There is nothing novel in the world apart from the history you don't know.

Robinson Dorion

JWRD Computing, TMSR OS
WoT : dorion, 54CCA1FC8C2E414C63BFB6CF0E48266E54D6B95A

dorion-mode.com , *office@rh3torica.com*

February 13, 2020

Overview

1. Genesis
2. Post-Satoshi
3. Wall Street Enters Bitcoin

Why discuss the history of Bitcoin ?

While Bitcoin is a Peer to Peer cash system, with no trusted third party or central authority, no trusted third party does not mean Bitcoin is not trustless. Commerce and finance are based on trust.

J.P. Morgan on Finance

Untermyer: "Is not commercial credit based primarily upon money or property?"
Morgan: "No sir. The first thing is character."
Untermyer: "Before money or property?"
Morgan: "Before money or property or anything else. Money cannot buy it...because a man I do not trust could not get money from me on all the bonds in Christendom."

- People are individuals, they're not equal.
- The Bitcoin Rule : He who has the money and credibility makes the rules.
- Three threads to weave : the history of Bitcoin development, finance and politics.

Birth and Infancy

- October 31, 2008 : Satoshi releases the whitepaper.
- November 16, 2008 : Satoshi publishes source code.
- January 3, 2009 : The genesis block is mined.
- January 9, 2009 : bitcoin-0.1.0 is published, executable only on Windows.
- 2008-2009 communications : metzdowd.com cryptography mailing list, sourceforge.com bitcoin-list and forum/message board are primary communication channels.
- November 22, 2009 : Satoshi makes first post on bitcoin.org.
- December 17, 2009 : bitcoin-0.2 released, Martii Malmi (sirius-m) ports to Linux
- July 6, 2010 :, Version 0.3 released, daemon and cli version included.

Undefined Behavior: Overflow Bug

CVE-2010-5139

- On August 15 2010, it was discovered that block 74638 contained a transaction that created 184,467,440,737.09551616 bitcoins for three different addresses.
- This was possible because the code used for checking transactions before including them in a block didn't account for the case of outputs so large that they overflowed when summed.
- A new version of the client was published within five hours of the discovery that contained a soft forking change to the consensus rules that rejected output value overflow transactions
- The block chain was forked.
- Although many unpatched nodes continued to build on the "bad" block chain, the "good" block chain overtook it at a block height of 74691 at which point all nodes accepted the "good" block chain as the authoritative source of Bitcoin transaction history.

Forks Authorized by Satoshi

semantic version number	Software release	Change type	Reason
0.1.0	wxBitcoin 0.1.0	original	
0.1.1	wxBitcoin 0.3.1	softfork	mostly-redundant 1 MB block size limit
0.1.2	wxBitcoin 0.3.5	softfork	fixes CVE-2010-5141
0.1.3	wxBitcoin 0.3.6	softfork	OP_NOPs made explicit
0.2.0	wxBitcoin 0.3.7	hardfork	scriptSig + scriptPubKey evaluations separated
0.2.1	wxBitcoin 0.3.10	softfork	fixes CVE-2010-5137 and CVE-2010-5139
0.2.2	wxBitcoin 0.3.12	softfork	fixes CVE-2010-5138

Source: `https://en.bitcoin.it/wiki/Consensus_versions`

Satoshi's public communications cease in December 2010, around the release of bitcoin-0.3.19

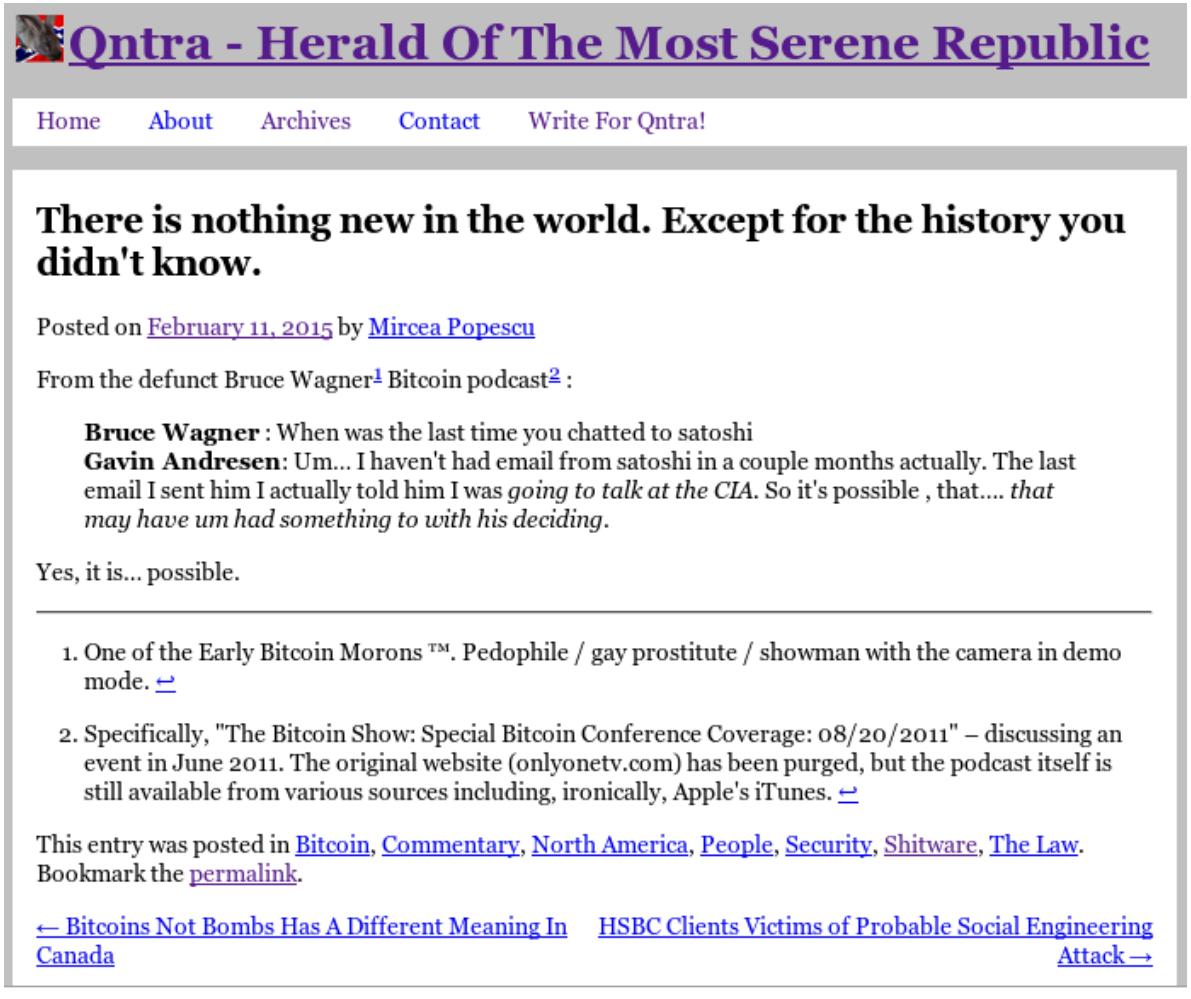
Overview

1. Genesis
2. Post-Satoshi
3. Wall Street Enters Bitcoin

Gavin Andresen's shady history, Act 1

April 2011 : Gavin Andresen (WoT: gavinandresen) announces on bitcointalk (archive) he'll visit the CIA for $3k to talk about Bitcoin. Satoshi cuts off communications with Gavin.

In Gavin's Own Words



Qntra - Herald Of The Most Serene Republic

Home About Archives Contact Write For Qntra!

There is nothing new in the world. Except for the history you didn't know.

Posted on February 11, 2015 by Mircea Popescu

From the defunct Bruce Wagner[1] Bitcoin podcast[2] :

> **Bruce Wagner** : When was the last time you chatted to satoshi
> **Gavin Andresen**: Um... I haven't had email from satoshi in a couple months actually. The last email I sent him I actually told him I was *going to talk at the CIA*. So it's possible , that.... *that may have um had something to with his deciding*.

Yes, it is... possible.

---

1. One of the Early Bitcoin Morons ™. Pedophile / gay prostitute / showman with the camera in demo mode. ↩
2. Specifically, "The Bitcoin Show: Special Bitcoin Conference Coverage: 08/20/2011" – discussing an event in June 2011. The original website (onlyonetv.com) has been purged, but the podcast itself is still available from various sources including, ironically, Apple's iTunes. ↩

This entry was posted in Bitcoin, Commentary, North America, People, Security, Shitware, The Law. Bookmark the permalink.

← Bitcoins Not Bombs Has A Different Meaning In Canada

HSBC Clients Victims of Probable Social Engineering Attack →

Bitcoin Finance : The Web of Trust

November 2010, Daniel Folkinshteyn (WoT: nanotube) starts the Bitcoin OTC Web of Trust.

- WoT viewer and wiki at `bitcoin-otc.org`
- #bitcoin-otc on #freenode IRC network
- gribble is the bot that manages the WoT
- Associate a GPG key with IRC nick as identity
- GPG contracts are best practice.
  `https://wiki.bitcoin-otc.com/wiki/GPG_Contract`
- Reputation accumulates with activity.

Mt. Gox 2010-2011

- Launched in 2007, Magic: The Gathering Online eXchange adds support for Bitcoin trading in July 2010.
- Original owner was Jeb McCaleb. He supported Bitcoin trading to trade his own Bitcoin, i.e. self-trading from day one.
- McCaleb was a U.S. citizen, sold Mt. Gox to Mark Karpeles (WoT : magicaltux) in March 2011 over legal concerns.
- June 19, 2011: Database hacked, login + password combos offered for sale, Mt. Gox denied hack.
- Dispute between Karpeles and McCaleb due to former not paying the latter.
- "Somebody" gains account with 400,000 BTC (10% of BTC in circulation at the time). Pushes Mt. Gox price down to $0.01 because withdrawal limits are USD based and withdraws "worthless" BTC.
- July 2011: bitomat.pl suffers 17k BTC loss after storing wallet on ramdisk. Mt. Gox acquires and makes customer's whole.
- October 28, 2011: hacked for 3k BTC, made customer's whole.

June 2011-December 2012 Bitcoin Drama Timeline

- 1.296 million BTC defrauded, stolen, hacked, ponzi'd, disappeared via various GLBSE assets and GLBSE (nefario, theymos) itself, Bitcoin Savings and Trust (pirate40), Mt. Gox, mybitcoin.com, bitcoin7.com, Bitcoinica, BTC-e, Tradehill, silkroad, bitfloor, Butterfly Labs (luke-jr), mybitcointrade.com, Bitcoin Magazine. Source: `http://trilema.com/2012/the-bitcoin-drama-timeline/`
- Many of these scams were pushed on `bitcointalk.org`. Hannah Wiggins (WoT: hanbot), a.k.a. MPOE-PR, lead much of the proactive criticisms of the unsustainability/demonstrated incompetence of many asset issuers. Some listened, most didn't. See her anthology for details : `http://trilema.com/2013/mpoe-pr-almost-two-years-in-the-swamp-an-anthology/`

Overview

1. Genesis
2. Post-Satoshi
3. Wall Street Enters Bitcoin

MPOE/MPEx 2011-2012

- July 22, 2011, Mircea Popescu registers in WoT
- August 2011, Mircea Popescu Options Emporium starts trading
- February 2012, S.MPOE IPO is announced, listed on MPEx
- August 2012, Satoshi Dice (S.DICE), owned by Erik Voorhees (WoT: evoorhees) is listed on MPEx

Select 2012 Bitcoin articles on Trilema by Mircea Popescu :

- The problem with PMBs, i.e. "Perpetual Mining Bonds"
- The reasons why Bitcoin securities can't be regulated by the SEC
- The politics of Bitcoin
  - Delineates fiat business exploiting bitcoin for fiat and Bitcoin businesses insulated from fiat.
- GPG contracts
- Bitcoin and the Poor
  - Why Bitcoin being elitist and capitalist is why Bitcoin is important. Bitcoin is fate. Do the right thing, you're part of it. Do the wrong thing, you're fucked. Amor fati.
- Let's dig a little deeper into this entire deflation "problem"
- MPEx ROTA

2012 IRC and WoT schism

- April 2012, Greg Maxwell (WoT : gmaxwell) attempts to censor Mircea Popescu (WoT : mircea_popescu) in #bitcoin-otc
- MP - and others in favor of freedom - move to #bitcoin-assets, owned by (kakobrekla).
- nanotube ghosts and WoT moves from being managed by gribble to assbot (kakobrekla).

Sources:
`http://trilema.com/2013/the-froth-of-our-days/` , `http://trilema.com/2014/a-little-bit-of-bitcoin-history/` , `http://trilema.com/2016/how-bitcoin-assets-was-born/`

Doomed Bitcoin Foundation

- Peter Vessenes establishes the self-proclaimed Bitcoin Foundation as his Coinlab venture fails.
- Sells membership for Bitcoin "donations".
- Promotes Butter Fly Labs, Mt. Gox, etc.
- Roger Ver (WoT : nonperson) , Mark Karpeles, Charlie Shrem (WoT : nonperson) are among founders and board members.
- Gavin Andresen and other coders associate themselves with this organization and begin drawing 6 figure USD salaries.

Development Devolves From Bad to Worse

- By 2013, more code and complexity had been layered onto the already shoddy codebase, e.g. the "anyone can spend" multisig softfork introduced in version 0.6 on April 1st, 2012 (Block #173805).
- For many years, calls for bug fixes and a protocol specification were ignored by the self proclaimed developers.
- "The code is the spec."
- Satoshi was an inventor, not a master programmer - he used Windows, after all.
- March 1, 2013 : MP pens "Bitcoind : not quite ready for prime time." documenting the deficiencies in the transaction creation code of the bitcoind wallet.
- March 11, 2013 : lead by Gavin Andresen, a second database, LevelDB, a Google technology, was introduced to version 0.8, while at the same time the blocksize limit was raised. Many people had stayed on the older versions and a massive fork emerged that nearly killed Bitcoin.
- July 2013, Gavin proposes introducing multisig and two factor authentication to Bitcoin transaction signing, MP pens "And Gavin moves on to the dark side. The Bitcoin project is officially hijacked."
- "Core Devs" attempt, but fail to merge PKI into Bitcoin, heartbleed SSL vulnerability exposed in 2014. If "Core Devs" were successful, private keys on nodes would've been readable.
- November 2014, luke-jr caught blacklisting s.dice and other gambling sites as default in the Gentoo Linux package of Bitcoin.

Trilema Technology

- January 21, 2013, Mircea Popescu publishes Why I nixed p2p, colored coins and all that jazz explaining why "decentralized" exchanges are not practical technically nor financially. Coder's prefer to "solve problems" in front of machine that don't exist that speak with people.
- February 2, 2013, Mircea Popescu publishes and overview of how MPEx architecture remains robust to attacks, from using multiple proxies to mitigate ddos to using GPG for authentication and privacy - rather than the ubiquitous PKI.
- October 13 2013, Mircea Popescu publishes : How to air gap. A practical guide.
- October 16, 2013 Mircea Popescu publishes : Things that matter these days ; things that don't matter these days documenting how Bitcoin network is doing more computing than any other human activity.
- October 19, 2013 : No Such IAbs (S.NSA) launches Phuctor, the RSA supercollider
- August 16th, 2014 : Mircea Popescu published The woes of Altcoin, or why there is no such thing as "cryptocurrencies" explaining how, in principle and demonstrable practice, weaker chains are vulnerable to hashing power attacks by larger chains. If a smaller chain hasn't been attacked yet it's because no one has cared enough to do it.

Bitcoin Finance

- January 2013, Matic Kocevar (kakobrekla) and Mircea Popescu partner to list BitBet (S.BBET) on MPEx
- April 3rd, 2013 : People! Bitcoin is not worth 100+ dollars per. STOP BUYING !
- April 8th, 2013 : Grave concerns re MtGox
  - "At this point I would advise anyone against keeping any sums on MtGox overnight, fiat or BTC."
- June 2013 : Mircea Popescu lists The Ministry of Games (S.MG) on MPEx
- July 2013 : Roger Ver publishes video of reading a statement from Mt. Gox office claiming Mt. Gox's issues are not caused by liquidity, but by mean banks. Andreas Antonopolous backs Roger's claim on Let's Talk Bitcoin.
- October 2013, Stanislav Datskovskiy (WoT: asciilifeform) and Mircea Popescu partner to list No Such IAbs (S.NSA) on MPEx
- October 2014, Jonathan Bahr (WoT: cazalla), Aaron Rogier (WoT : BingoBoingo)and Mircea Popescu list qntra.net (S.QNTR) on MPEx

Bitcoin Politics, 2013

Select Trilema articles:

- January 9, 2013 : Soft consensus, aka fecal matter. explains how 'consensus' is typically desired by the heard, who lack skin in the game and want something for free. People are only those with skin in the game, Bitcoin is for those with skin in the game.
- February 12, 2013 : Bitcoin prices, Bitcoin inflexibility
  - "Yet another one of them is that consumers revolt, entrepreneurs intervene, before the end of 2015 there's about a thousand to a million different Bitcoin forks, each with its ten million-ish monetary base worth about a dollar, on global average. The size of the inter-Bitcoins market, the complexity and confusion ensuing makes pretty much everything unmanageable for the "ordinary person"."
- February 16, 2013 : Bitcoin vs. Fiat a comparison explains that Bitcoin is winning and will continue to win because it best preserves property rights.
- November 23, 2013 : Bitcoin as replacement for the electoral system explains how Bitcoin lowers the cost of reducing moral hazard and thus is better positioned to self-regulate.

Bitcoin Politics, 2014, P1

- February 10, 2014 : The Most Serene Republic, and its laws.
- March 18th, 2014 : Interacting with fiat institutions, a guide. The SEC requests information on S.DICE listing, MP requires SEC to recognize Bitcoin as sovereign to continue discussion.
- April 2014, What the WoT is for, how it works and how to use it.
- April 2014, The sins of the group of posers behind the so called "Bitcoin Foundation"
- August 15, 2014 : La Serenissima and personal sovereignty
    - "La Serenissima does not recognise nor will ever enforce any sort of claim of any entity that purports to impinge on the sovereignty of persons. No entity may claim rights to person's identity under this rule, and if they try to they're being the enemy and should be treated like the enemy. For all intents and purposes identity is allodial property of the person therein represented, and no convention may touch it."

Bitcoin Politics, 2014, P2

- October 2014 : USGavin the lolcow makes the following points : Nobody has the authority to fork Bitcoin. If you're not in the WoT you don't exist. The poor have no say in money.
- November 4th, 2014 : The Bitcoin Foundation Incorporated with expressed objective to make a reference implementation by removing unnecessary code.
- November 4th, 2014 : The #bitcoin-assets deed system goes live.
  - Creates transactions that embed deeds into Bitcoin transactions. Uses block chain for time stamping mechanism.
  - Only accepts PGP signed material from the Bitcoin Lords.
- November 16, 2014 : Actual Bitcoin corporations (ABCs) versus fiat-based frauds trying to masquerade as Bitcoin companies (while masquerading as companies in the first place) on the solid theory that the general public is too stupid to make any difference, this one included, and on the flimsy theory that the general public matters in Bitcoin (FBF-TTMABC-WMACITFP-OTSTTTGPITSTMAD-TOI-AOTFTTTGPMIBs, alphabets for short). builds on the previous Politics of Bitcoin from 2012.