

Bitcoin, Magical Thinking, and Political Ideology

Alex Payne

Last week, investor Chris Dixon posed a provocative dichotomy when introducing his employer's USD $25M investment in Bitcoin service Coinbase:

"The press tends to portray Bitcoin as either a speculative bubble or a scheme for supporting criminal activity. In Silicon Valley, by contrast, Bitcoin is generally viewed as a profound technological breakthrough."

Now working at vogue venture capital firm Andreessen Horowitz, Dixon is in a fine position to speak for Silicon Valley. But to the extent that the Valley is a placeholder for the technology industry at large, I beg to differ. Bitcoin is "generally viewed" quite differently.

Most charitably, Bitcoin is regarded as a flawed but nonetheless worthwhile experiment, one that has unfortunately attracted outsized attention and investment before correcting any number of glaring security issues.

To those less kind, Bitcoin has become synonymous with everything wrong with Silicon Valley: a marriage of dubious technology and questionable economics wrapped up in a crypto-libertarian political agenda that smacks of nerds-do-it-better paternalism. With its influx of finance mercenaries, the Bitcoin community is a grim illustration of greed running roughshod over meaningful progress.

Far from a “breakthrough”, Bitcoin is viewed by many technologists as an intellectual sinkhole. A person’s sincere interest in Bitcoin is evidence that they are disconnected from the financial problems most people face while lacking a fundamental understanding of the role and function of central banking. The only thing “profound” about Bitcoin is its community’s near-total obliviousness to reality.

Regulation and Other Minor Details
Bitcoin owes its present flexibility to a lack of regulation (or, more accurately, a lack of understanding around existing regulations and/or unwillingness to comply with them). If the broader Bitcoin experiment doesn’t implode, the currency will be regulated just as any other. In this best-case scenario for Bitcoin, what of the benefits Dixon claims?

We’re told that Bitcoin “fixes serious problems with existing payment systems that depend on centralized services to verify the validity of transactions.” If by “fixes” you mean “ignores”, then yes: a Bitcoin transaction, like cash, comes with the certainty that a definite quantity of a store of value has changed hands, and little else. How this verifies any “validity” or cuts down on fraud I’m not sure; stolen Bitcoins are spent as easily as stolen cash, which is why theft of Bitcoins has been rampant.

With those risks in mind, are the fees that existing card networks and payment processors charge – Dixon’s “roughly a 2.5% tax on all transactions” – outrageous, or are we perhaps

collectively subsidizing the cost of fraud prevention and regulatory compliance? In what plausible universe will legitimate Bitcoin transactions be allowed to take place without such protections, and thereby without the associated costs? (Incidentally, you can expect to pay a similar “tax” just to reclaim some semblance of the anonymity that Bitcoin fails to provide in the form of mixers, a zingy term for money laundering.) To be sure, the credit card companies have fattened their margins beyond the raw cost of moving money around, but we have a miraculous salve for this called regulation.

If Bitcoin’s strength comes from decentralization, why pour millions into a single company? Ah, because Coinbase provides an “accessible interface to the Bitcoin protocol”, we’re told. We must centralize to decentralize, you see; such is the perverse logic of capital co-opting power. In order for Bitcoin to grow a thriving ecosystem, it apparently needs a US-based, VC-backed company that has “worked closely with banks and regulators to ensure that the service is safe and compliant”.

And Coinbase certainly feels, uh, compliant. It took me over a week to use the service to turn US dollars into a fraction of a Bitcoin, an experience that coupled the bureaucratic tedium of legacy consumer financial services with the cold mechanization of notoriously customer-hostile PayPal, but with the exciting twist that I have no idea from moment to moment how much my shiny new Internet money is actually worth.

Magical Thinking

While most of the claims around Bitcoin are merely wince-inducing, there is one that deserves particular attention: that Bitcoin is "a way to offer low-cost financial services to people who, because of financial or political constraints, don't have them today."

Economic inequality is perhaps the defining issue of our age, as trumpeted by everyone from the TED crowd to the Pope. Our culture is fixated on inequality, and rightly so. From science fiction futures to Woody Allen character sketches, we're simultaneously alarmed and paralyzingly transfixed by the disappearance of our middle class. A story about young people dying in competition with one another just to continue lives of quiet desperation isn't radical left-wing journalism, it's the pop fiction on every teenager's nightstand and in every cinema right now.

With this backdrop of looming poverty, nobody can reasonably deny that the euphemistically "underbanked" are in desperate need of financial services that empower them to participate fully in the global economy without fear of exploitation. What's unclear is the role that Bitcoin or a similar cryptocurrency could play in rectifying this dire situation.

The push toward Bitcoin comes largely from the libertarian portion of the technology community who believe that regulation stands in the way of both progress and profit. Unfortunately, this alarmingly magical thinking has little basis in economic reality. The gradual dismantling of much of the US

and international financial regulatory safety net is now regarded as a major catalyst for the Great Recession. The "financial or political constraints" many of the underbanked find themselves in are the result of unchecked predatory capitalism, not a symptom of a terminal lack of software.

Silicon Valley has a seemingly endless capacity to mistake social and political problems for technological ones, and Bitcoin is just the latest example of this selective blindness. The underbanked will not be lifted out of poverty by conducting their meager daily business in a cryptocurrency rather than a fiat currency, even if Bitcoin or its ilk manages to reduce marginal transaction costs (at scale and in full regulatory compliance, that is). But then, we should note that Dixon wasn't talking about lifting anyone out of poverty, just "offer[ing them] low-cost financial services". Also notable is that both Andreessen and Horowitz supported Mitt Romney's failed presidential bid, giving us some insight into the likely level of concern for economic inequality around Dixon's office.

In Bitcoin, the Valley sees another PayPal and the associated fat exit, but ideally without the annoying costs of policing fraud and handling chargebacks this time around. Bankers in New York and London see opportunities for cryptocurrency market-making. International investors see the potential for arbitrage and are taking advantage of cheap electricity, bringing the environmental destruction of real-world mining to the brave new world of digital money.

In other words: Bitcoin represents more of the same short-sighted hypercapitalism that got us into this mess, minus the accountability. No wonder that many of the same culprits are diving eagerly into the mining pool.

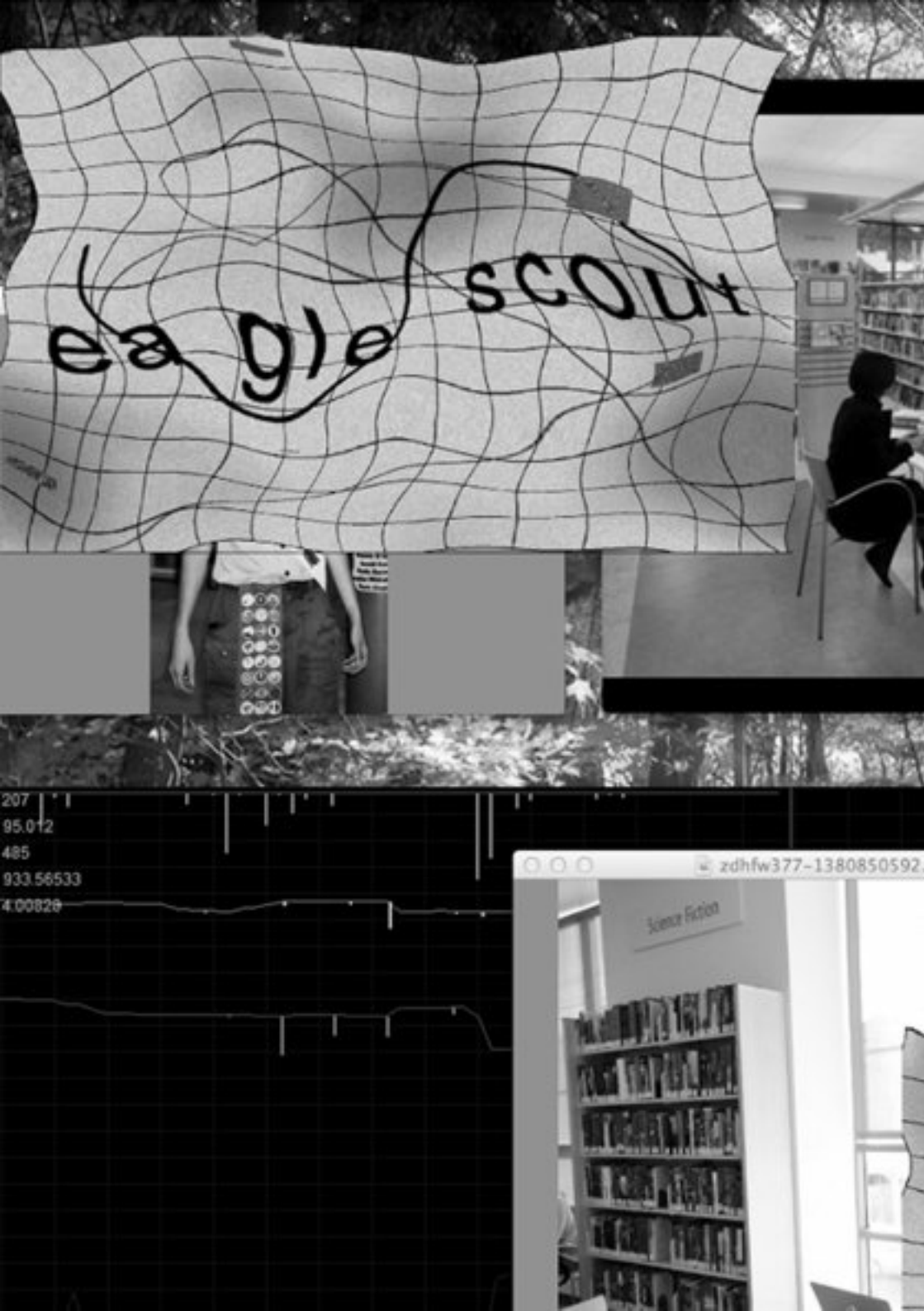
Moving Past The Failed Techno-Libertarian Agenda
For the past few months I've been giving a talk, informed largely by feedback on my post about the tradeoffs of joining startups earlier this year. The talk delves into the history of Silicon Valley and venture capital, tying past to present. Though I cover a lot of ground in a short sprint, I hope my message is clear: that the dominant socio-political ideology of Silicon Valley has failed to deliver sustainable profits to the broader investor class while technological innovation has slowed and jobs have dried up. It's time for new thinking.

Bitcoin is not without its left-wing supporters, but I think it's safe to say the currency has mostly proven to be a rallying point for those who see the state and central banks as little more than obstacles to a libertarian techno-utopia, a worldview perhaps best captured in The Californian Ideology. In this sense, Bitcoin is ready-made for a cultural moment when Silicon Valley ideologues are discussing plans for a new opt-in techno-centric society and sliding so far right that a return to monarchy is on their table.

Working in technology has an element of pioneering, and with new frontiers come those who would prefer to leave civilization

behind. But in a time of growing inequality, we need technology that preserves and renews the civilization we already have. The first step in this direction is for technologists to engage with the experiences and struggles of those outside their industry and community. There's a big, wide, increasingly poor world out there, and it doesn't need 99% of what Silicon Valley is selling.

I've enjoyed the thought experiment of Bitcoin as much as the next nerd, but it's time to dispense with the opportunism and adolescent fantasies of a crypto-powered stateless future and return to the work of building technology and social services that meaningfully and accountably improve our collective quality of life.


eagle scout
207
95.012
485
933.56533
4.00828
zdhfw377-1380850592
Science Fiction

Bitcoin and the Speculative Anarchist
Adam Rothstein (excerpt)

When I tell my close friends—who know of, and share, my anti-capitalist anarchist views—that I own some cryptocurrency (my current holdings equal something under 10 USD) I get the same sort of looks that I did when I told them in 2009 that I used Twitter. "How can you support that libertarian bullshit?"

...

My reasons for being involved in cryptocurrencies are not based on sweeping visions nor utilitarian schemes. Even the most radical anarchist, in struggling against the appropriation of surplus value through the alienation of labor, is sometimes forced to move some commodities around in order to live in this world. "Master's house" and "master's tools" notwithstanding, the rent is due. The only alternative is heading off into the hills, or living the life of a begging monk. You need to take part in the larger economy of the world in order to survive, and so you are forced to participate in that system. You buy your groceries in the United States in USD because you are paid in USD. Your political views are not decided when you are forced into a market.

The same thing goes for voluntary markets; joining a market is not a politics. Just as buying groceries with dead presidents doesn't invalidate your radical ideas, downloading a cryptocurrency wallet does not transform you into a seasteading libertarian. The decision to participate in Bitcoin, in other words, means less than your conduct within the bitcoin market. To be truly anti-capitalist, one must understand the range of markets that exist, so that one can choose the right

behavior in any of them. The right behavior can only be a choice within the conditions of the market.

Cryptocurrencies are not a market that anyone is currently forced into. (The rent is still due in dollars, not Dogecoin.) It is a sideline deal, like a timebank, or a regular poker game. People make weird deals all the time, but a weird deal does not a currency make. In this era of late capitalism, tangential, voluntary-markets are proliferating—thanks in no small part to the technology which makes many of them possible.

But this phenomenon is not strictly an effect of digital technology. Bartering, for example, is a voluntary market that has co-existed with capitalism for hundreds of years. Or consider this: People use Tide laundry detergent as drug currency. It is relatively expensive, not too hard to shoplift. Combine the high value of the brand name with relatively low margins made by the retailers, and you get a burgeoning grey market in which small shopkeepers don't think too hard about buying a discount load of washing detergent bottles out of the back of someone's trunk for cash. Who is conducting unethical behavior in the context of this market? The drug users looking to get a quick five bucks? The retailers who are just trying to make a profit running a store? The customers who are so loyal to the brand that they'll pay inflated prices? Or Procter & Gamble, who in 1946 invented alkylbenzene sulfonates so good at washing clothes in a gentle machine, completely changing the way that we do laundry? This is how markets

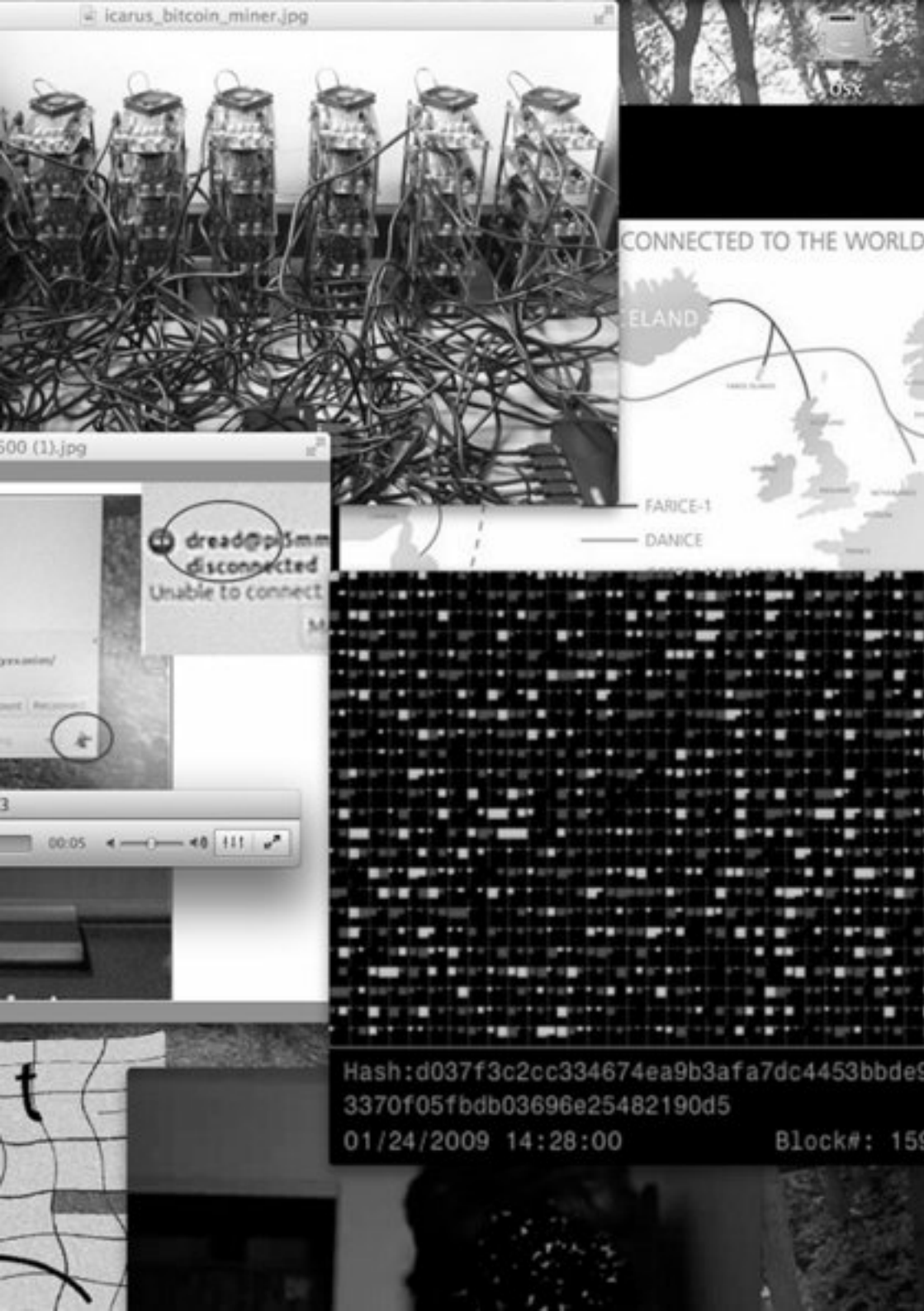
develop—through the accretion of many individual decisions, some borne of greed, others of necessity, others of sheer invention. If there is some transformative social potential in cryptocurrency, it will emerge from a collusion of behaviors occurring under unique conditions, in the context of experimentation and risk.

For now, this is a speculative technology, and there is plenty of speculation. This is a most basic period of evolution, a time of big ideas and unbridled greed. Most of the aforementioned altcoins aren't even really planned, they are just cloned and released into the wild to see how they do with a little bit of extra marketing and a few tweaks to the block pattern. This is an Accelerando dimension, where you can make a new listing on a financial exchange by tweaking a few lines of code and uploading it to Github. Kanyecoin flopped, not just because of the legal pressure from the music star whose likeness it stole, but because someone got greedy and DDoS'ed all the smaller pools on the opening day, driving miners away to other coins. Dogecoin has survived, despite being birthed from a meme—because its large coin capacity and random block rewards that make it more fun to mine. The true Hobbesian SF fantasy is happening in the competition between altcoins, because nobody really knows what makes a good altcoin, until they see who emerges from the cryptocurrency mining Thunderdome.

The technology will continue to evolve, as people continue to

figure out exactly what it is for, what people will adopt, and what will make them money. To what extent will it produce collective, communal behavior, and to what extent will it merely reproduce the harsh logic of markets? Will cryptocurrencies end up being peer-to-peer in any more significant way than a drug market or a stock market? These questions are still unanswered in a satisfactory way.

The beta release rolls onward, as the human species continues to see what it can do with all of this wonderful technology it has created, mostly as it tries to make a buck off of its fellows. This is evolution, I guess. Not of human beings, who actually trend towards altruism and organization. But of technology, which is always adopted first and foremost by those who are attempting to leverage gain out of it. Can we make it a business? Can we make it a weapon? Can we convince others it is a business or a weapon, by investing our accumulated capital in it, to accumulate more capital? This is capitalism's eternal demand, the logic of capitalism. Technology, on the other hand, whether attempting to replace the current means of currency, transportation, or communication, is a tool, neither good nor bad, and certainly not neutral. We use it, but it also changes us as individuals and as a collectivity, and we probably will take a long time to understand how.


icarus_bitcoin_miner.jpg
CONNECTED TO THE WORLD
ELAND
FARICE-1
DANICE
Unable to connect
Hash:d037f3c2cc334674ea9b3afa7dc4453bbde
3370f05fbdb03696e25482190d5
01/24/2009 14:28:00
Block#:

A Shining Beacon
Dread Pirate Roberts
Silk Road Forums 20.03.2012

Hey gang,

I read more than I post in the forum, and my posts are rarely of a personal nature. For some reason the mood struck me just now to put the revolution down for a minute and just express a few things. There is a curtain of anonymity and secrecy that covers everything that goes on behind the scenes here. It is often fast paced and stressful behind this curtain and I rarely lift my head long enough to take in just how amazing all of this is. But when I do I am filled with inspiration and hope for the future. Here's a little story about what inspires me:

For years I was frustrated and defeated by what seemed to be insurmountable barriers between the world today and the world I wanted. I searched long and hard for the truth about what is right and wrong and good for humanity. I argued with, learned from, and read the works of brilliant people in search of the truth. It's a damn hard thing to do too with all of the misinformation and distractions in the sea of opinion we live in. But eventually I found something I could agree with whole heartedly. Something that made sense, was simple, elegant and consistent in all cases. I'm talking about the Austrian Economic theory, voluntaryism, anarcho-capitalism, agorism etc. espoused by the likes of Mises and Rothbard before their deaths, and Salerno and Rockwell today.

From their works, I understood the mechanics of liberty, and the effects of tyranny. But such vision was a curse. Everywhere

I looked I saw the State, and the horrible withering effects it had on the human spirit. It was horribly depressing. Like waking from a restless dream to find yourself in a cage with no way out. But I also saw free spirits trying to break free of their chains, doing everything they could to serve their fellow man and provide for themselves and their loved ones. I saw the magical and powerful wealth creating effect of the market, the way it fostered cooperation, civility and tolerance. How it made trading partners out of strangers or even enemies. How it coordinates the actions of every person on the planet in ways too complex for any one mind to fathom to produce an overflowing abundance of wealth, where nothing is wasted and where power and responsibility are directed to those most deserving and able. I saw a better way, but knew of no way to get there.

I read everything I could to deepen my understanding of economics and liberty, but it was all intellectual, there was no call to action except to tell the people around me what I had learned and hopefully get them to see the light. That was until I read “Alongside night” and the works of Samuel Edward Konkin III. At last the missing puzzle piece! All of the sudden it was so clear: every action you take outside the scope of government control strengthens the market and weakens the state. I saw how the state lives parasitically off the productive people of the world, and how quickly it would crumble if it didn’t have it’s tax revenues. No soldiers if you can’t pay them. No drug war without billions of dollars being siphoned off the

very people you are oppressing.

For the first time I saw the drug cartels and the dealers, and every person in the whole damn supply chain in a different light. Some, especially the cartels, are basically a defacto violent power hungry state, and surely would love nothing more than to take control of a national government, but you average joe pot dealer, who wouldn't hurt a fly, that guy became my hero. By making his living outside the purview of the state, he was depriving it of his precious life force, the product of his efforts. He was free. People like him, little by little, weakened the state and strengthened the market.

It wasn't long, maybe a year or two after this realization that the pieces started coming together for the Silk Road, and what a ride it has been. No longer do I feel ANY frustration. In fact I am at peace in the knowledge that every day I have more I can do to breath life into a truly revolutionary and free market than I have hours in the day. I walk tall, proud and free, knowing that the actions I take eat away at the infrastructure that keeps oppression alive.

We are like a little seed in a big jungle that has just broken the surface of the forest floor. It's a big scary jungle with lots of dangerous creatures, each honed by evolution to survive in the hostile environment known as human society. All manner of corporation, government agency, small family businesses, anything that can gain a foothold and survive. But the

environment is rapidly changing and the jungle has never seen a species quite like the Silk Road. You can see it, but you can't touch it. It is elusive, yet powerful, and we are evolving at a rapid clip, experimenting, trying to find sturdy ground we can put roots down in.

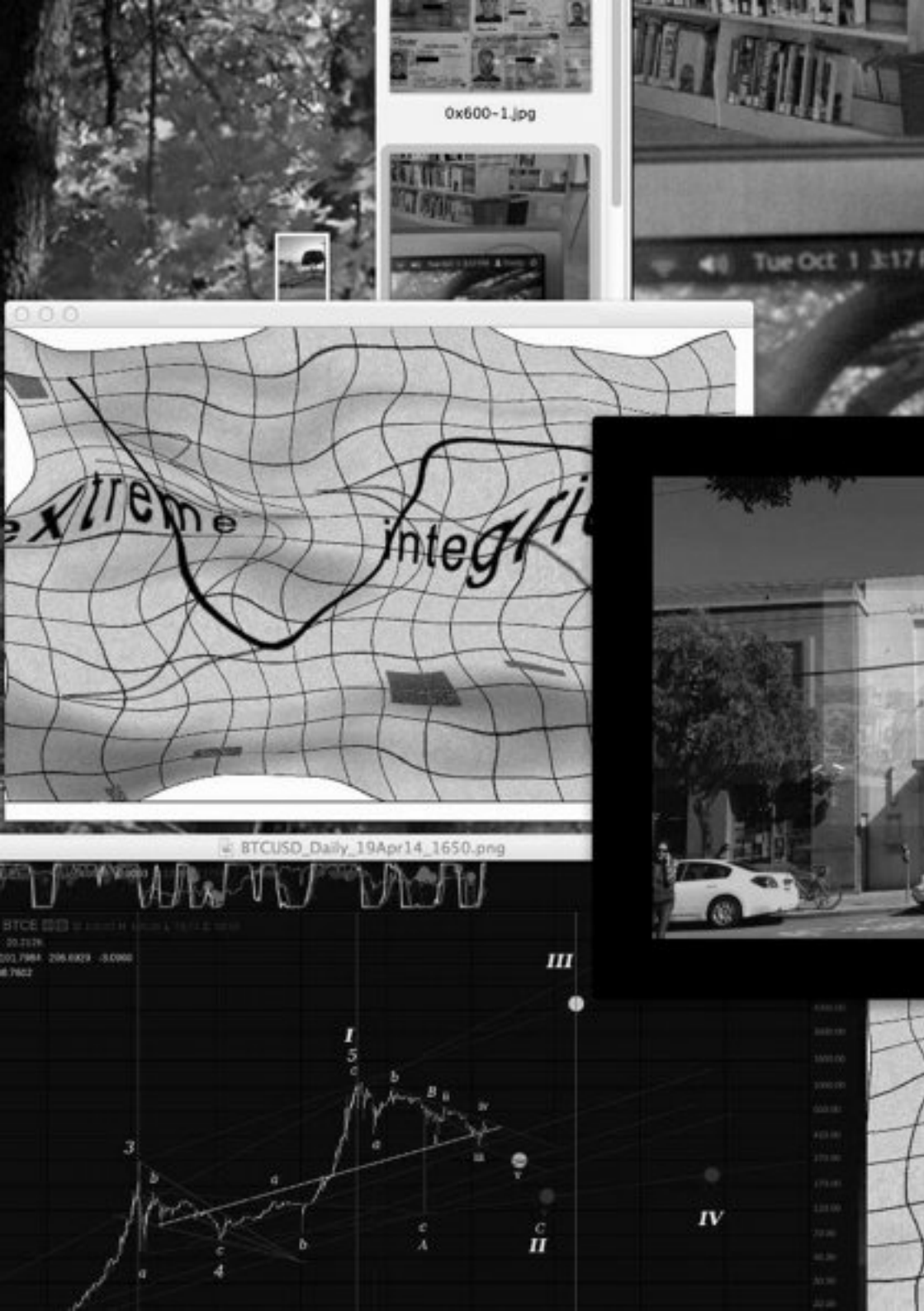
Will we and others like us someday grow to be tall hardwoods? Will we reshape the landscape of society as we know it? What if one day we had enough power to maintain a physical presence on the globe, where we shunned the parasites and upheld the rule of law, where the right to privacy and property was unquestioned and enshrined in the very structure of society. Where police are our servants and protectors beholden to their customers, the people. Where pace our leaders earn their power and responsibility in the harsh and unforgiving furnace of the free market and not from behind a gun, where the opportunities to create and enjoy wealth are as boundless as one's imagination.

Some day, we could be a shining beacon of hope for the oppressed people of the world just as so many oppressed and violated souls have found refuge here already. Will it happen overnight? No. Will it happen in a lifetime? I don't know. Is it worth fighting for until my last breath. Of course. Once you've seen what's possible, how can you do otherwise? How can you plug yourself into the tax eating, life sucking, violent, sadistic, war mongering, oppressive machine ever again? How can you kneel when you've felt the power of your own legs? Felt them

stretch and flex as you learn to walk and think as a free person? I would rather live my life in rags now than in golden chains. And now we can have both! Now it is profitable to throw off one's chains, with amazing crypto technology reducing the risk of doing so dramatically. How many niches have yet to be filled in the world of anonymous online markets? The opportunity to prosper and take part in a revolution of epic proportions is at our fingertips!

I have no one to share my thoughts with in physical space. Security does not permit it, so thanks for listening. I hope my words can be an inspiration just as I am given so much by everyone here.

Dread Pirate Roberts


0x600-1.jpg
Tue Oct 1
extreme
integri
BTCUSD_Daily_19Apr14_1650.png
III
I
5
3
4
II
IV

New Societies, Old Shells
Robert O'Brien

The following interview was conducted between the author, Luke Munn (LM) and Robert O'Brien (RO) on October 9, 2014 via Skype.

Identity Construction

LM: ...my thesis is around this notion of digital disembodiment, this 'always on' dematerialised self which circulates constantly on the network, the digital paradigms which pressure this identity to start expanding beyond the physical human form, in terms of capital but also socially, psychologically, etc.....

RO: There was quite an interesting situation a few months back of the notion of the digital self that continued on. It was this case in the States of a woman being found dead in her house, 2 years after the fact. And the reason is, she had set up all these digital payments and bills and they were continuing to be paid, and the only reason she was discovered was basically because the money had run out.

This is actually a really important concept, this notion of identity and there are two ways of looking at it. Our model in Western society in particular is that identity is actually constructed from the banking system. If you [personally] don't have a bank account, you have a significant other like a parent that proxies you. But if you don't have a bank account it's very difficult to operate. It's because they give us our identity, they construct our identity for us, at least in the economic sense. Obviously there is a social identity, the friends and families we

interact with on a daily basis, but for a lot of our stranger interactions, how it's formed, it's based on banks.

It's actually quite a significant thing. My friend's wife, who's Thai, she's this brilliant cook. She basically been a cook on street markets for all of her life. She wants to come to New Zealand but she can't because all those street markets are cash businesses. They don't exist within the banking system, so they don't formally exist, so therefore she's got no formal record of her employment that is recognized and therefore cannot apply for residency in New Zealand.

So there's that social construction, then an economic construction, which has been going for a long time and - as you pointed out - we now have this digital construction that can actually live - as in the case of that American woman - in its own right for a long time. And there's no reason why that couldn't technically exist for a lot longer. And that segues into ideas of Bitcoin in particular.

The interesting thing with regards to Bitcoin is that a bit of software cannot go and open a bank account, it cannot have an identity within our existing economic systems. But a Bitcoin piece of software can open a Bitcoin account and therefore construct its own digitally native identity in its own right.

What you're doing is essentially giving identity to some notion of algorithm. It's got a plastic structure to it, though it changes

and evolves over time, much as we do. We change pretty much everyday but our identity carries through. So now you have a digital version of that, with these algorithms and whatever medium they exist in - whether a car or a sensor device on the wall - there's no reason why that algorithm can't move about, can't do things. This challenges the notion of what is ownership. If an algorithm in its own right can have some sort of economic identity, which it can then use to construct a social identity - albeit always in the digital realm - but in the case of the self driving car it also means it has a physical manifestation in the sense of that particular medium. There's some interesting technical aspects within Bitcoin that makes that quite doable on a broader scale, beyond just opening up your own Bitcoin address or account.

Beginnings and Blinding

Bitcoin hasn't come out of nowhere. A lot of the discussions to replicate cash in the digital environment came out of the cypherpunk movement. That's where Julian Assange and all the rest came from. There's really two aspects to it. The notion of anarchism, where we're getting a flat society where we don't have the leviathan, the legitimate force, everyone is just working in this cooperate egalitarian society. Then there's this notion of anarcho capitalism, which is that we can have these purely competitive free markets with no government interference. There's two different things but they tend to conflate. That was what a lot of cypherpunk was about, thats where a lot of the cryptography came from. So a lot of the

cryptography used in HTTPS was where a lot of this stuff was being discussed and used.

But prior to that, the real founder of digital cash is David Chaun. He's really the great grandfather of all of this in many respects. He was basically paranoid about privacy. He implemented or worked out how to do email privacy using a technique called blinding, which is a cryptographic technique. Bitcoin doesn't actually have blinding in it. You can think of this way. If you put a letter in an envelope and then give it to someone to stamp, but the impression of that stamp goes through to what's in the letter. So they can't actually see what they're stamping - they're only stamping the envelope. So then they hand you back the envelope with the stamp on it and you can take that out and take it to someone else and say 'Look, it was stamped by such and such so therefore must be legitimate'.

What that does is, that breaks a link. Citibank for example, know that I'm an employee but they don't need to see all the transactions that I'm doing. You just need to know that I'm employed by Citibank, but you don't need to know my name or credentials or any of that. That's your only criteria. That's what blinding does. So he [David] used that for email but then went on to use that for digital tokens.

David Chaun went on to form a company called Digicash but at that time Mastercard and Visa were also trying to do cash-like

digital tokens. So how that email stuff gets applied to digital tokens is this. If you're trying to replicate the operation of cash in digital form, you basically have to unlink it from where its been used and where it came from. The properties of cash are that it's anonymous. You don't need to know where that cash came from in order for me to buy a KG of Peruvian YKK. You just want to know that it's cash. You don't need to know anything about me, because all you're concerned about is the cash. Likewise I don't want to show my bank that I'm pulling out $USD 900 to pay for cocaine. So in that case I would want to get the digital token from my bank, but not show my bank what I'm spending that on. Likewise I don't want to give you information about where I got it from. You just need to know that its legitimate and hasn't been spent, those bits.

Double Spending and Identity Shifting

One of the important things about the internet and computing in general is that bits are copied. You cannot distinguish one bit or one byte from another. They're all the same. The internet is one big copying machine of bits. As a result, the real challenge is, "How do you prevent bits from being copied?" That's known as the double spending problem. It's not actually so much copied, they will be copied. The bigger question is, "How do you stop them from being renamed?" Taking on one identity and moving to another. And thats known as spending, renaming one thing to another.

Blinding did that with tokens. The big difference with the

Digicash system is that there had to be a central issuing authority. So to get that unlinkable property that also prevented renaming, you had to have a central service. That was how Digicash tried to solve the problem. What you've got here is a payment system which issues a token. When you need to spend it, you send the token back to the payment service, and the payment service creates a new 'coin' and passes it on to the person. But you had to have a central payment service to do that.

If you actually read through a number of the cypherpunk emails, they actually almost got Bitcoin decades ago, almost.

The big difference between Digicash and Bitcoin is that Bitcoin drops the unlinkability requirement. Instead it tries to put anonymous behaviour into the bitcoin addresses in the sense that they're pseudo anonymous. They can stay anonymous as long as you stay within the system, but as soon as you go out of that system they're no longer anonymous.

The other big difference with Bitcoin is that every transaction is linked. You can follow the complete providence chain. The history of every single transaction is there and public.
This blockchain is fully replicated. It's shared all around. So the ledger of spending is now shared by everyone. The blockchain is just divided up into this stratified structure. Satoshi basically brought all these components together.

As long as you stay within the system, then you were good, you could stay anonymous. But it's surprisingly hard to stay anonymous. So someone is going to know you somewhere. That was the downfall of things like Silk Road. Because it was centralized, it was easy to attack, despite the fact that it was using a decentralized anonymous payment system, because effectively they ran an escrow service.

LM: A tumbler [Bitcoin service used to disguise where coins come from] right?

RO: They didn't run any tumblers, it was literally escrow. Much like you do today, if you get cash out, like a $20 note, that's reserve bank money. As soon as you go deposit that into the Bank of New Zealand, you've now exchanged or converted that $20 note on par for a BNZ ledger entry. It's BNZs money, it's not yours. They're just giving you the right to access it. That's how they construct identity.

You might go to to an ATM machine and get it out and then you've converted it from BNZ money to reserve bank money. The fact that it's on par - that we call it 'the New Zealand dollar' - confuses the matter. A lot of people don't understand the difference. So effectively when you were going to Silk Road you were converting from Bitcoin to Silk Road coins. They operated their own internal credit system. You funded your balance, it was like a prepaid system. That's how the FBI for example were able to seize all those coins, because they were in a hot wallet

as part of the fund of the system. There was apparently a whole lot of other coins that had been put into cold storage and they can't track those down.

So typically when you provide some sort of prepaid service, you start operating treasury functions. That's the distinction between hot wallet and cold wallet. Any bank is what's called conditionally solvent. IF everyone didn't trust the BNZ anymore, and did a run on the bank, the bank would collapse if it didn't have any support structure around it, like taxpayers. They're always conditionally solvent. They're always trying to balance their capital ratios with their liquidity requirement, or what they think demand depositors will do. And the big reason for the global financial crisis is attributed to the fact that they were using off book mechanisms to fudge effectively their capital ratios. What they were doing is using derivatives, repurchase agreements which are typically still assets on book but they're not on your book. You can do fancy stuff with them. In which case the banks were saying to other banks and regulators, 'yeah we're meeting our capital requirements according to the laws and regulations', but in fact had all these underlying structures. So when the subprime stuff started coming, what happened was they were saying, 'We've been doing all this shadow banking, this off book stuff, to maximize our profits, so maybe all our counterparties are doing the same. If that's the case then we don't really know what their current standing is in terms of being solvent or not'. And of course as soon as you get that, you get a crisis of confidence.

And you see the same thing happening within the Bitcoin ecosystem, the velocity which happens all the time, so you can see that with Mt Gox...

LM: The collapse, the currency speculation and these wild fluctuations...

RO: Yeah, so the price speculation reflects the general market. The price of Bitcoin is [based on the fact] that a lot of speculators have no clue what's going on. So you'll get governance bumps and crises of confidence all the time, because that's true in any highly competitive environment. There's this notion within capitalism - a fiction if you like - that capitalists like free markets. They don't. Capitalists prefer monopolies. If you can get a monopoly you can extract massive profits. If you have a true functioning free market, there's practically no profit. Too competitive a market, there's no profit. The maximal capitalist that we're told is the engine of our economy in classical economics, is actually not at all. They're basically dictatorial, they want a monopoly. The true free market is too competitive to enable cooperation to form. That's an important point.

Bitcoin is a good example of all of that, whereby if you're an extremely anarcho capitalist society, where competition and individual property rights rule the world, you'll find that basically you end up with a society like Somalia. And the sort of question that arises is what are the new institutional forms

within such a society, that find a middle ground between the capitalist that wants complete monopoly and complete control, (i.e. a feudal society) versus this highly competitive “survival of the fittest but nobody can survive because everyone’s competing with each other” anarcho capitalism. So you’ve got to look at the new institutional forms, the rules and social norms that we live by to help us cooperate. And this ties very much into the notions of identity construction and identity economics. We can just look at our own notions of herd mentality, that notion that we are highly social animals, so therefore we tend to herd around people like us, groups like us.

So the question is, ‘How do we form groups?’ On one extreme we’ve got total state governance. You can think of Mao or Stalin as being the penultimate capitalist because they control everything. There’s really no difference between a capitalist and a full blown communist in that sense, no difference at all. Versus the American notion of libertarianism, where we’re all toting guns and shooting the shit out of each other. So those are your two polar opposites and somewhere in there is some middle ground.

New Institutions

There’s an area of economics that tends to get completely overlooked that’s known as institutional economics. It looks at how groups form. How do they cooperate and what’s actually going on here? It’s got a lot to do with trust. So one of the interesting aspects for me with Bitcoin is looking at the new

institutional forms. The institutions are the social norms, the rules we live by. A lot of people would call banks institutions, which they are, but institutions are a broader thing, they're how we come together to minimize risk. One of the key things about a highly competitive environment is that theoretically you and I would be completely rational, and we'd have perfect information. So we all have exactly the same information and we have this massive brain that lets us process that information instantaneously and we can make a rational choice based on maximizing our utility. That's an abstraction, a neoclassical abstraction, complete bullshit but a useful one in some areas.

Institutions come in because that world doesn't exist. We don't have perfect information. Information is completely asymmetrical. We don't have this über brain that can process every bit of information that comes through us, we ration. If you think of our brain as being some computer in its own right, it's got a ration where it pays attention. The way it rations things is by doing shortcuts, and one of the biggest shortcuts is group formation. I can trust you because you're like me. The more I interact with you, the more I can trust you and do things and take your opinion on board. And in turn that opinion is going to alter how I do things. So it's a shortcut, it's a way of dealing with a lack of information and the ability to process the information that we do have. And thats what social norms do, that's what institutions do. We trust our bank that they will pay our money back, for example.

So the question with Bitcoin is, 'What are the new institutions that are forming?' Silk Road is really interesting from that point of view. Was Silk Road - or is Silk Road today, the new manifestations of it - a new institutional form? Here's an anarcho capitalist system trying to run inside a capitalist system, doing something that the outer shell doesn't like you doing, i.e. buying drugs anonymously and then selling them. So how the hell does something like that exist? How do people learn to cooperate in that environment? Bitcoin wasn't necessarily playing a role in the marketplace, per se, because we were dealing with Silk Road credits. Bitcoin was the way to pay in and fund my account, and then if I was selling the drugs, I could then take it out as Bitcoin, so it gave me a degree of liquidity. But within the marketplace, how did that come about? How did trust and group formation occur?

This is pretty much what DPR was doing, if you look at his forum posts, his writings. [There are] various discussions about American libertarianism, which is quite different from the classical notions of libertarianism, two quite different things. In those channels, in those forums, there was a lot of conversation repeating much of the ideals of the cypherpunk movement. And it's through those conversations that people were forming groups. That's how they were building their trust in that marketplace, and that was very evident in the conversations, developing social norms - what good and bad practice was. All this, despite the fact that, if I bought drugs off you and you didn't deliver them, it's not like I could ring up the police and

get the government to do some legitimate force on you, knock on your door and arrest you for fraud - I couldn't do that. So how does a society like Silk Road exist as this anarcho capitalist enclave in a broader system? How does it develop these institutional norms? A lot of these themes were coming through conversations in forums, and you see that pattern repeated in a lot of digital forums. How do these groups form? 4Chan is classic for that. Whether the conversation is just pictures of naked celebrities, a culture develops around those exchanges even in an anonymous environment, and you saw the same thing happening with Silk Road. Because the question was not only, 'What happens if you don't deliver the drugs?', the question also was, 'What happens if DPR takes off with all the coins?' He could have done that at any time, but he didn't. It could have been rather profitable and better for him if he just took off with all the coins but he didn't.

And you see that kind of pattern, that odd notion of trust - occurring over and over again within Bitcoin services. So look at Mt Gox, where it came from. It bootstrapped off an existing community. You're familiar with that?

LM: With the marketplace but not the original community...

RO: Right, so Mt Gox stands for Magic The Gathering [Online] eXchange, an exchange for the trading of magic cards. They knew of a cheaper way to trade with cards, so Bitcoin came along and started using it, and then they became the exchange

for Bitcoin. They were one of the first ones to do that. But they were already starting out of a system. Not as extreme as Silk Road obviously, because if you didn't send me my cards, I could get theoretically get the police to knock on your door. That was relatively legitimate activity, but nonetheless there was a strong community that they were already part of, which was Magic the Gathering and the social norms that were around that, such that they could then bootstrap the trading side of things onto that.

It's really interesting to look at how these new institutional forms are developing in different ways. If you look at something like Coinbase, that's really just an escrow service. They put themselves across as a Bitcoin wallet service, but really they're doing the same sort of treasury functions, cold wallet storage, and credit liquidity of a bank. They are closer to a traditional bank than say, Silk Road, which was doing something else and constructing these new forms.

You see the same thing with online gambling. When Satoshi Dice came out, you could see all the discussions around whether it was good for Satoshi Dice to be doing all these transactions on the blockchain as opposed to being a central marketplace. So there's always this tradeoff between centralization versus decentralization. Alexander Galloway discusses this in his book, Protocol. He's looking at Foucault, philosophy, critical media and in this particular case, how control comes out of decentralized protocols. How does control

exert itself, and in what way? He's looking at DNS and HTTP but a lot of his work could fit with Bitcoin just as easily.

[Note: from this point, the interview shifts to more directed questions and is based on notes rather than direct transcription]

LM: From the Bitcoin workshop notes I noticed a lot of the suggestions you received were around the relationship between cryptocurrency and the government. On the one hand people were wanting more government support for Bitcoin, but on the other minimal regulation or interference.

RO: I've run a number of those workshops throughout the country now, and I try to leave my opinion out of it. Each workshop is autonomous, the notes from the previous workshops aren't shared. So what happens is that you tend to get the same ideas coming through over and over again. Most people view Bitcoin as money, as something new, a novel technology useful mainly for financial gain, and so there's not a lot of deeper thinking around some of these issues. For me, money is an information system, but for some of these participants, Bitcoin is a way to dismantle state infrastructures and replace them with individuals operating in purely free markets….

LM: Agorism….

RO: Right, and it's interesting that in the US, industry is trusted

more than the government, whereas here in New Zealand, government is trusted more than industry. Although based on the last election, we'll have to see if that still stands up.

LM: Bitcoin rose up out of this software developer scene and then, with the publishing of the Gawker article on Silk Road, was continually aligned with some of these 'illegitimate' spaces. So Bitcoin has this connection to very specific niche communities, do you see an image problem there?

RO: Well cryptocurrency emerged from this niche scene, a certain type of software developer with a specific political ideology, the so called 'greybeards', or 'neckbeards', with these intense discussions around cryptographic techniques. So that was always going to be something that mainstream developers didn't touch. I've followed a lot of these conversations and are very familiar with the ideas, so for myself coming from a distributed computing background, Bitcoin's jump into the mainstream was very surprising. One of the key things here is that there are specific incentives of the system which are perfectly aligned for greed. That especially in the early days, you could make up a mining kit, speculate on the future value - these were qualities that broadened the audience beyond the niche communities interested in digital currency. And the fact you could buy real things, that if you have some of these ideologies, perhaps you're more inclined to recreational drug use. That if you're a white male developing software all day on a computer, chances are you might be into porn. So Bitcoin had

a distinct use value. And there's a natural connection here, because these illegitimate industries are already marginalized by the existing banking system, so they're going to jump on board.

LM: So is anonymity hindering more of a mainstream uptake? Is this anonymity, or really pseudo anonymity, still necessary for Bitcoin?

RO: I don't think it's hindering any public uptake because the public really doesn't care about privacy. They still don't really understand the power of algorithms to uncover private information. You mentioned the Gawker article on the Silk Road, and that was a really important moment that brought Bitcoin into the public consciousness, but also conjured up this myth of total anonymity. Being pseudo anonymous isn't the same as being truly anonymous, but most people don't understand the difference. But that combination of Silk Road with Gawker was significant. Up until that point Bitcoin was trading at around $7 USD I think, and after it jumped up to more than $30 USD. And that started this tidal wave of articles where the two were always linked, the Silk Road and Bitcoin, the Silk Road and Bitcoin. There was a lot of shock or superficial journalism, focusing on the fact you could obtain drugs or porn. But I don't think governments actually care that their currencies are being used to purchase these things. Why does the European Union, for example, print 500 EUR notes? You can fit 100 million Euro in a briefcase. And cash is very

good at that unlinking. You don't care where it came from, only that it's legitimate, as I mentioned before. So in some ways, it's still much easier to purchase your drugs via the major financial hubs, like New York or London.

And the technology media has largely equated Bitcoin with money, or misunderstood it. It's only very recently - I'm talking about the beginning of this year - that they've begun to focus more on the blockchain and the possibilities within that.

LM: That brings us nicely to the last question I had for you. Where do you think Bitcoin is headed in the next few years, the next 5 or 10 years?

RO: There's this notion of the semantic web coined by Tim Berners-Lee, and I see cryptocurrencies - of which Bitcoin is the poster child - creating what I've called the computational web, combining the blockchain with the transactional model inherent to cryptocurrency to produce a new type of web. Bitcoin has been called 'the internet of money', and that's true but only really part of it. That ignores what Bitcoin really does, which is to prevent bits from being renamed. Add that to this decentralized line of providence and you start to envision a new web. It becomes something like a 'blackboard' [artificial intelligence application based on the blackboard architectural model], a coordination space that tracks what you're putting in. So for me, the blockchain is a tuple space. Money in that sense is an information realm that helps us coordinate a range of

products, goods and services - I'll give you 1 New Zealand dollar for Widget A. So money really becomes a tool for coordinating activities. IBM has recently published an article along these lines, using Bitcoin for the Internet of Things as a mechanism for enabling machine to machine communication, social networking and decentralization. There's a kind of natural evolution or progression to all of this. We always start with centralization because it's easy. That's what gives us Facebook and the rest of these massively centralized walled gardens. For me, Bitcoin presents the opportunity to structure our systems more like the web, which is inherently generative in that anyone can create new pages, where a range of users and objects are contributing to this system, where computation is fundamental to its design.

There's an important difference between the two though. With the web, the authority in terms of verifying and regulating information is the server. With Bitcoin, authority resides in the blockchain. With Bitcoin, the content or webpage equivalent are all coming out of this shared resource. In that sense, blockchain has the ability to provide a coordination system. You could have a light in your house, for example, which receives a transaction, remembers that it's last state was off, so then switches on. In the same way, you could have a range of lights listening for transactions to other objects, so that when you open the door, they turn on. You've setup a shared space allowing asynchronous conversations with your light bulbs.

Bitcoin is also interesting for this ability to provide verified information, as a catalyst for building interesting trust relationships, for the fact that the computation required to minimize risk is reduced. Tim Berners Lee, in ‘Weaving the Web’, talks about how the internet is entirely dependent on this tightly coded set of relationships, the DNS system is the “one centralized Achilles’ heel by which [the web] can all be brought down or controlled”. From a software development point of view, this is a very brittle infrastructure. Every time something changes, you need to update, to reconfigure, to prevent everything breaking. The blockchain instead offers this loosely coupled approach, where objects are able to evolve and change over time.

About the Contributors:

Adam Rothstein is an interdisciplinary artist and freelance writer
poszu.com

Ludwig von Mises was a philosopher, Austrian School economist, sociologist, and classical liberal
mises.org

The Wine and Cheese appreciation Society of Greater London is part of the Junge Linke gegen Kapital und Nation network
junge-linke.org/en

Scott Lenney writes about culture and politics
metamute.org

Dread Pirate Roberts is the online pseudonym of the owner(s) and manager(s) of the former online marketplace Silk Road

Alex Payne is a programmer, writer, and occasional angel investor
al3x.net

Robert O'Brien works on identity, privacy, reputation and money in pervasive computing markets
outofrhythm.com