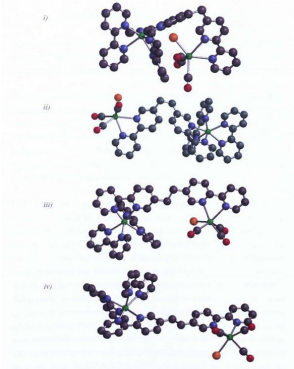
The Secret Lives of Cryptocurrencies:
Time Travel, Regulation, Whales & Refugees

Wassim Alsindi PhD

DIRECTOR OF RESEARCH
PARALLEL INDUSTRIES
WWW.PLLEL.COM // @PARALLELIND

LITTLE BIT ABOUT ME

SCIENCE KID



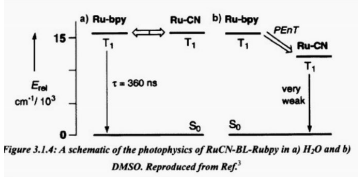


Figure 3.1.4: A schematic of the photophysics of RuCN-BL-Rubpy in a) H_2O and b) DMSO. Reproduced from Ref.[3]

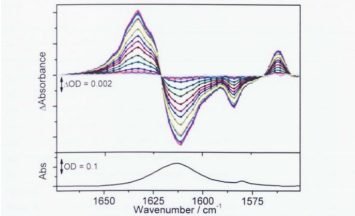
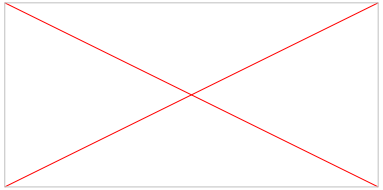
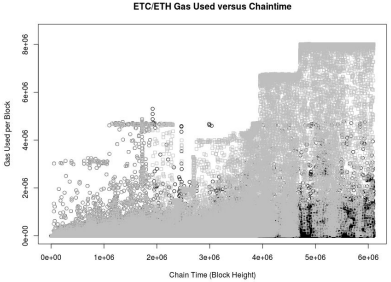


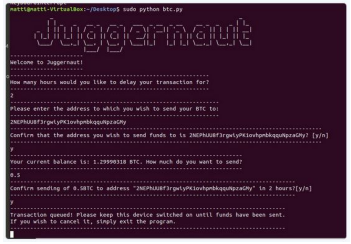
Figure 4.4.3.3: The FTIR (bottom) and ns-TRIR spectra between 1 and 750 ns (top) of RubpyamideBPM in D_2O solution.

EXPERIMENTAL ARTS

D-TECH RESEARCH
#ReachingEveryone
#Forkonomy
#TokenSpace







A Question or Two for You.

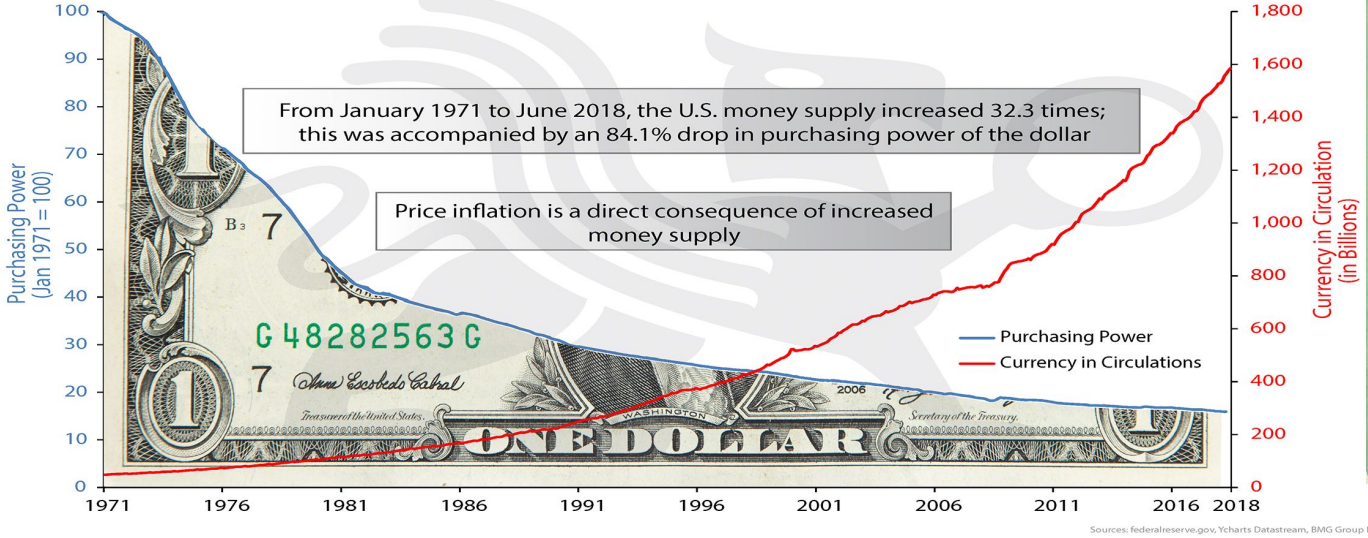
THESE THINGS...DO NOT SEEM TO BE RELATED :)

- Why does Cryptocurrency Matter?
  - Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

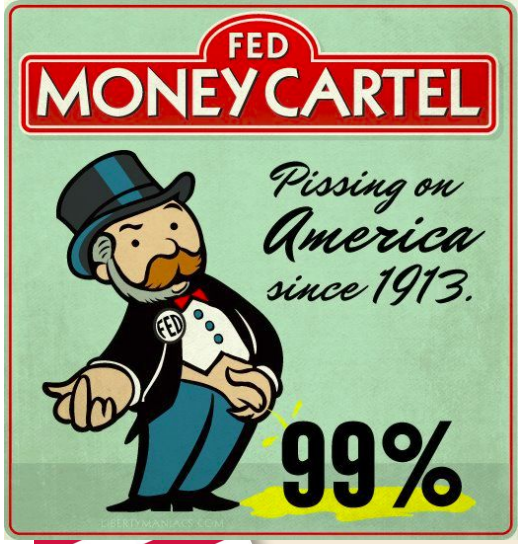
THESE THINGS...DO NOT SEEM TO BE RELATED :)

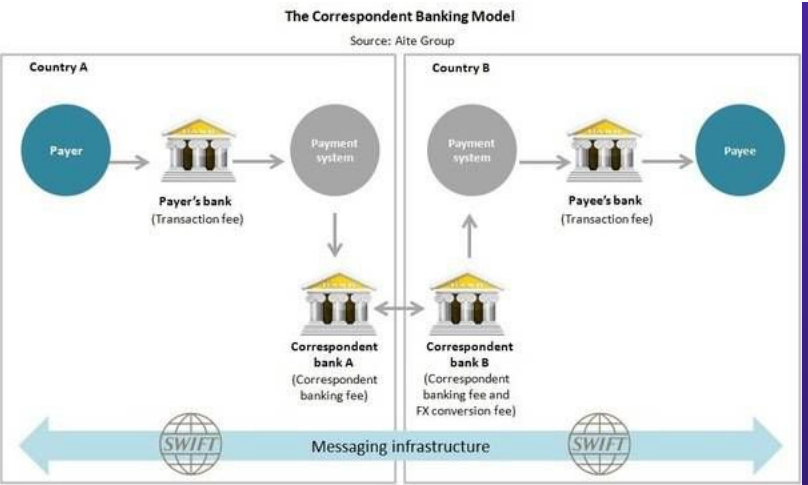
- Why does Cryptocurrency Matter?
  - Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

USD – Purchasing Power & Currency in Circulation



Sources: federalreserve.gov, Ycharts Datastream, BMG Group Inc.





BLOCKCHAIN TECHNOLOGY STACK

Application Layer

Acts as the User Interface that combines business logic and customer interactions.

dApp Browsers

Decentralized Applications

Application Hosting

Programming Languages

Services and Optional Components

Serves to enable application operations with a view to connecting with other technologies and platforms.

Data Feeds

Off-chain Computing

Governance/ DAOs

State Channels

Multi signatures

Oracles

Wallets

Digital Assets

Smart Contracts

Digital IDs

Protocol Layer

Decides the methods of consensus and network participation.

Consensus Algorithms

Side Chains

Permissioned and Permissionless

EVMs

Network Layer

Acts as a transportation medium and interface for the Peer-to-Peer network and decides how data is packetized, addressed, transmitted, routed and received.

RPLx

Roll Your Own

Block Delivery Networks

Trusted Execution Environment

Peer-to-Peer

Infrastructure Layer

In-house infrastructure or Blockchain as a Service (BaaS) to control the nodes.

Mining

Network

Virtualization

Nodes

Tokens

Storage

Social/Political:
Decision-making & interests arising from network participants

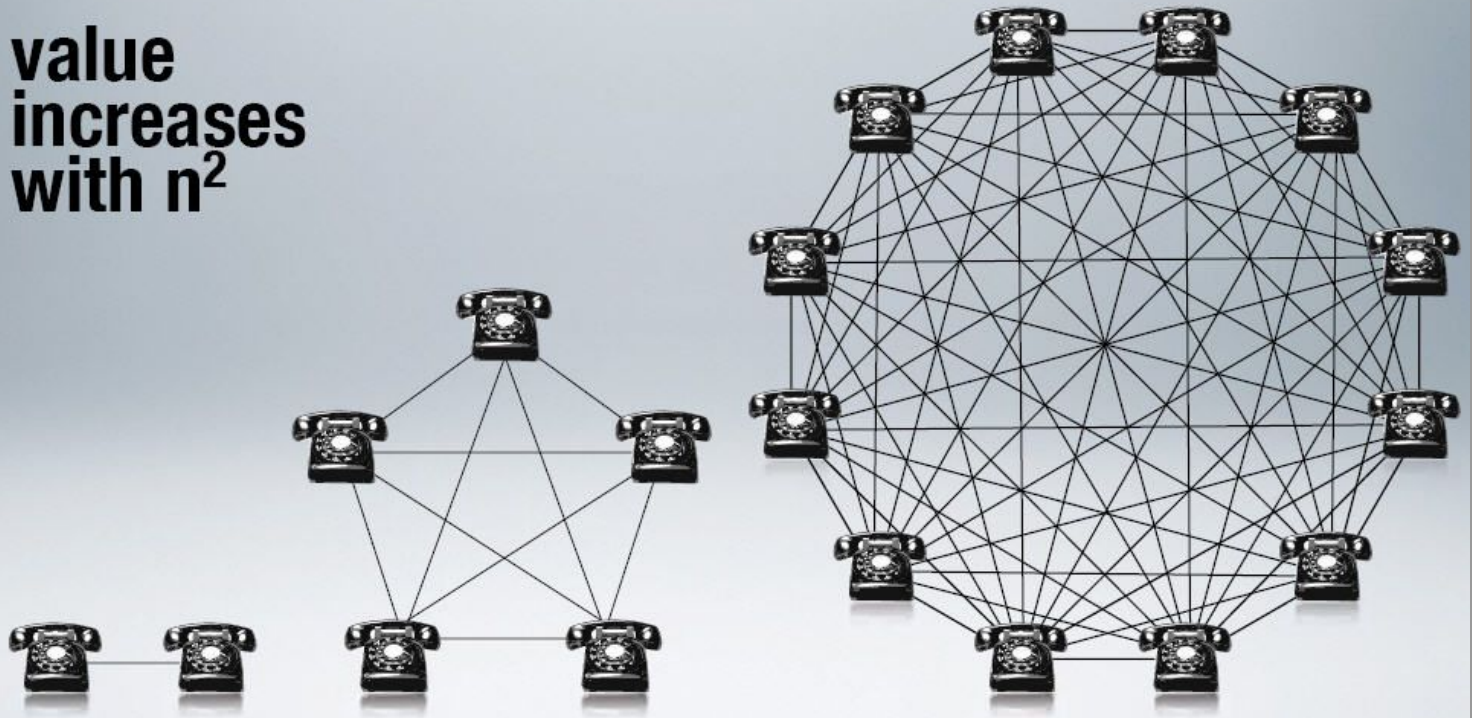
Monetary:
Transactions, addresses, incentives and issuance. Emergent economic characteristics within a value transfer system

Protocol:
Cryptographic primitives, software specifications, consensus rules & message broadcasting

Logical:
Data storage & structure. Redundancy, scalability externalities on infrastructure, reliance on central points of failure

METCALFE'S LAW

value increases with n^2



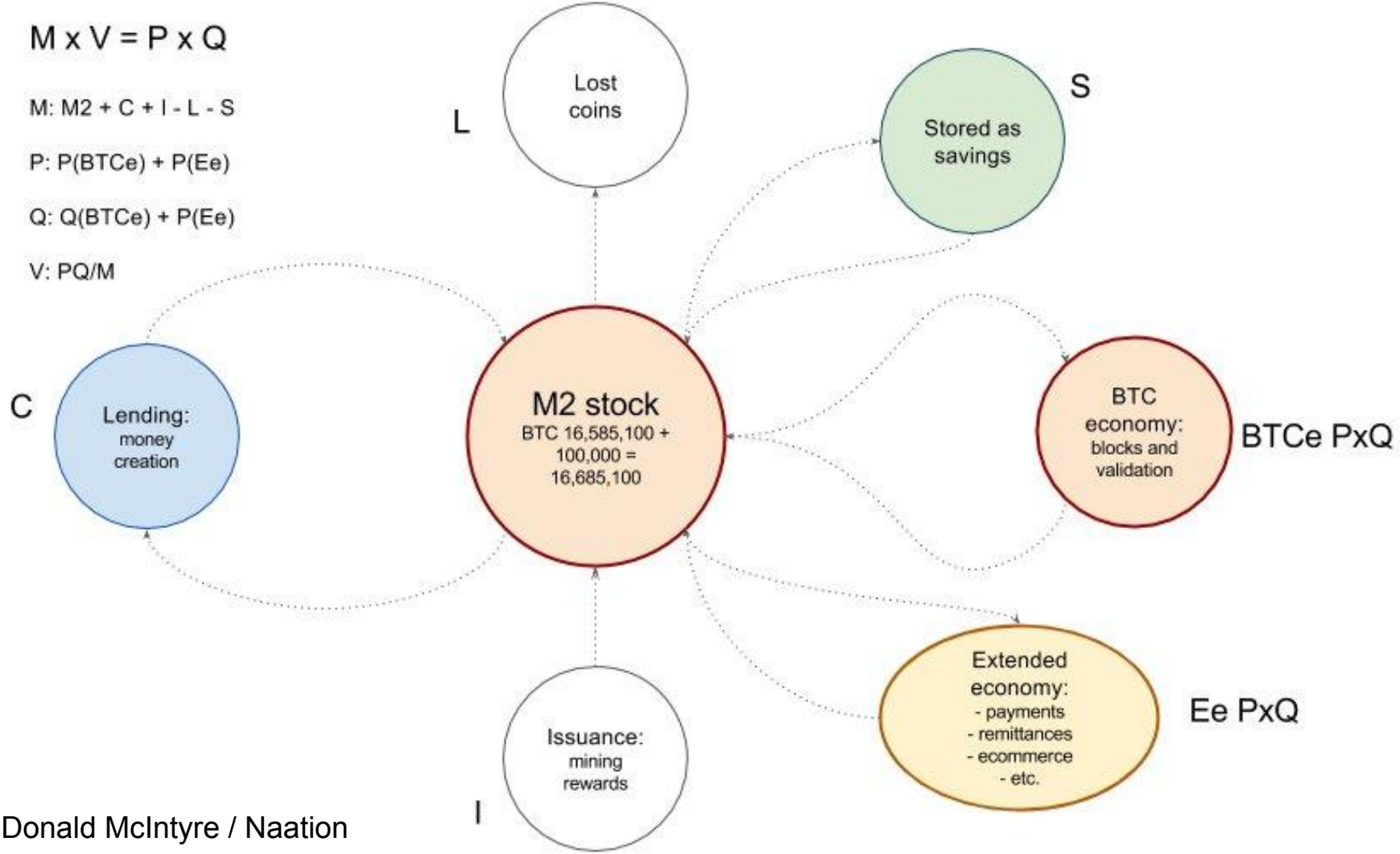
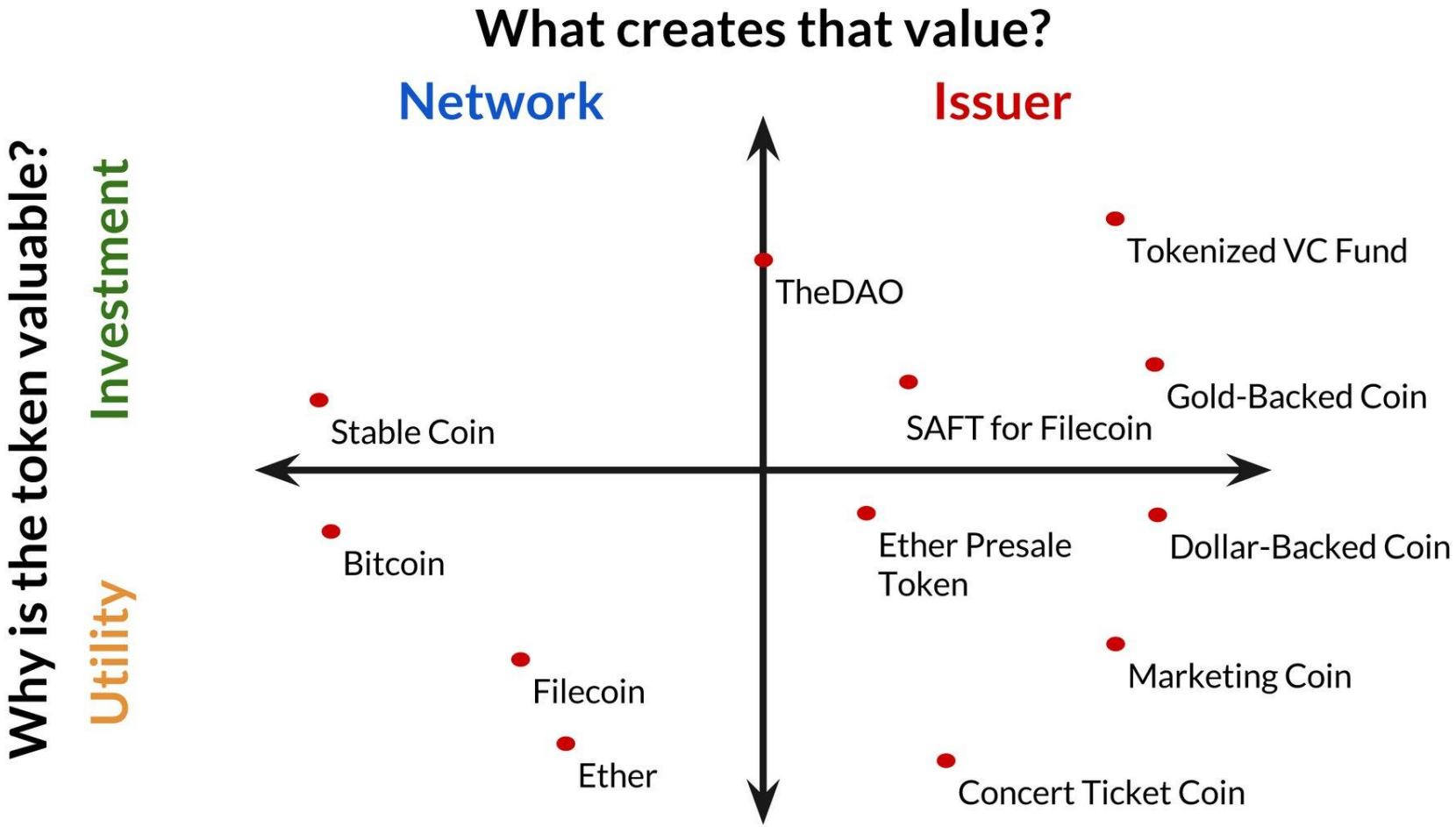


Fig: Donald McIntyre / Naation


What creates that value?
Network
Issuer
Why is the token valuable?
Investment
Utility
TheDAO
Tokenized VC Fund
Gold-Backed Coin
SAFT for Filecoin
Stable Coin
Bitcoin
Ether Presale Token
Dollar-Backed Coin
Marketing Coin
Filecoin
Ether
Concert Ticket Coin

THESE THINGS...DO NOT SEEM TO BE RELATED :)

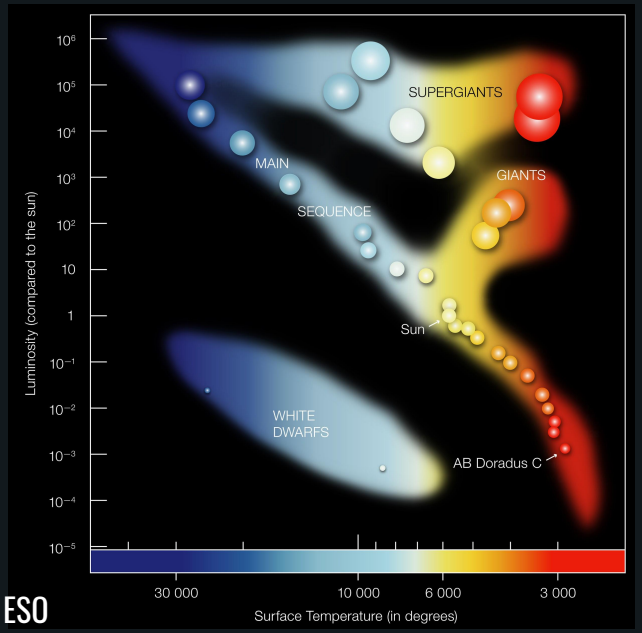
- Why does Cryptocurrency Matter?
  - Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

WTF IS FORKONOMY?

Apples-to-Apples Comparisons in a sea of Fruit Salad

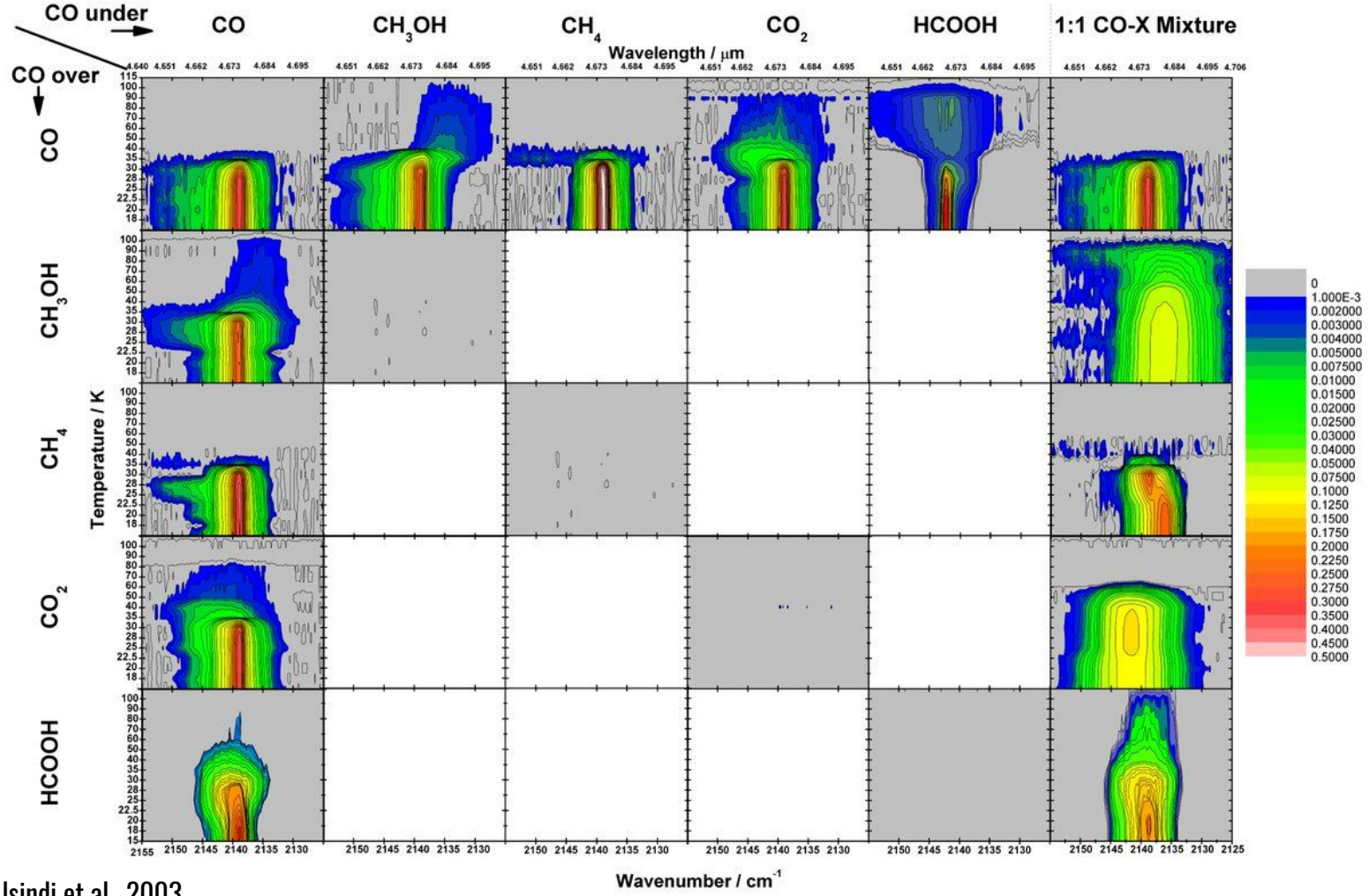
Credit: NASA, ESA, and S. Beckwith (STScI) and the HUDF Team
http://spacetelescope.org/images/heic0406a/

Credit: ESO/V. Beletsky
https://www.eso.org/public/images/uhd_beletsky_alma_15/



Credit: ESO
https://www.eso.org/public/images/eso0728c/

Credit: @LaurentMT
https://blog.goodaudience.com/gravity-10e1a25d2ab2



Credit: W. Z. Alsindi et al., 2003.

Credit: https://yourinnerrhino.com/2016/12/17/refinements-re-refined/

Testimonial Review: "Just a bunch of jargon"

Forks and Forkability

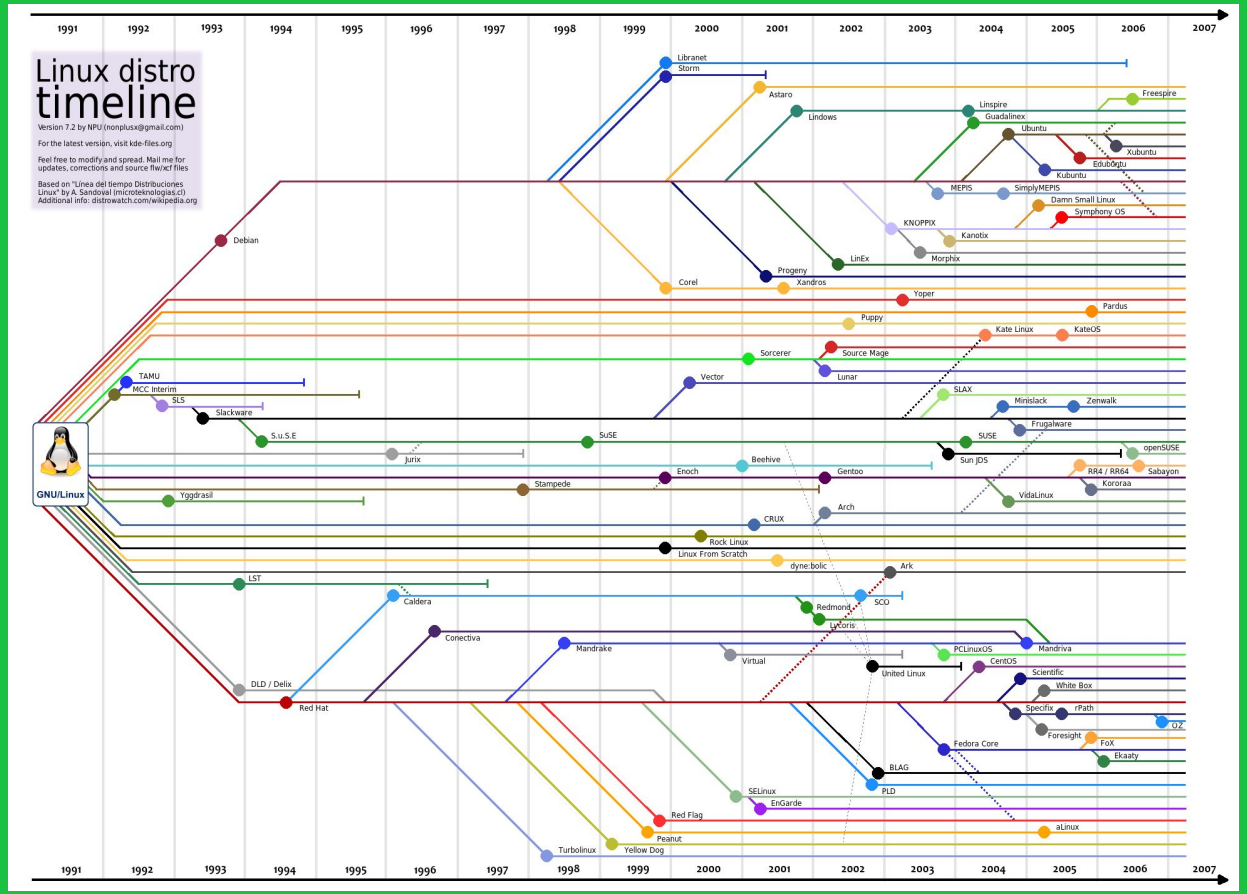
WTF is forkonomy?

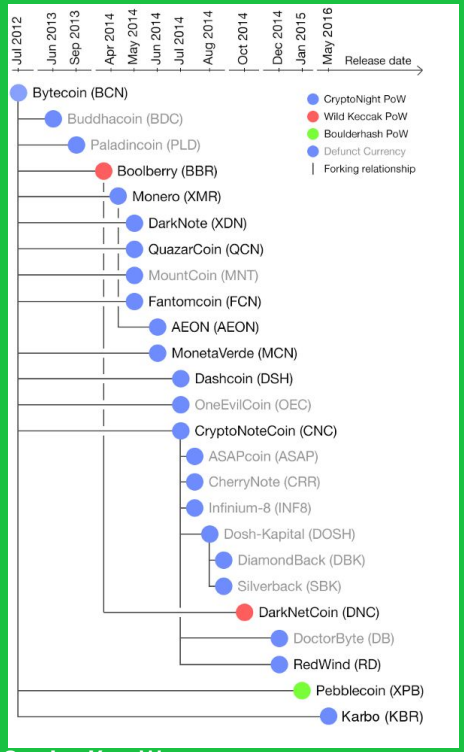
O RLY?

@parallelind

FORKS IN THE ROAD
PARALLEL DIMENSIONS?

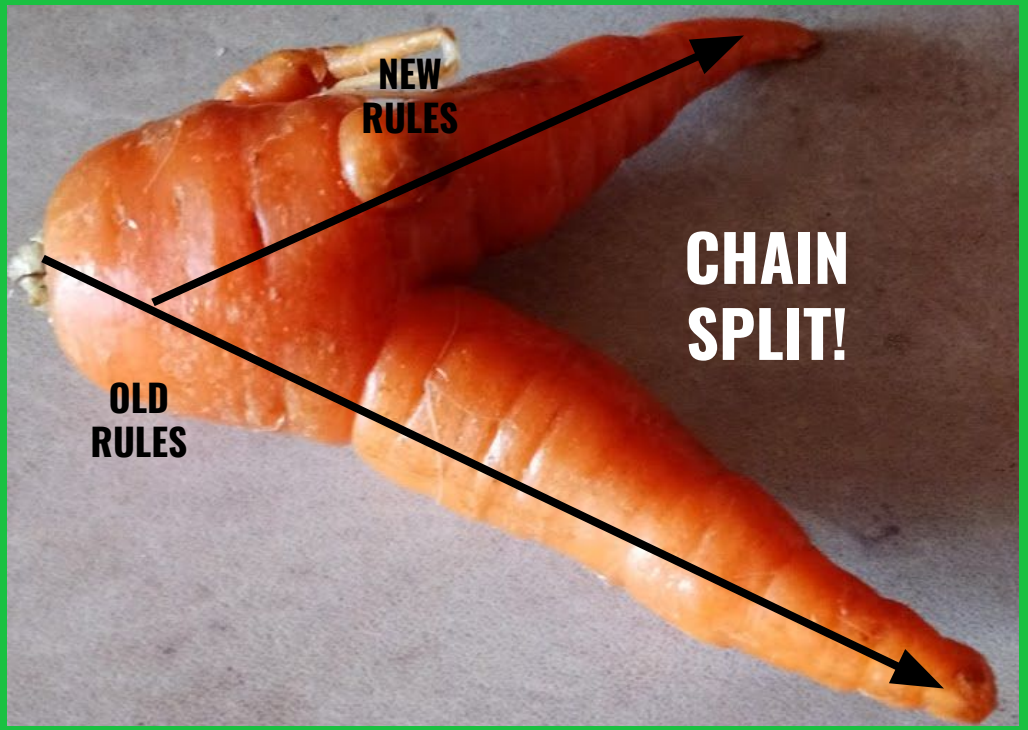
CODEBASE FORKS





Credit: Kun Woo
https://medium.com/@favakrypt/the-long-fork-story-of-monero-xmr-cryptonote-code-forks-chain-splits-and-network-upgrades-bc5250b4db5

LEDGER FORKS



> DYNAMIC PROCESS
> PARAMETER / CONSENSUS TWEAKS*
> NETWORK FRAGMENTATION
> REPLAY ATTACKS*
> CHAIN REORGS / WIPEOUTS*

> HARD - RULE RELAXATION / IRREV.
> SOFT - RULE CONSTRICTION / OPT-IN
> VELVET - MIN. CONSENSUS-BREAKING

*SOMETIMES / GENERALLY SPEAKING

Credit: Wassim's lunch

Credit: http://thecreativeadventurer.com/blog/exploring-glasgows-buchanan-street

Credit: https://pixabay.com/en/car-asphalt-delorean-parking-lot-3249993/

Credit: https://pixabay.com/en/car-asphalt-delorean-parking-lot-3249993/

WHAT MAKETH A FORK?
INTENTION, SUPPORT, POLITICS

Chandler Guo
@ChandlerGuo

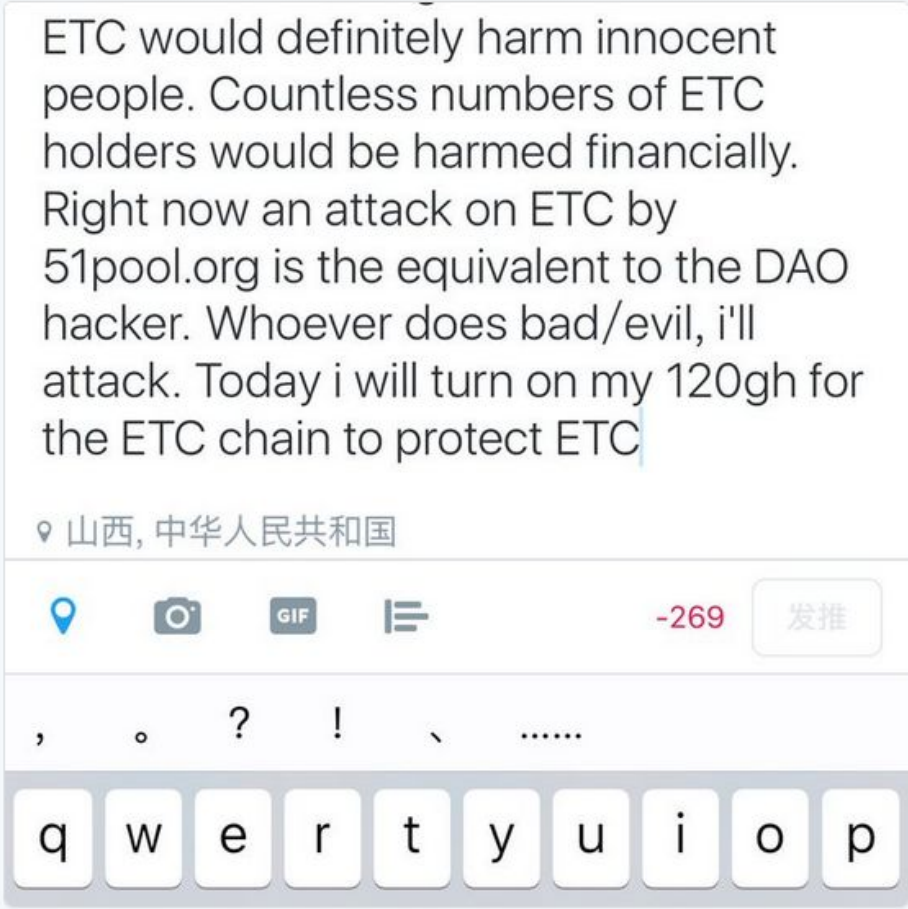
Follow

I am Chandler Guo, a 51% attack on Ethereum Classic (ETC) is coming with my 98G hashrate

powtopos
pow to pos
powtopos.com

1:33 PM - 24 Jul 2016

Chandler Guo @ChandlerGuo · 31 Jul 2016
Today i will turn on my 120GH for the ETC chain to protect ETC



Credit: http://www.twitter.com/chandlerguo

And so I joined Ethereum Classic initially mostly as a protest. And I wanted to say, 'Listen, this is not ok. Not everybody agrees. You don't have 99% of the community behind you. There is certainly a subset of your population that thinks you have betrayed the social contract you raised the money for, and you have, in a way, damaged your community. And we're not going to take it. We're going to make sure that you understand that the decisions you have made are not free and they have some form of consequence.'

But then after interacting with the Classic community and having a lot of conversations and getting to know them, I've come to the conclusion that it is a self-sustaining ecosystem if it wants to be. Meaning that there is a tremendous amount of opportunity for Ethereum Classic to diverge from ETH and actually become its own coin and chart its own course and have a different philosophy and different roadmap. And that, in and of itself, is actually a really exciting thing. Whenever you find a good ecosystem, a good value, good developers, good community you don't just throw that away. That's something you keep, cherish, and grow and see where it goes."

Credit: https://www.ethnews.com/charles-hoskinson-tells-us-why-he-is-100-etc
https://www.youtube.com/watch?v=f9YDXaVTXkg
https://toshitimes.com/ouroboros-vs-casper-vitalik-buterin-and-charles-hoskinson-in-a-heated-debate/

Grothendieck
TEAM

Wassim || Parallel Retweeted

BigBlockers @big_blockers 3m

rogerkver has unfollowed @ProfFaustus. SAD!

5 6 13

Wassim || Parallel Retweeted

BigBlockers @big_blockers 8m

ProfFaustus has unfollowed @rogerkver. SAD!

15 15 47

John McAfee ✓

@officialmcafee

Follow

Jihan Wu, Roger Ver and myself discussing how to put marriage and divorce on the blockchain.

Dr Craig S Wright ✓

@ProfFaustus

Follow

The fact, Bitcoin was never anti-banking. It was opposed to anti-free-market intervention.

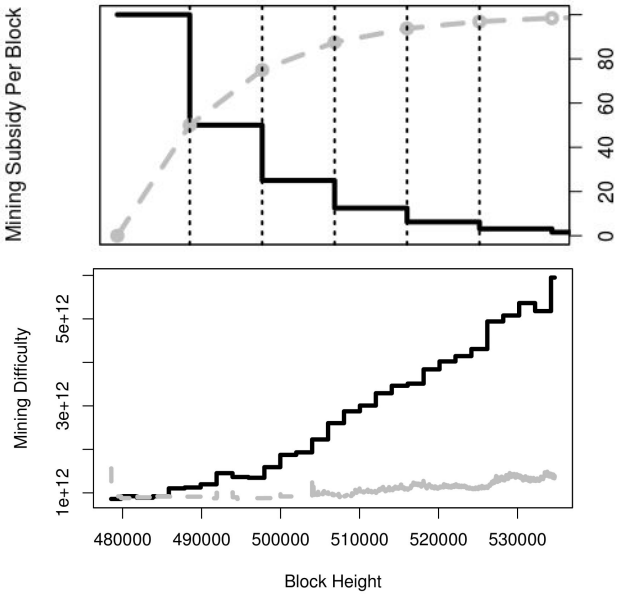
The purpose of Bitcoin is to stop just the thing that Jihan, ABC and others are now calling for.

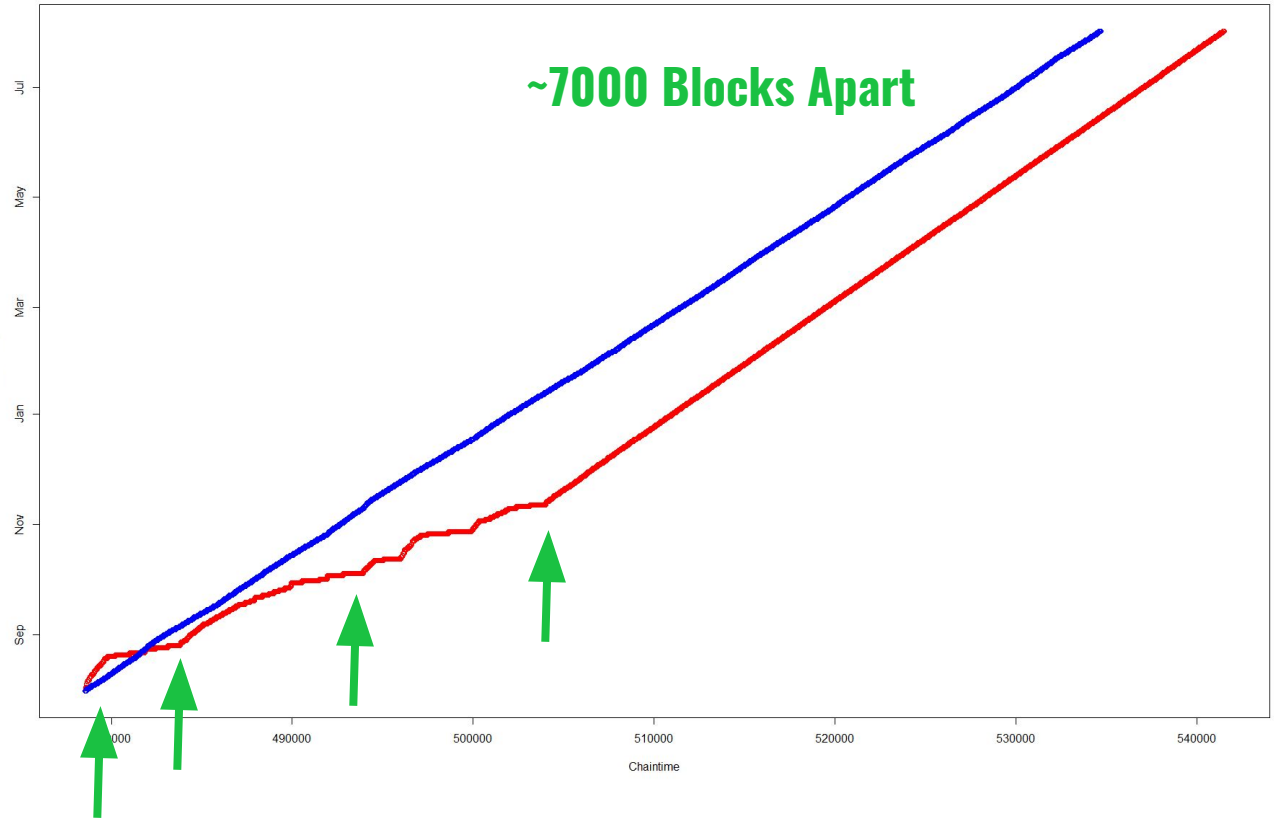
9:37 AM - 1 Sep 2018

Credit: https://facebook.com/calvinayre / https://twitter.com/officialmcafee / https://twitter.com/big_blockers / https://twitter.com/ProfFaustus

BTC & BCH

R: “Chain dynamics”
D1: Supply inflation & % issued over time,
D2: Mining Difficulty





BCH Difficulty Algorithm “Adjustments”

Data: http://blockchair.com, Image: Parallel Industries, http://forkonomy.pllel.com

Bitcoin Cash double spends

Double spend is when a set of coins is spent in more than one transaction. This can happen for various reasons, but one of the reasons **is fraud attempts**.

If you are accepting 0-conf payments, it's in your interest to detect double spend attempts. If you want merchants to accept your 0-conf payments, it's in your interest to help detect double spend attempts.

Bitcoin XT detects double spends relayed to it. It allows you to react to double spends. It's also the only Bitcoin Cash node that forwards double spends to allow other nodes to detect them.

Help gathering double spends here and detecting them network wide by running Bitcoin XT and connecting to at least one other Bitcoin XT node, such as `respends.thinlink.com:8333`

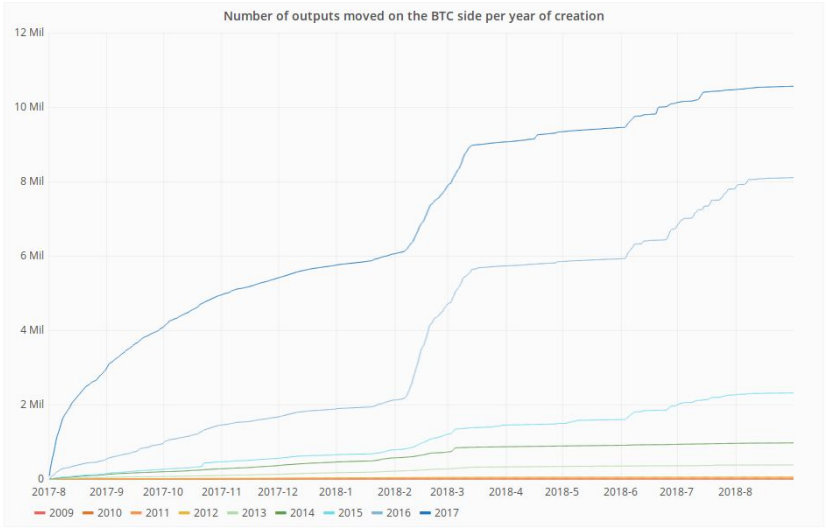
Below are double spends detected with Bitcoin XT. Tags are applied to some as analysis for cause or motivation of the double spend.

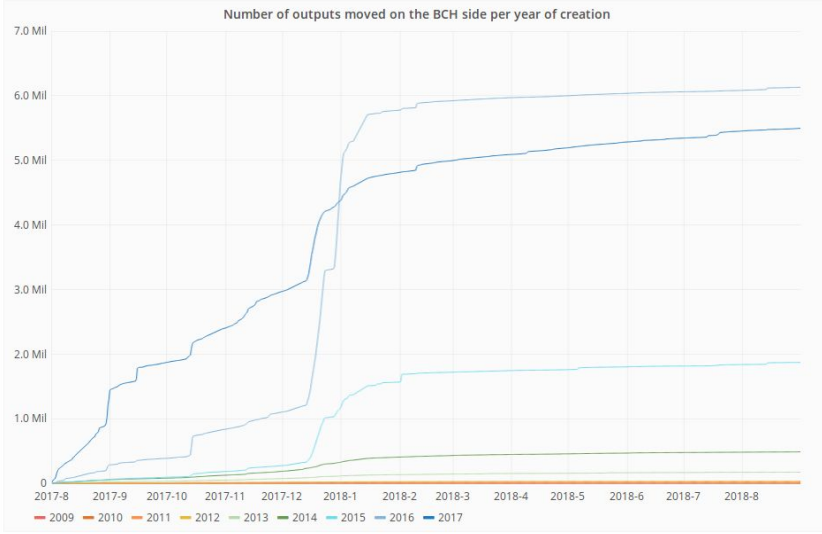
Last updated 2018-08-29 17:57:56.354944

Previous 1 2 3 4 5 6 7 8 Next

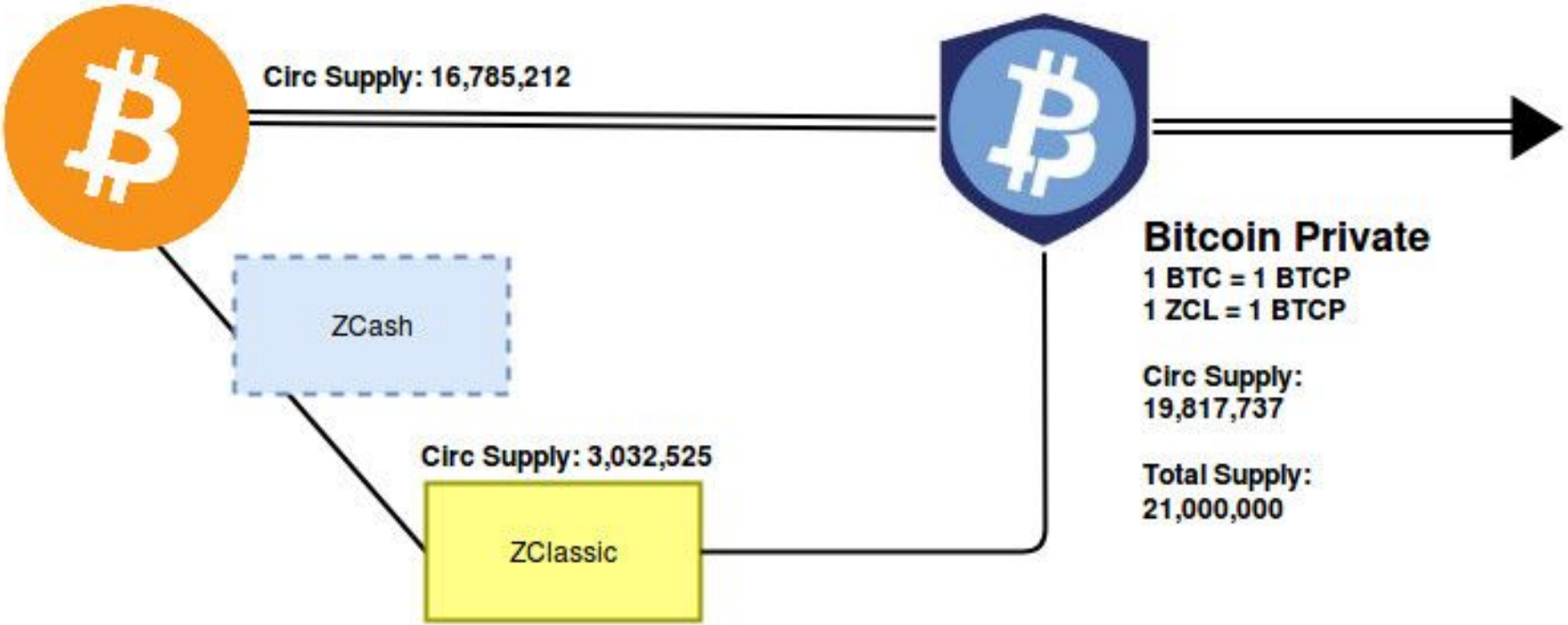
Original 🏆	Double
Raw data	Raw data
Hash: 8a…04	Hash: 71…0f
First seen: 2018-08-29 17:47:10	First seen: 2018-08-29 17:47:10
Status: Confirmed!	Status: Lost!
Fee: 1.64444444 sat / bytes	Fee: 1.63716814 sat / bytes
Tags:	Tags:
Inputs:	Inputs:
0.05765851 BCH from a8…e7	0.05765851 BCH from a8…e7
Outputs:	Outputs:
0.00000700 BCH to qpzfq6ptdnngrmaz5jl9s3xe24rhj58xwv0unyfud9	0.05764781 BCH to qrkzmsdyw6dzl7c5zv4c8lw58czfrxtau5nv9pu3l6
0.05764781 BCH to qrkzmsdyw6dzl7c5zv4c8lw58czfrxtau5nv9pu3l6	0.00000700 BCH to qpzfq6ptdnngrmaz5jl9s3xe24rhj58xwv0unyfud9

Credit: Doublespend.cash & Forks.network



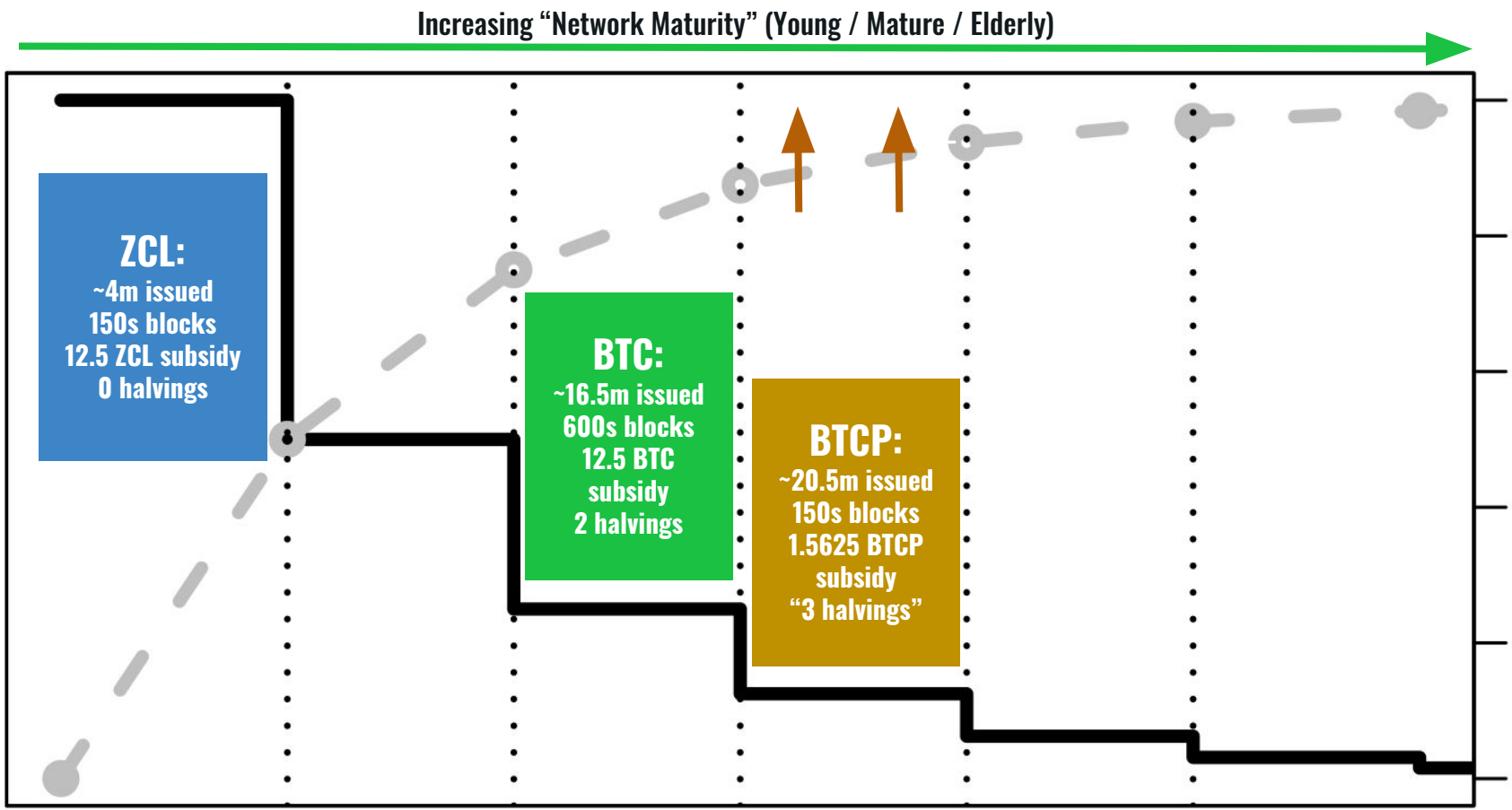


FORK-MERGE
HOW TO BREED CHAINS TOGETHER (BADLY)



Credit: https://steemit.com/crypto/@gktown/bitcoin-private-fork-resembles-github-fork-merge-infographic

BTC, ZCL & BTCP Supply inflation / % issued over time

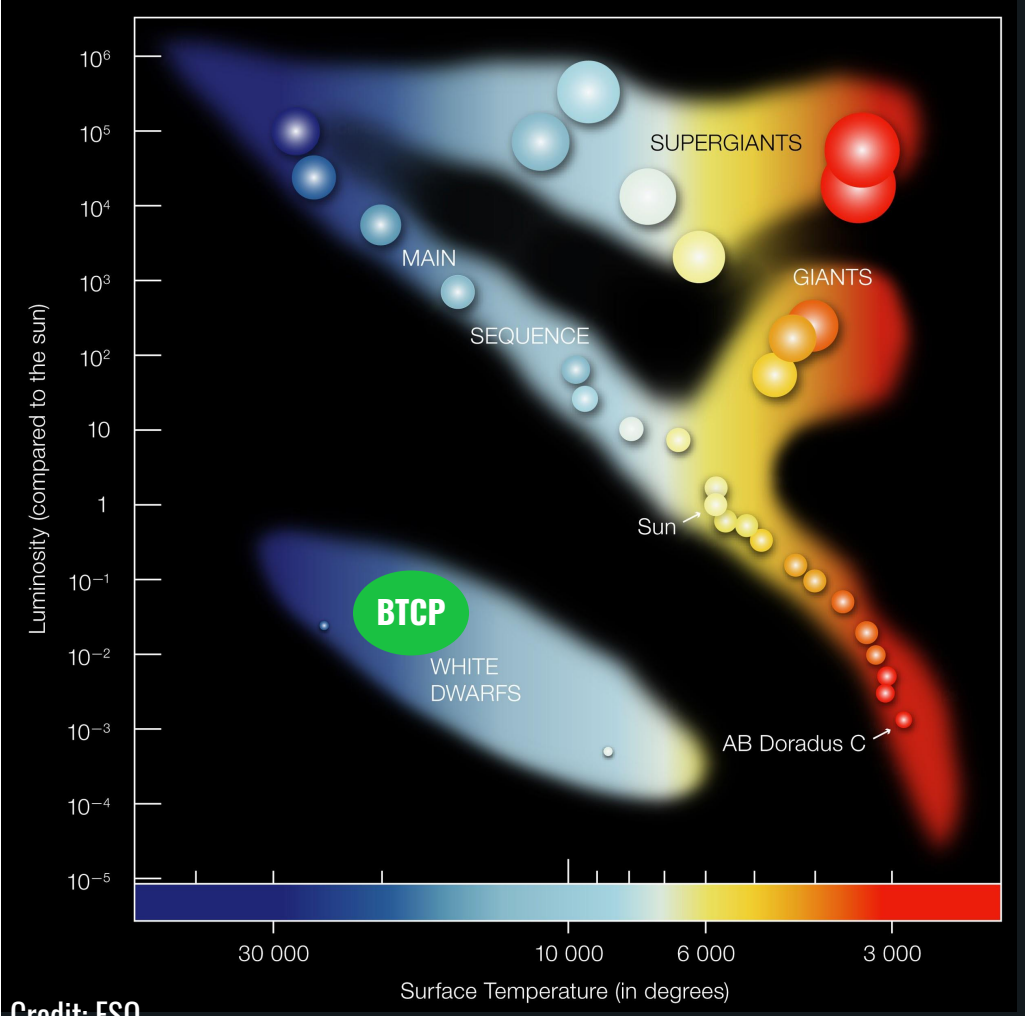


(all three networks have 21m supply cap)

Credit: Parallel Industries, http://forkonomy.pllel.com

2018-08-31 16:30:50
Bittrex - ZCL/BTC (D)
O: 0.00104892 H: 0.00120000 L: 0.00102416 C: 0.00109540
BTCP/BTC, HITB
ZCL/BTC, D
ZCL/BTC
0.02000000
0.01900000
0.01800000
0.01700000
0.01600000
0.01500000
0.01400000
0.01300000
0.01200000
0.01100000
0.01000000
0.00900000
0.00800000
0.00700000
0.00600000
0.00500000
0.00400000
0.00300000
0.00200000
0.00109540
0.00063390
-0.00000000
-0.00100000
charts by TradingView
Dec
2017
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
2018
Feb
Mar
Apr
May
Jun
Jul
Aug
29
COINIGY Digital Asset Intelligence
Charting library by TradingView
Data © 2018 Coinigy Inc. All Rights Reserved.

2018-08-31 16:32:48
Bittrex - ZCL/BTC (D)
O: 0.00104892 H: 0.00120000 L: 0.00102416 C: 0.00109540
BTCP/BTC, HITB
ZCL/BTC, D
ZCL/BTC
0.00460000
0.00440000
0.00420000
0.00400000
0.00380000
0.00360000
0.00340000
0.00320000
0.00300000
0.00280000
0.00260000
0.00240000
0.00220000
0.00200000
0.00180000
0.00160000
0.00140000
0.00120000
0.00109540
0.00100000
0.00080000
0.00063390
0.00040000
0.00020000
Apr
9
17
May
9
17
Jun
9
17
Jul
9
17
Aug
9
17
25
2
charts by TradingView
COINIGY Digital Asset Intelligence
Charting library by TradingView
Data © 2018 Coinigy Inc. All Rights Reserved.



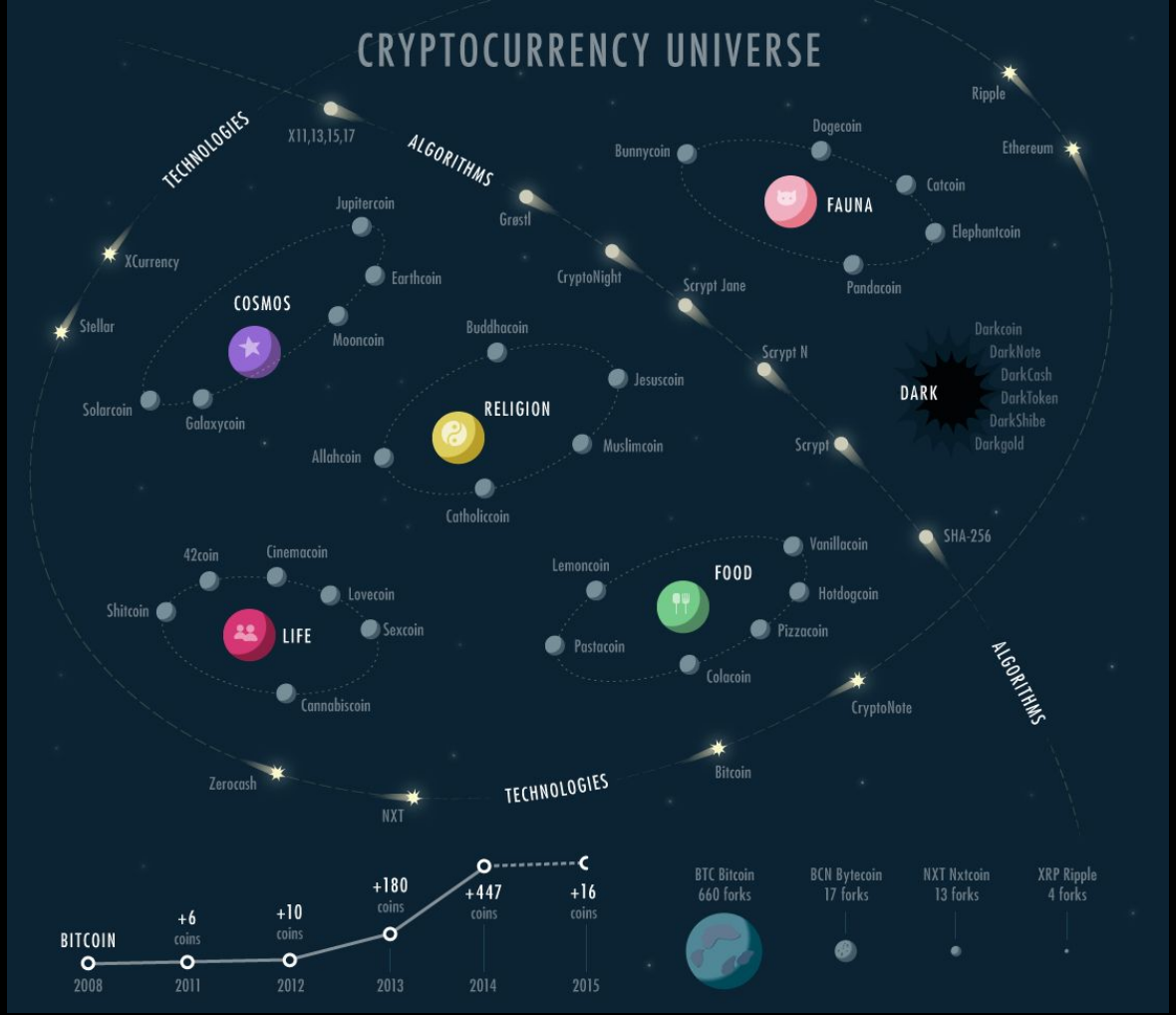
Credit: ESO
https://www.eso.org/public/images/eso0728c/

WHITE DWARF CHAIN?

- > UTXO MERGE = “FULL LEDGER”
- > INSUFFICIENT MINING SUBSIDY
- > NO TX FEE MARKET
- > TINY HASHRATE (EQUIHASH = ASICs)
- > 51% ATTACKS TRIVIAL (<$50/HR)
- > NO SoV / MoE PROPOSITION
- > NO “ECONOMIC GRAVITY”

TLDR: MATING CHAINS REKT BTCP

PEERING BEHIND THE VEIL
BLOCKCHAINS AS TIME MACHINES



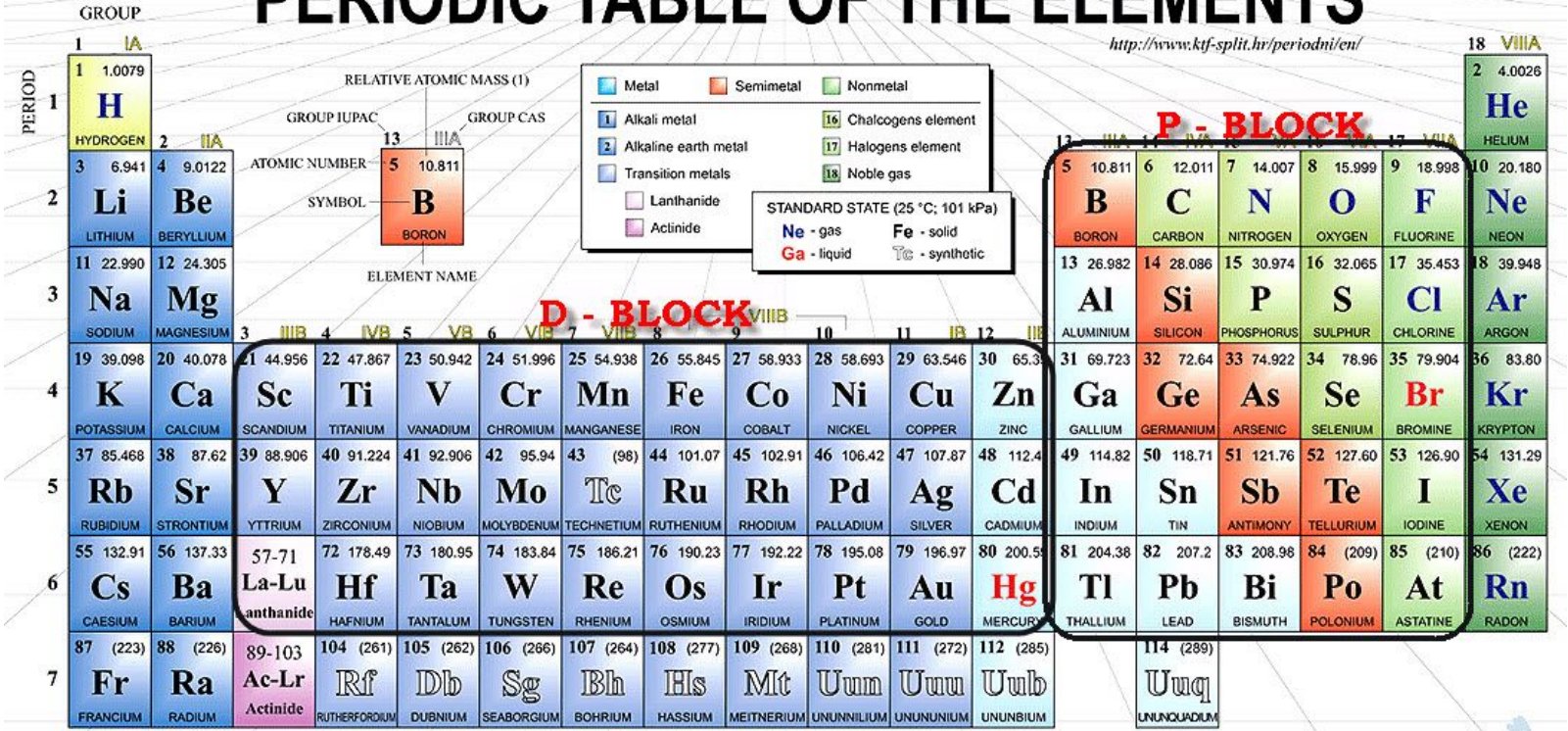
Credit: https://steemit.com/bitcoin/@tahajelassi/cryptocurrency-universe

THESE THINGS...DO NOT SEEM TO BE RELATED :)

- Why does Cryptocurrency Matter?
  - Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

PERIODIC TABLE OF THE ELEMENTS

http://www.ktf-split.hr/periodni/en/



LANTHANIDE

57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
138.91	140.12	140.91	144.24	(145)	150.36	151.96	157.25	158.93	162.50	164.93	167.26	168.93	173.04	174.97
La	Ce	Pr	Nd	Pm	Sm	Eu	Gd	Tb	Dy	Ho	Er	Tm	Yb	Lu
LANTHANUM	CERIUM	PRASEODYMIUM	NEODYMIUM	PROMETHIUM	SAMARIUM	EUROPIUM	GADOLINIUM	TERBIUM	DYSPROSIUM	HOLMIUM	ERBIUM	THULIUM	YTTERBIUM	LUTETIUM

ACTINIDE

89	90	91	92	93	94	95	96	97	98	99	100	101	102	103
(227)	232.04	231.04	238.03	(237)	(244)	(243)	(247)	(247)	(251)	(252)	(257)	(258)	(259)	(262)
Ac	Th	Pa	U	Np	Pu	Am	Cm	Bk	Cf	Es	Fm	Md	No	Lr
ACTINIUM	THORIUM	PROTACTINIUM	URANIUM	NEPTUNIUM	PLUTONIUM	AMERICIUM	CURIUM	BERKELIUM	CALIFORNIUM	EINSTEINIUM	FERMIUM	MENDELEVIUM	NOBELIUM	LAWRENCIUM

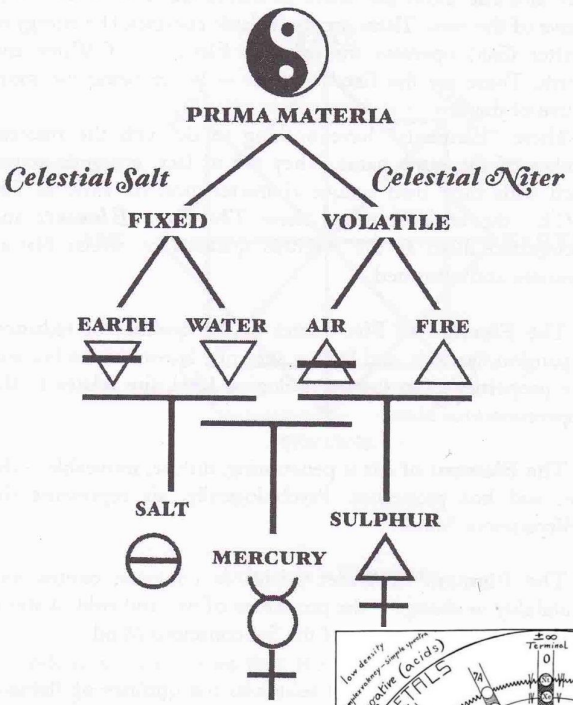
(1) Pure Appl. Chem., 73, No. 4, 667-683 (2001)

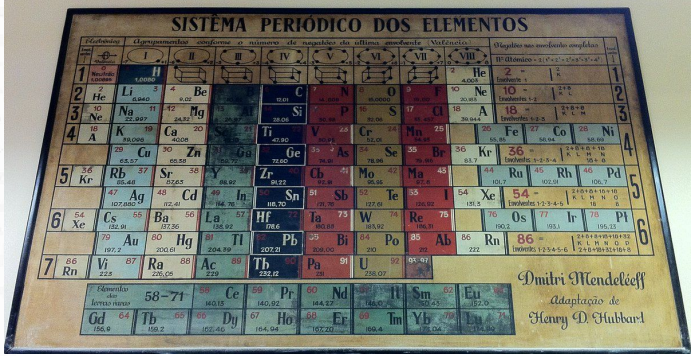
Relative atomic mass is shown with five significant figures. For elements have no stable nuclides, the value enclosed in brackets indicates the mass number of the longest-lived isotope of the element.

However three such elements (Th, Pa, and U) do have a characteristic terrestrial isotopic composition, and for these an atomic weight is tabulated.

Editor: Aditya Vardhan (adivar@nettlinx.com)

Copyright © 1998-2003 EniG. (eni@ktf-split.hr)


PRIMA MATERIA
Celestial Salt
Celestial Niter
FIXED
VOLATILE
EARTH
WATER
AIR
FIRE
SALT
MERCURY
SULPHUR


SISTEMA PERIODICO DOS ELEMENTOS
Dmitri Mendeléieff
Adaptação de
Henry D. Hubbard

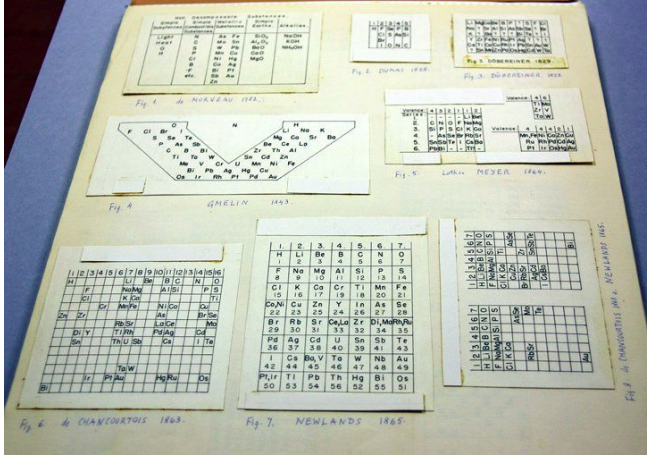
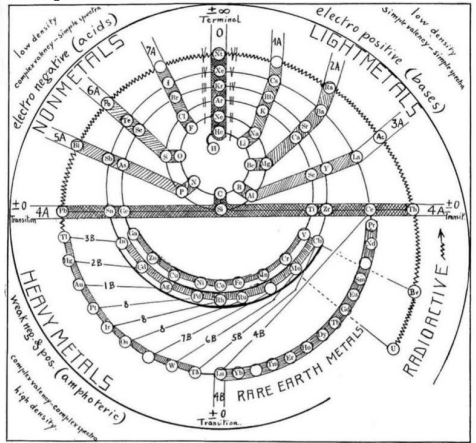
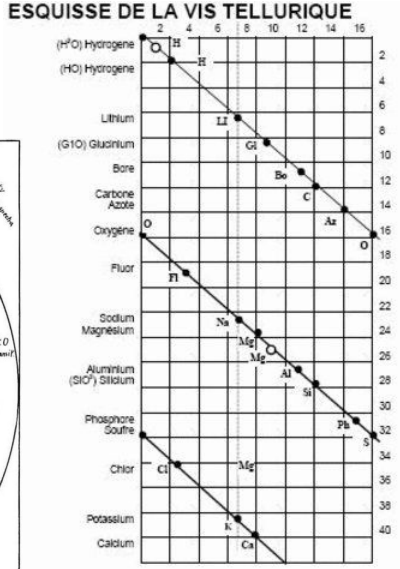
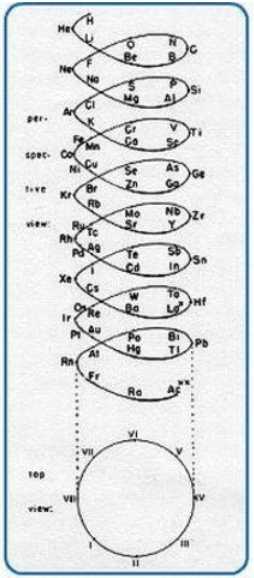
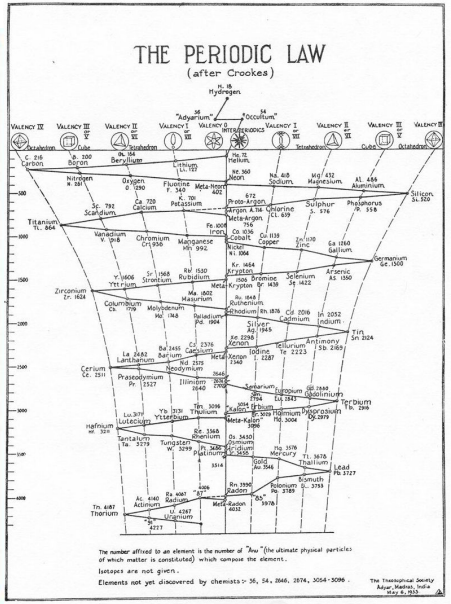


Fig. 1. de NORVEAU 1782.
Fig. 2. DUMAS 1858.
Fig. 3. DOEBEREINER 1829.
Fig. 4
GMELIN 1843.
Fig. 5. Lothar MEYER. 1864.
Fig. 6. de CHANCOURTOIS 1863.
Fig. 7. NEWLANDS 1865.


electro negative (acids)
electro positive (bases)
NONMETALS
LIGHTMETALS
HEAVY METALS
RARE EARTH METALS
RADIOACTIVE

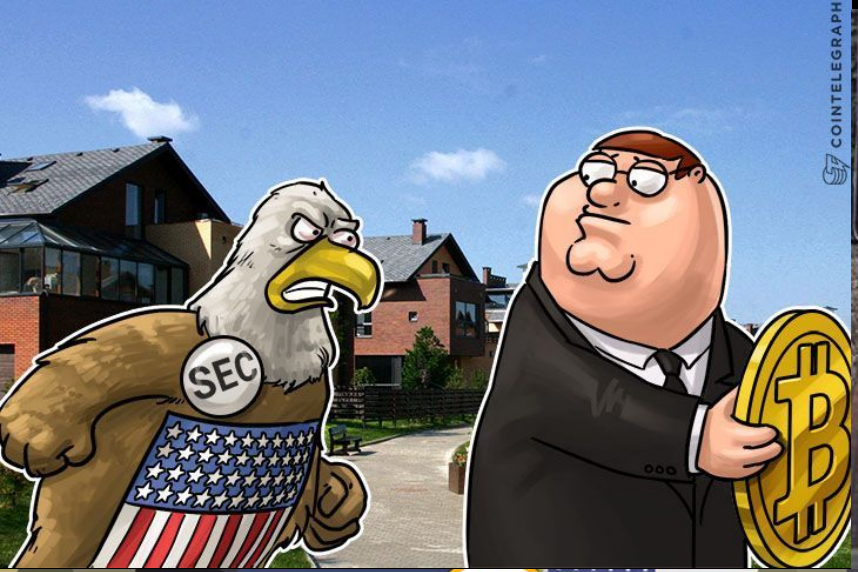

ESQUISSE DE LA VIS TELLURIQUE
(H²O) Hydrogene
(HO) Hydrogene
Lithium
(G10) Glucinium
Bore
Carbone
Azote
Oxygene
Fluor
Sodium
Magnésium
Aluminium
(SiO²) Silicium
Phosphore
Soufre
Chlor
Potassium
Calcium


per-
spec-
tive
view:
top
view:


THE PERIODIC LAW
(after Crookes)
Hydrogen
"Adamas"
"Occultum"
MENDELEEVIOUS
Helium
Lithium
Beryllium
Boron
Carbon
Nitrogen
Oxygen
Fluorine
Neon
Sodium
Magnesium
Aluminium
Silicon
Phosphorus
Sulphur
Chlorine
Argon
Potassium
Calcium
Scandium
Titanium
Vanadium
Chromium
Manganese
Iron
Cobalt
Nickel
Copper
Zinc
Gallium
Germanium
Arsenic
Selenium
Bromine
Krypton
Rubidium
Strontium
Yttrium
Zirconium
Niobium
Molybdenum
Ruthenium
Rhodium
Palladium
Silver
Cadmium
Indium
Tin
Antimony
Tellurium
Iodine
Xenon
Caesium
Barium
Lanthanum
Cerium
Praseodymium
Neodymium
Samarium
Europium
Gadolinium
Terbium
Dysprosium
Holmium
Erbium
Thulium
Ytterbium
Lutecium
Hafnium
Tantalum
Tungsten
Osmium
Iridium
Platinum
Gold
Mercury
Thallium
Lead
Bismuth
Thorium
Uranium
The number affixed to an element is the number of "Ana" (the ultimate physical particles of which matter is constituted) which compose the elements.
Isotopes are not given.
Elements not yet discovered by chemists :- 36, 54, 2046, 2074, 3054-3096.
The Theosophical Society
Adyar, Madras, India
May 6, 1933

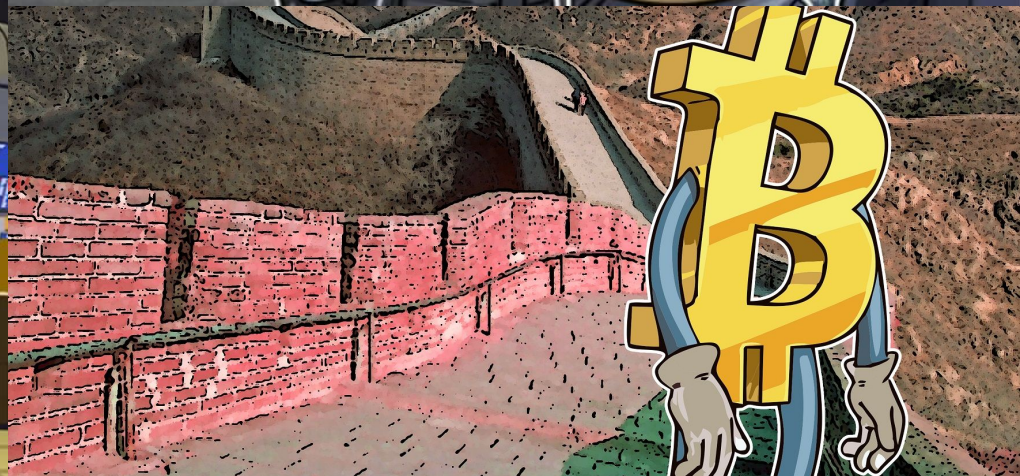
TOKENSPACE
WHY DO WE NEED TAXONOMIES ANYWAY?

Regulation, Risk, Hacks, Law


SEC

Bitcoin laundry
CLOSED

OH DEAR GOD!
CHINA IS BANNING BITCOIN!
SELL! SELL IT ALL, DAMNIT!



Business

Bitcoin draws calls for more regulation at Davos

share

‘We will all lose out’ Will Philip Hammond announce a Bitcoin Budget?

PHILIP Hammond should use the Budget to capitalise on the huge growth in cryptocurrencies like Bitcoin, a former senior banker at JP Morgan has said.

INDY/TECH

BITCOIN LATEST: THERESA MAY 'VERY SERIOUSLY' CONSIDERING TAKING ACTION AGAINST DIGITAL CURRENCIES

OPINION

Op Ed: Exploring the SEC's New "Sufficiently Decentralized" Test

Digital Asset Transactions
Met Gary (Plastic)

William Hinman
Director, Division of Corporation Finance

San Francisco, CA

June 14, 2018

Remarks at the Yahoo Finance A

'MONEY HAS CHANGED OVER TIME': US SUPREME COURT CITES BITCOIN IN POSITIVE LIGHT

WILMA WOO | JUN 22, 2018 | 08:00

MOST REASONABLE PEOPLE AGREE THAT:

CRYPTO-ASSETS ARE NOT "MUH TULIPS"

Money

EXANTE

1. Durable
2. Portable
3. Fungible
4. Intrinsic value

Aristotle
IV BC

1. Store of value
2. Medium of exchange
3. Unit of account

W.S. Jevons
XIX AD

Bitcoin Obituaries

Bitcoin has died 245 times

Obituary Stats | Submit Obituary | Obituary Generator

"Bitcoin price THREAT: Bitcoin WON'T last past 2018" – Express | $11,582.56

Bitcoin will not survive but that does not mean the entire cryptocurrency craze is dead with useful cryptos like Ripple...

READ MORE

"The end of bitcoin" – The Week | $11,582.56

To really work as money, bitcoin needs to be widely used. There need to be lots of actors providing a...

READ MORE

"Bitcoin could be here for 100 years but it's more likely to 'totally collapse,' Nobel laureate says" – CNBC | $11,582.56

Bitcoin will likely "totally collapse," Nobel Prize-winning economist Robert Shiller has told CNBC, adding that it reminds him of "tulip...

READ MORE

Money	Tulips	Fiat	Gold	Bitcoin
Store of value	*	****	*****	****
Medium of exchange	****	****	***	*****
Unit of account	*	****	**	**

Naval
@naval

Following

Tulips are not durable, not scarce, not programmable, not fungible, not verifiable, not divisible, and hard to transfer. But tell me more about your analogy...

2:11 AM - 9 Dec 2017

2,959 Retweets **7,305** Likes

257 3.0K 7.3K

Value [edit]

In 2006, the House of Commons Library published a research paper which included an index of prices in po

Regarding the period 1750–1914 the document states: "Although there was considerable year on year fluct since 1945". It goes on to say that "Since 1945 prices have risen in every year with an aggregate rise of ov

The value of the index in 1751 was 5.1, increasing to a peak of 16.3 in 1813 before declining very soon afte 25.3 in 1920, before declining to 15.8 in 1933 and 1934—prices were only about three times as high as the

Inflation had a dramatic effect during and after World War II—the index was 20.2 in 1940, 33.0 in 1950, 49.

The following table shows the equivalent amount of goods and services that, in a particular year, could be p

The table shows that from 1971 to 2015 the British pound lost about 92% of its buying power.

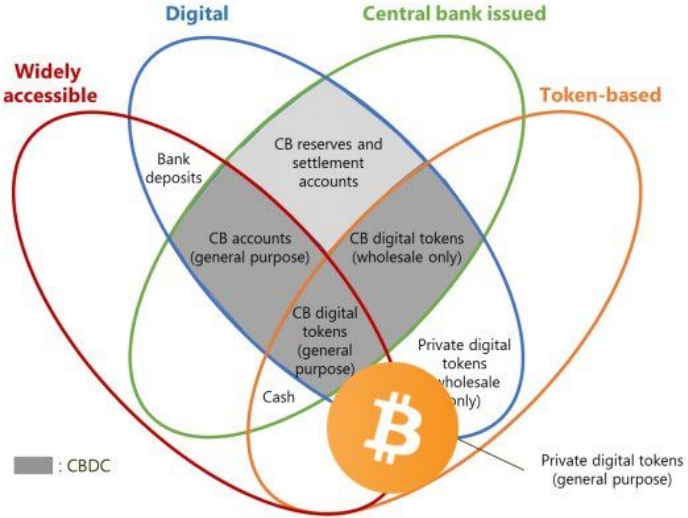
Buying power of one British pound compared to 1971 GBP

Year	Equivalent buying power	Year	Equivalent buying power	Year	Equivalent buying power	Year	Equivalent buying power	Year	Equivalent buying power
1971	£1.00	1981	£0.271	1991	£0.152	2001	£0.117	2011	£0.0900
1972	£0.935	1982	£0.250	1992	£0.146	2002	£0.115	2012	£0.0850
1973	£0.855	1983	£0.239	1993	£0.144	2003	£0.112	2013	£0.0826
1974	£0.735	1984	£0.227	1994	£0.141	2004	£0.109	2014	£0.0800
1975	£0.592	1985	£0.214	1995	£0.136	2005	£0.106	2015	£0.0780
1976	£0.510	1986	£0.207	1996	£0.133	2006	£0.102		
1977	£0.439	1987	£0.199	1997	£0.123	2007	£0.0980		
1978	£0.407	1988	£0.190	1998	£0.125	2008	£0.0943		
1979	£0.358	1989	£0.176	1999	£0.123	2009	£0.0952		
1980	£0.303	1990	£0.161	2000	£0.119	2010	£0.0910		

Money	Tulips	Fiat	Gold	Bitcoin
Store of value	*	****	*****	****
Medium of exchange	****	****	***	*****
Unit of account	*	****	**	**

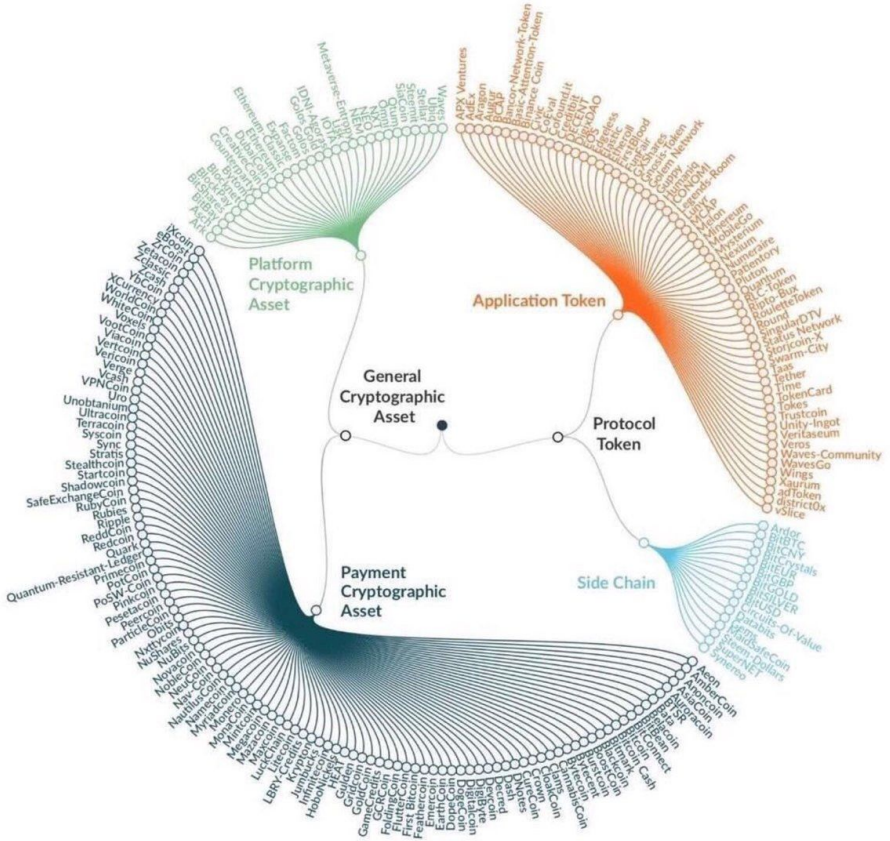
The money flower: a taxonomy of money

Graph 1



Notes: The Venn-diagram illustrates the four key properties of money: *issuer* (central bank or not); *form* (digital or physical); *accessibility* (widely or restricted) and *technology* (account-based or token-based). *CB* = central bank, *CBDC* = central bank digital currency (excluding digital central bank money already available to monetary counterparties and some non-monetary counterparties). *Private digital tokens (general purpose)* include crypto-assets and currencies, such as bitcoin and ethereum. *Bank deposits* are not widely accessible in all jurisdictions. For examples of how other forms of money may fit in the diagram, please refer to the source.

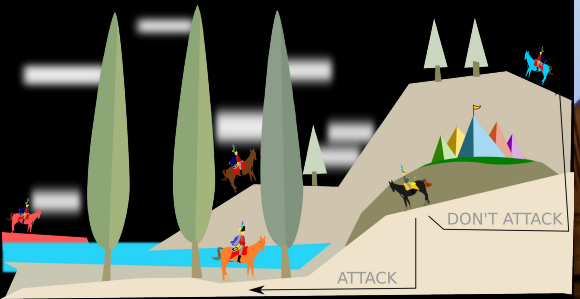
Source: Based on Bech and Garratt (2017).

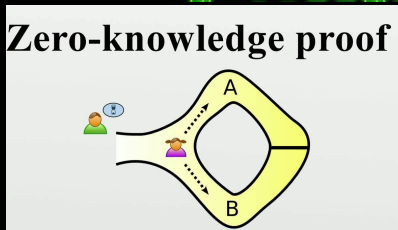


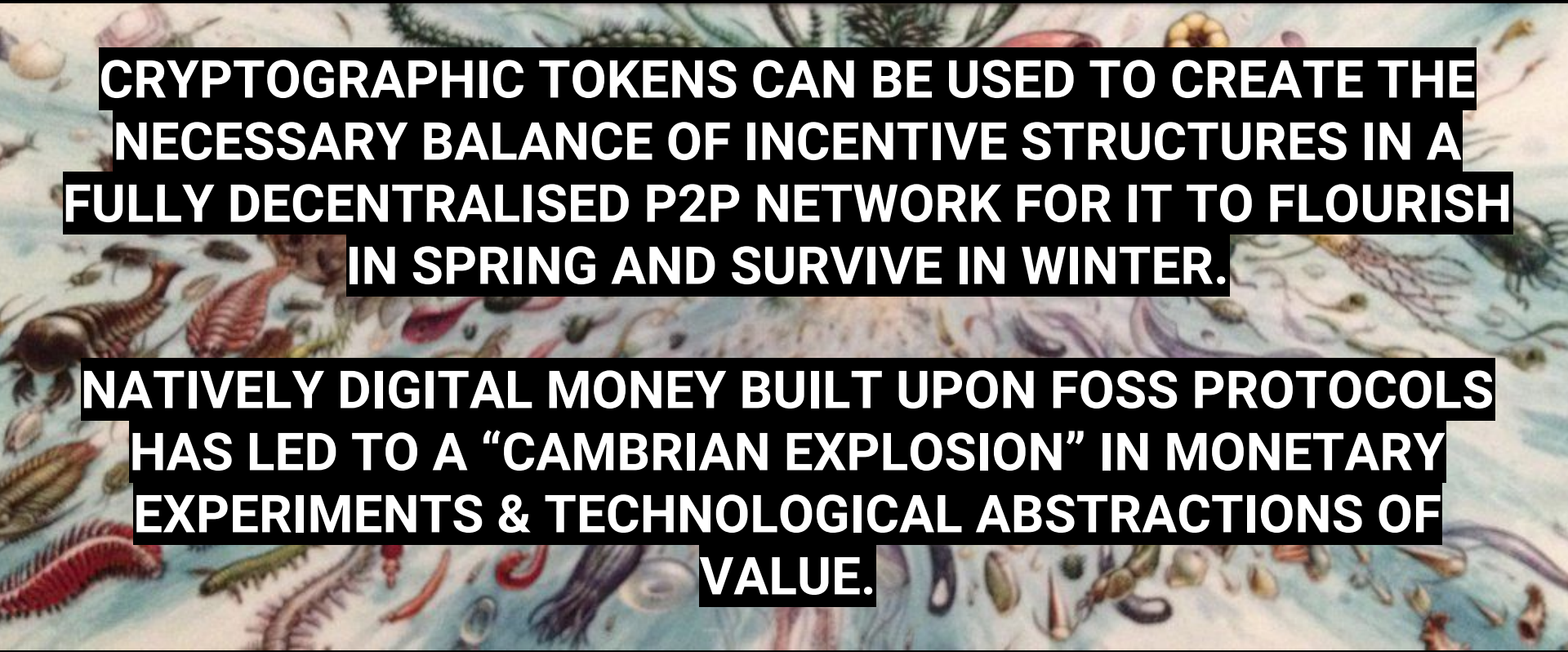
CRYPTO -
From Ancient Greek κρυπτός (kruptós, “hidden, secret”).
ECONOMICS -
From economy, from Latin oeconomia, from Ancient Greek οἰκονομία (oikonomía, “management of a household administration”), from οἶκος (oîkos, “house”) + νέμω (némō, “distribute, allocate”).

A Multi-Disciplinary Field

Game Theory & Behavioural Economics
Finance, Investing & Trading
Geopolitics & Regulation
Thermodynamics & Entropy
CS Distributed Networks & Applied Cryptography






CRYPTOGRAPHIC TOKENS CAN BE USED TO CREATE THE NECESSARY BALANCE OF INCENTIVE STRUCTURES IN A FULLY DECENTRALISED P2P NETWORK FOR IT TO FLOURISH IN SPRING AND SURVIVE IN WINTER.
NATIVELY DIGITAL MONEY BUILT UPON FOSS PROTOCOLS HAS LED TO A “CAMBRIAN EXPLOSION” IN MONETARY EXPERIMENTS & TECHNOLOGICAL ABSTRACTIONS OF VALUE.

How are crypto-assets different from traditional financial instruments?

How are crypto-assets different from traditional financial instruments?

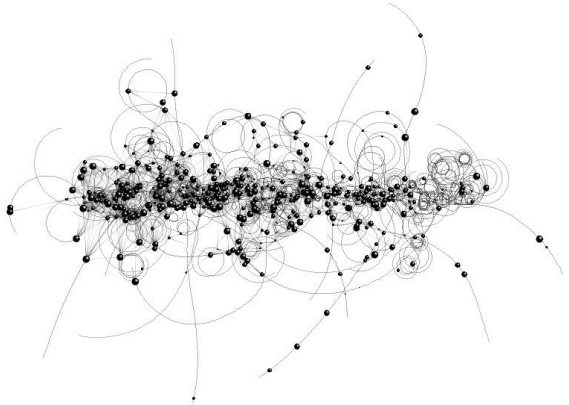
(Monetary | Commodity | Capital / CFs)
(NOT Fractional | Debt-Based | No Counterparty Liability)
(Incompatible Value Proposition Models)
(Bearer assets like metals *sans specie* w/ programmability)
(Decentralised / Borderless)
(Culture)

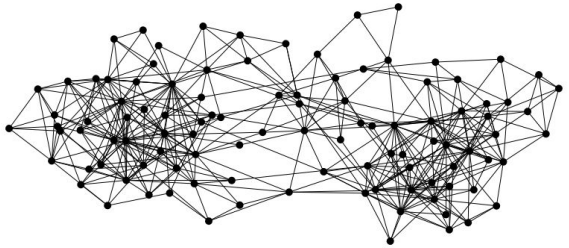
Bitcoin: A Protocol and a Currency

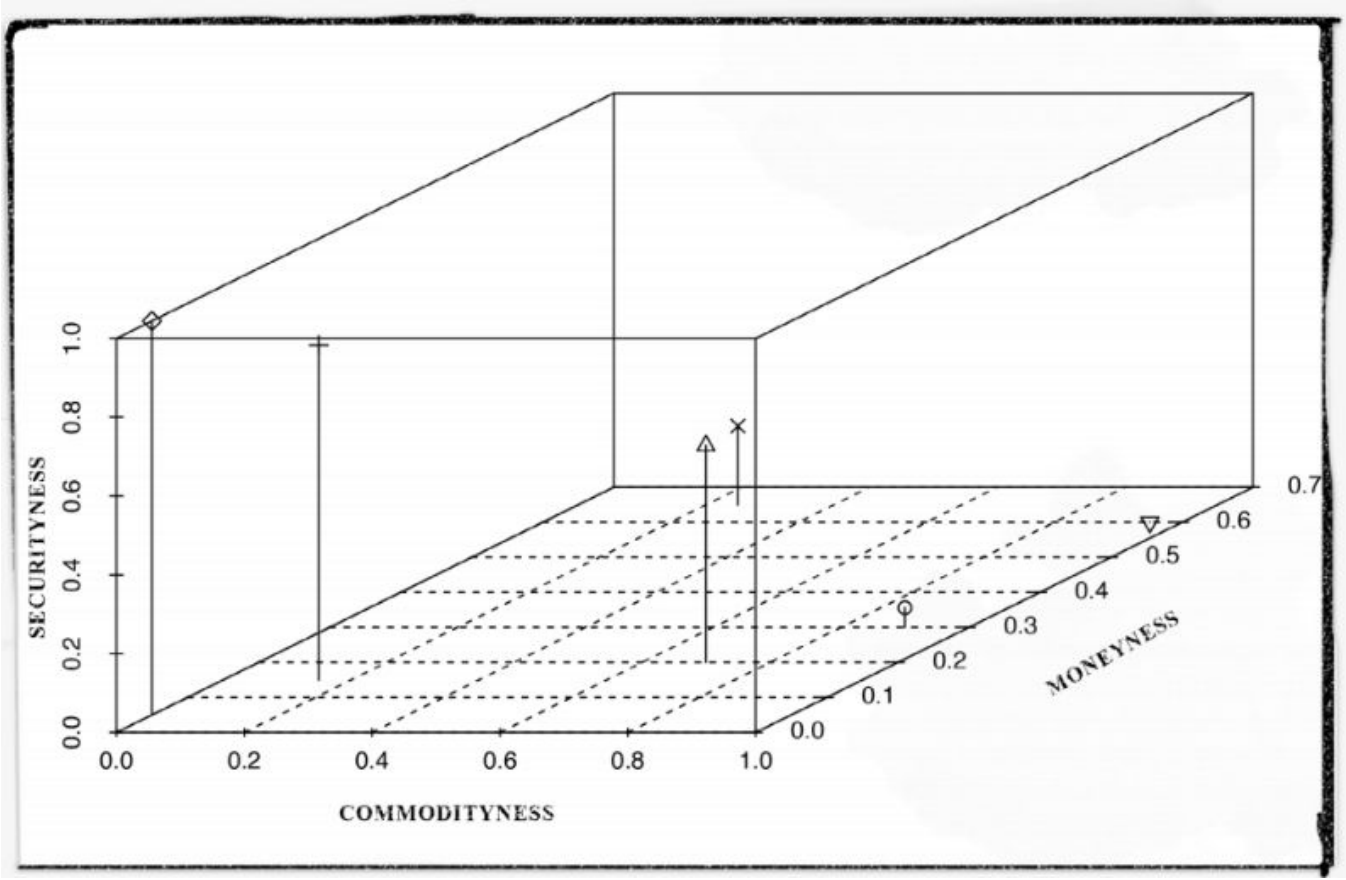
- **B**itcoin: protocol, software, and community
- **b**itcoin**s**: units of the currency

bitcoins are sent using Bitcoin

- bitcoins are the first powerful Bitcoin protocol application: a native digital asset created inside the protocol







{ TokenSpace Example }

- ○ BTC
- △ ETH
- \+ XRP
- × USD
- ◇ AAPL
- ▽ GOLD

Credit: 21Cryptos Magazine & Parallel Industries, http://21cryptos.com http://www..pllel.com

OPINION

Op Ed: Exploring the SEC's New "Sufficiently Decentralized" Test

Digital Asset Transactions
Met Gary (Plastic)

William Hinman
Director, Division of Corporation Finance

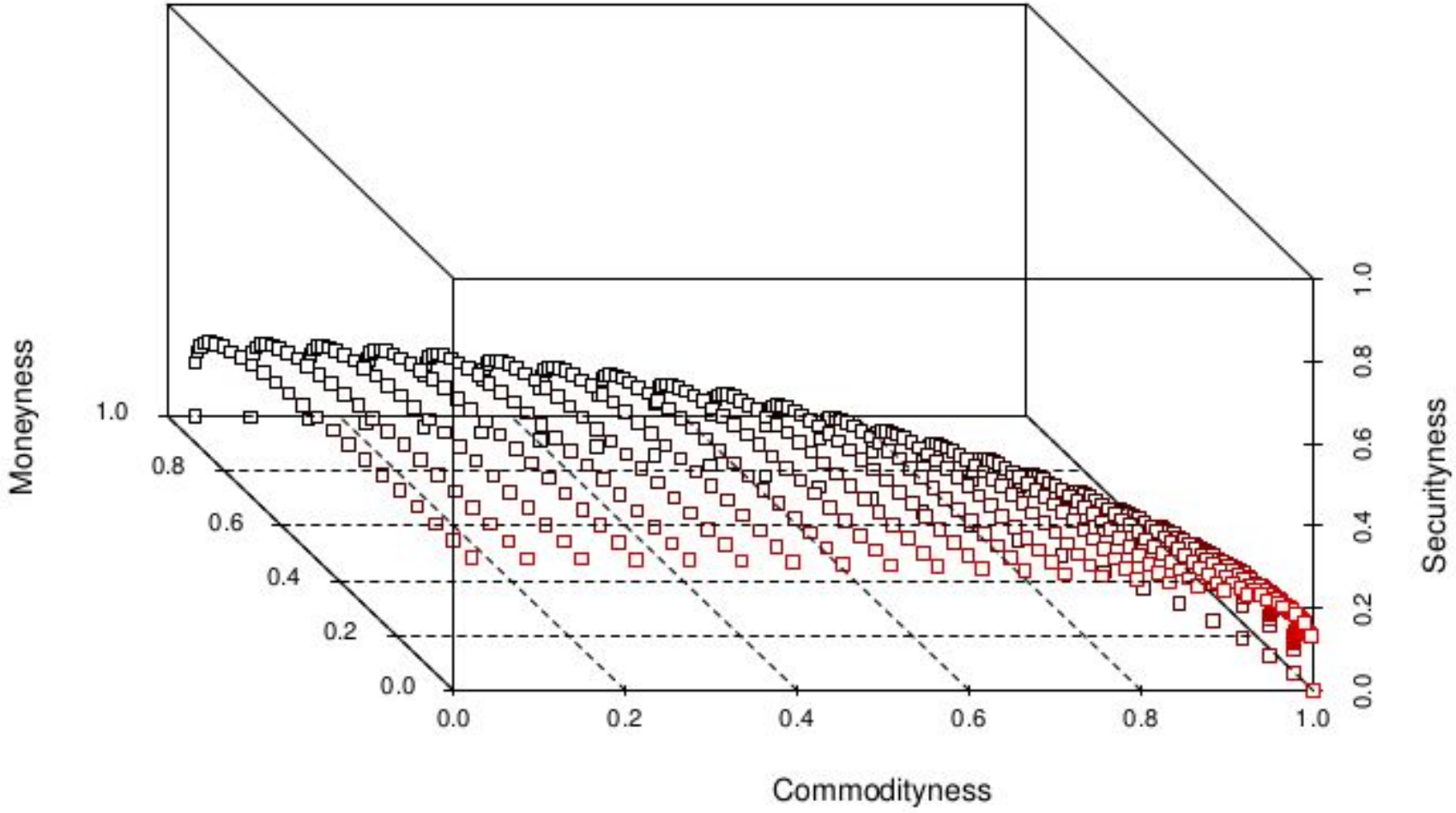
San Francisco, CA

June 14, 2018

Remarks at the Yahoo Finance A

'MONEY HAS CHANGED OVER TIME': US SUPREME COURT CITES BITCOIN IN POSITIVE LIGHT

WILMA WOO | JUN 22, 2018 | 08:00


Moneyness
1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0
Commodityness
Securityness
0.0
0.2
0.4
0.6
0.8
1.0

Securityness: Example Scores as of October 2018		
Asset	$\tilde{\mathcal{S}}$	Notes
AAPL	1.0	Ideal type for securitised asset.*
XRP	0.85	Supply concentration & nodes insider-heavy, no validation reward, missing ledger history
DAO	0.9	Collective investment vehicle
BTC	0.05	Leaderless, permissionless
ETH (2014)	0.85	Token sale of pre-functional network utility
ETH (2018)	0.55	*"sufficiently decentralised"***
Gold (metal)	0.0	Ideal type for non-securitised asset
Soy beans	0.0	Ideal type for non-securitised asset
USD	0.2	Reliance on faith in government and fiscal prudence of Federal Reserve. Unlikely to still be fully collateralised/backed by gold, no audit.

Moneyness: Example Scores as of October 2018		
Asset	$\overline{\mathcal{M}}$	Notes
AAPL	0.05	Ideal type of non-monetary asset, limited utility as MoE due to liquidity.
XRP	0.15	Used as reg-arb vehicle and speculative asset. Utility limited to friction-increasing applications. Central parties can censor.
Gold metal (uncoined)	0.4	Non-standardised, prone to dilution, necessitates verification by mass.
Gold coins (pre-state minting)	0.5	Dilution *via* clipping.
Gold coins (state minted)	0.6	Improved anti-forgery.
Soy beans	0.05	MoE restricted to barter, consumption or use as underlying for a derivative instrument.
CHF	0.8	Ideal type of modern fiat currency.
USD	0.7	Inflationary, with supply debasement (Triffin dilemma).
GBP	0.6	Post-reserve currency hangover, Brexit uncertainty.
BTC	0.3*	Post-bootstrap uncertainty.
ETH (2014)	0.05**	
ETH (2018)	0.2**	Not intended to be a monetary asset but has become an MoE and UofA in some circumstances.

Commodityness: Example Scores as of October 2018		
Asset	$\bar{\mathcal{C}}$	Notes
AAPL	0	Ideal type of a non-commoditised asset.
XRP	0.15	Too censorable to be freely tradeable.
DAO	0.45	Hybrid of security and commodity.
BTC	0.9	Ideal type of a digital commoditised asset.
ETH (2014)	0.1	Non-functional network.
ETH	0.7	Used as a digital utility for token sales and persistent scripts.
Gold (metal)	0.95	Ideal type of a legacy commoditised asset.
Gold (state minted)	0.8	Purity assessment and faith in provenance.
Soy beans	1.0	Ideal type of a legacy commoditised consumable asset.
USD (pre-1971)	0.55	Proxy for precious metals, state backed.
USD	0.25	Loss of gold peg, debasement of supply.

Parallel Industries @parallelind · Dec 8

Thinking about the Gnosis crowdsale. The reverse auction, time to finish and amounts raised are well documented, and this article is interesting too. US investors included, 90+% insider allocation, promise of PM as-yet-undelivered. Delisted from Polo. Why?

Blockchain startup Gnosis to freeze tokens after strong sale

After an initial digital currency sale that raised $12.5 million in just 12 minutes, blockchain startup Gnosis has decided to leave most of its remaining curren...

reuters.com

$13.36 (+8.65%)

Updated 9 minutes ago

Gnosis aims to provide an open source platform for the creation of prediction markets.
Using Gnosis, individuals will be able to create prediction markets for events, allowing users to buy shares of the outcome they see as most likely. The project plans to build additional services on top of the core platform to make it easier for users to interact with different markets. Third-party developers will also be able to introduce their own services.

Overview | Profile | Metrics

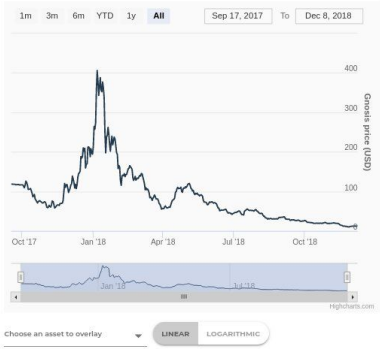
Market Cap	$14.76M
Market Cap Y2050	$0.13B
24Hr Volume	$0.34M
24Hr Price Change	+13.47%
Circulating Supply	1,104,590.00
Y2050 Supply	10,000,000.00
% Y2050 Supply Issued	11.05%
All Time High (01/05/2018)	$461.17
% down from ATH	-97.09%

Historical ROI

1 week	+10.11%
1 month	-33.23%
3 months	-54.88%
6 months	-80.49%
1 year	-87.67%

Supply Snapshot

Type	Fixed
Max	10000000
Portion sold to market	4.17%
Portion held by company	95.83%
Ongoing emission type	N/A



Supply Details

*Gnosis used a reverse dutch auction to sell tokens to the public in an initial coin offering. The terms of the offering were such that if enough coins were purchased quickly, less than 5% would end up in circulation immediately, with the rest held by the issuing company. Since the ICO sold out in under 15 minutes, this is what happened.

1. ICO Insanity

Parallel Industries @parallelind · 44s

Somehow forgot to mention the relationship between GNO and WIZ.

Staking rewards = cashflows = capital asset.

Andrew Kang
@Rewkang

Follow

1) Suprised that no-one has pointed out that the two-token model pioneered by @gnosisPM, and adopted by many other projects (e.g. @SpankChain) is broken and its stability is extremely susceptible to external market volatility

6:21 AM - 27 Aug 2018

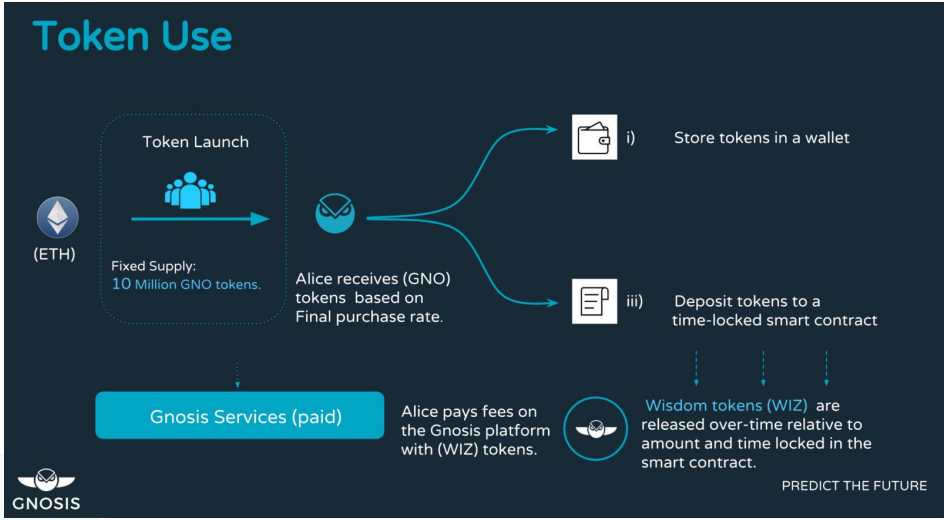
18 Retweets 68 Likes

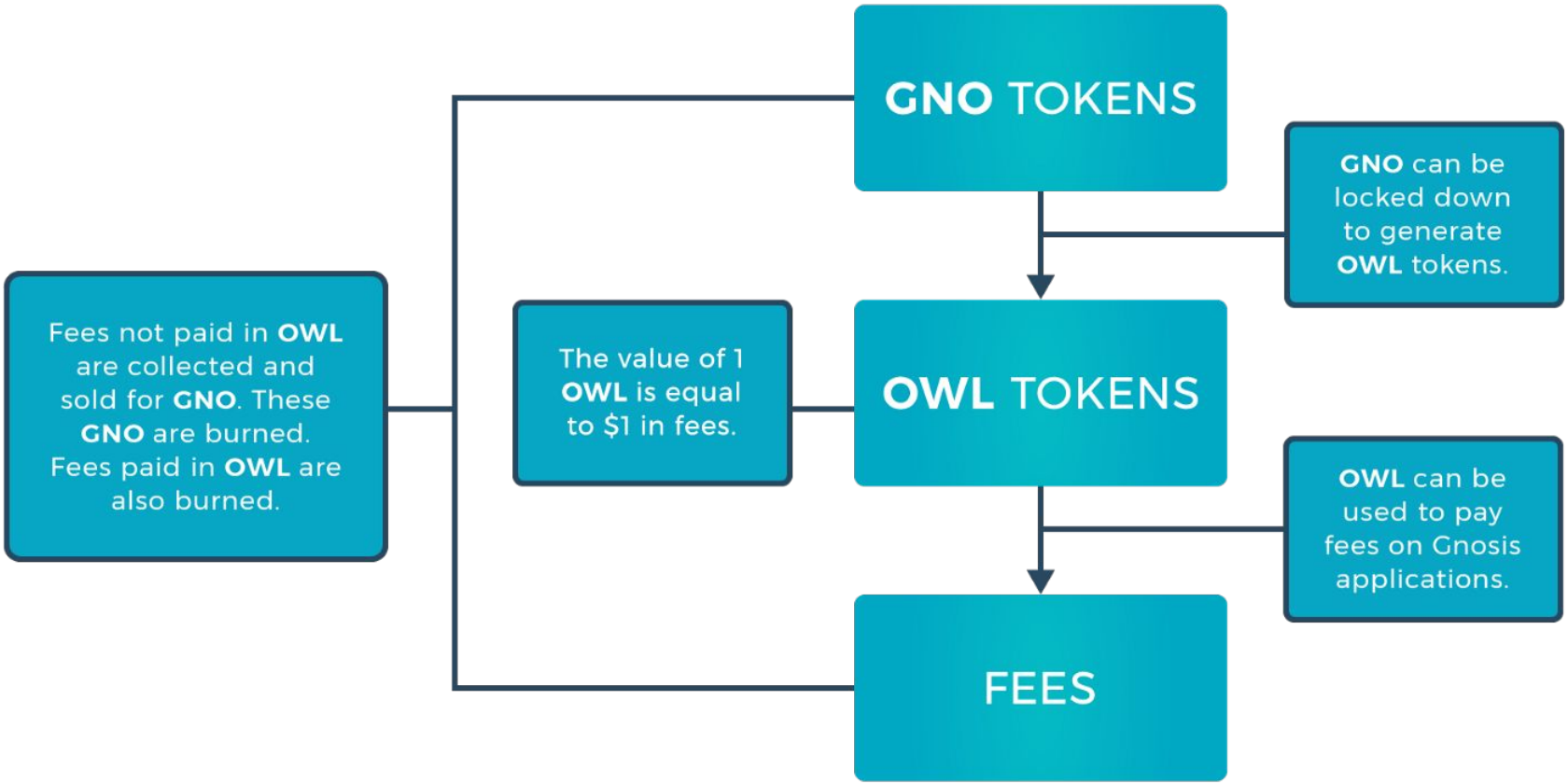
6 18 68

Andrew Kang @Rewkang · Aug 27

6) Intense criticism has been seen by Basis for using a similar approach. Unfortunately, Gnosis's approach to maintaining a peg is even poorer. In their system, monetary supply does not shrink in direct response to price, but instead to fees collected by the system.

1 1 4

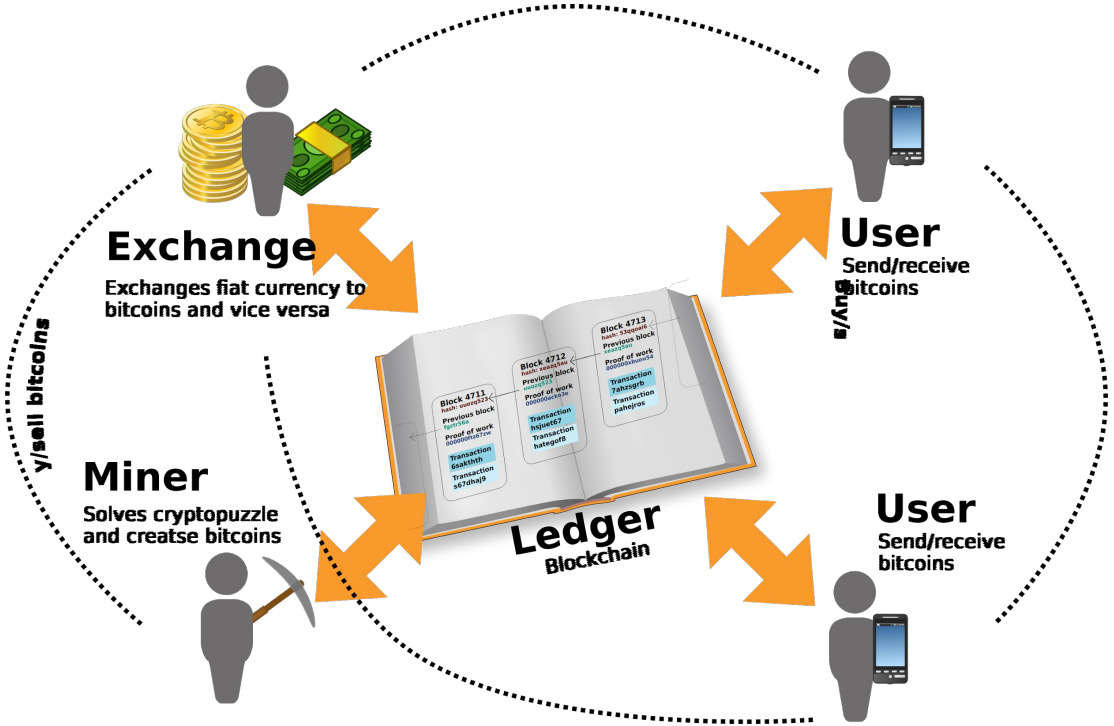



GNO TOKENS
GNO can be locked down to generate OWL tokens.
Fees not paid in OWL are collected and sold for GNO. These GNO are burned. Fees paid in OWL are also burned.
The value of 1 OWL is equal to $1 in fees.
OWL TOKENS
OWL can be used to pay fees on Gnosis applications.
FEES

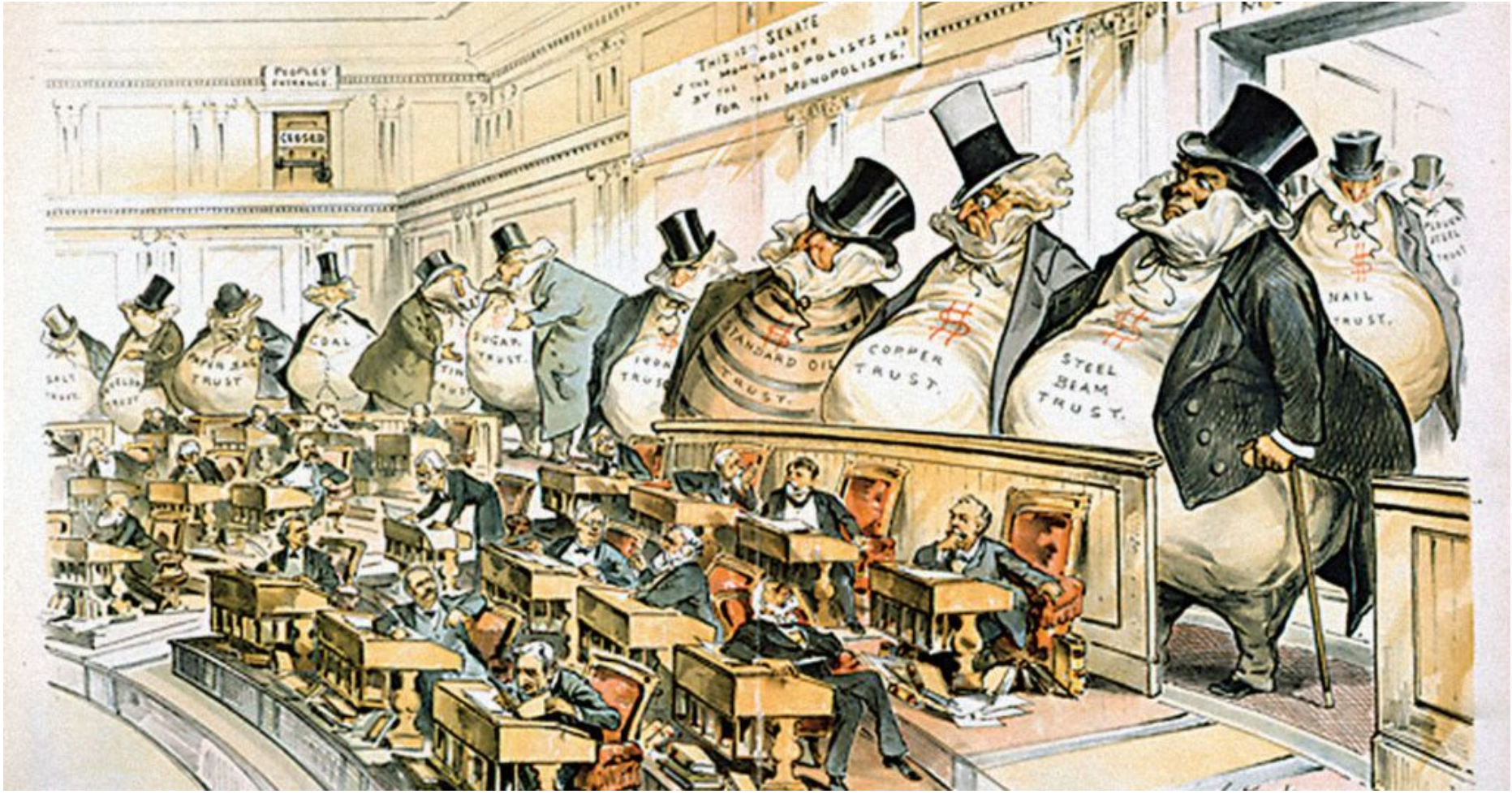
THESE THINGS...DO NOT SEEM TO BE RELATED :)

- Why does Cryptocurrency Matter?
  Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

Network Stakeholders



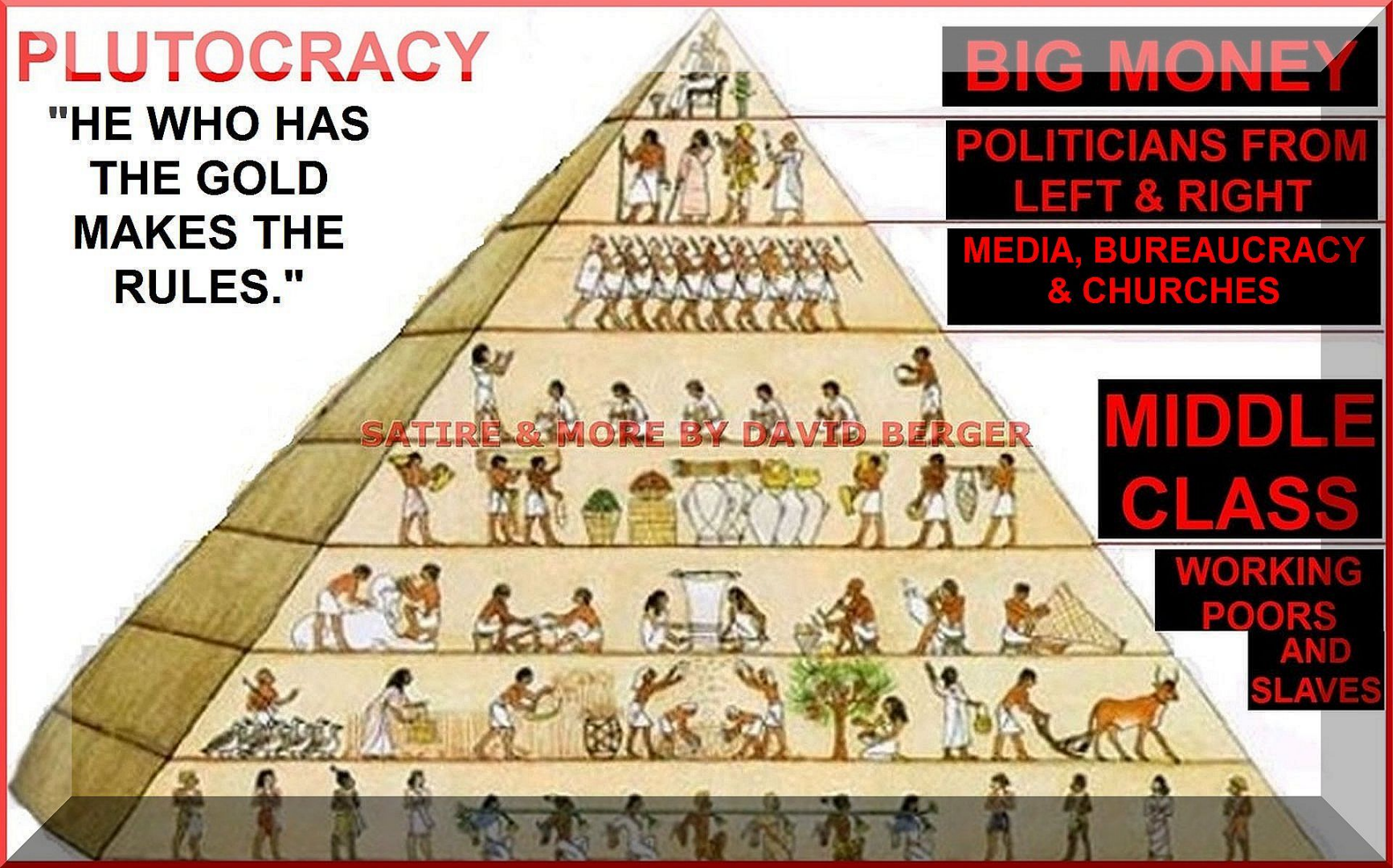
Credit: Robert McCall, Hieronymous Bosch, Lucan Cranach the Elder



Credit: Joseph Keppler,, 'The Bosses of the Senate.' Puck 1889

PLUTOCRACY

"HE WHO HAS THE GOLD MAKES THE RULES."



The Tragedy of the Commons

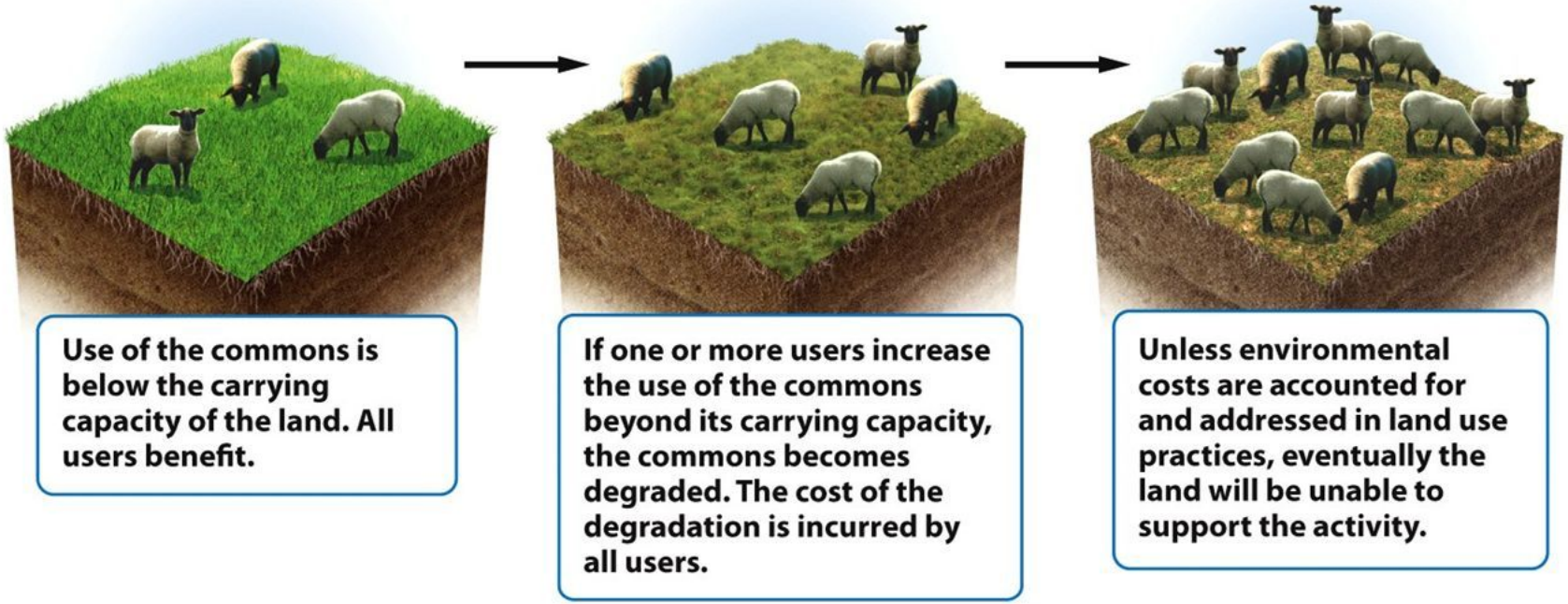


Figure 10.2
Environmental Science
© 2012 W. H. Freeman and Company

Masternode Network

PIRL Premium

Premium Masternodes

20,000 Pirl Collateral
A dedicated or VPS Linux server.
Static public IP Address
Run the main node, content node, and storage node binaries.
Rewarded on 1 Pirl per block for the main node,
and also respective rewards for both the content and storage nodes.

Powered by IPFS

PIRL Storage

Storage Masternodes

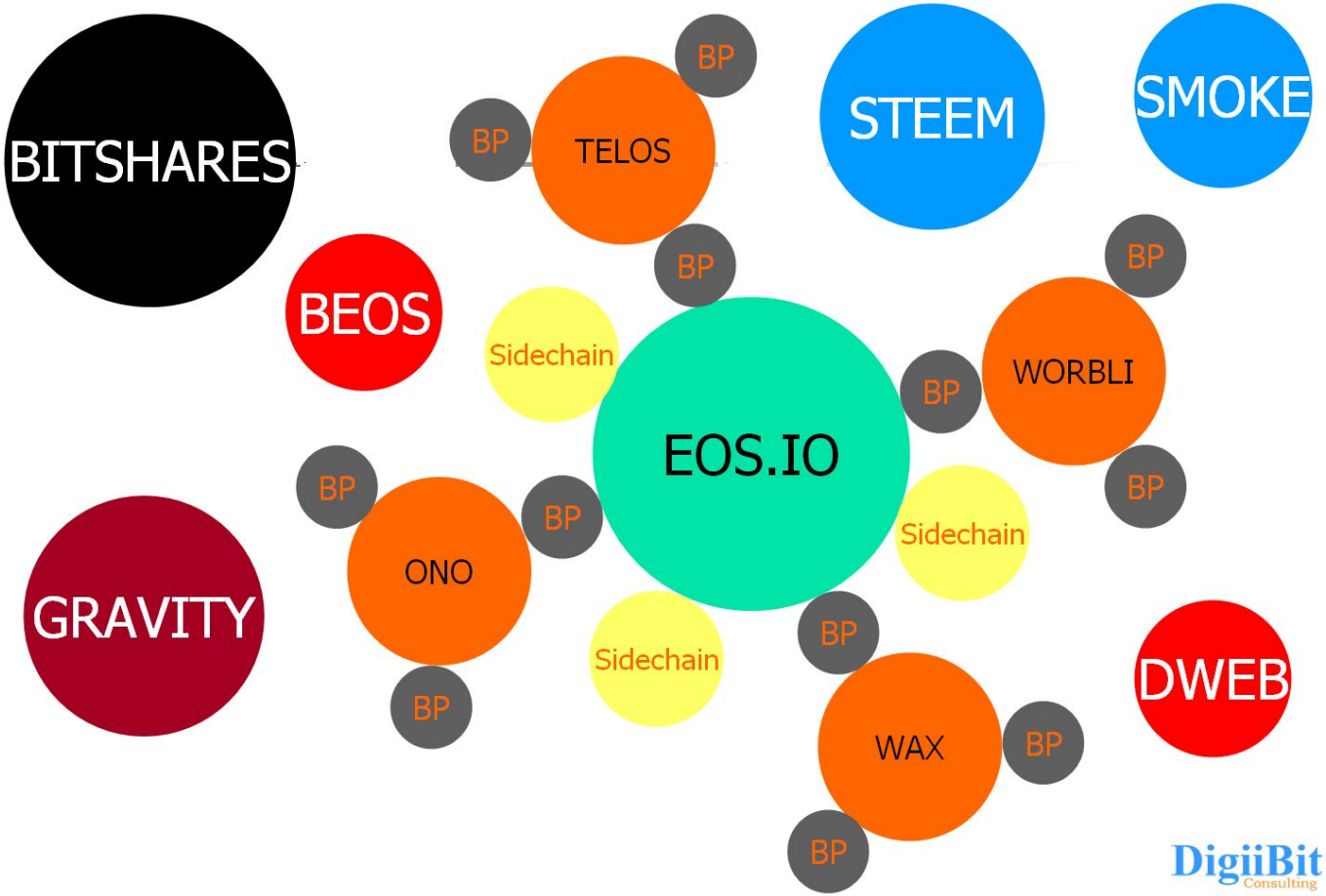
10,000 Pirl Collateral
A dedicated or VPS Linux server.
Static public IP Address
Run the storage node binary.
Rewarded according to
storage space, and bandwidth used.

PIRL Content

Content Masternodes

10,000 Pirl Collateral
A dedicated or VPS Linux server.
Static public IP Address
Run the content node binary.
Rewarded according to bandwidth used.

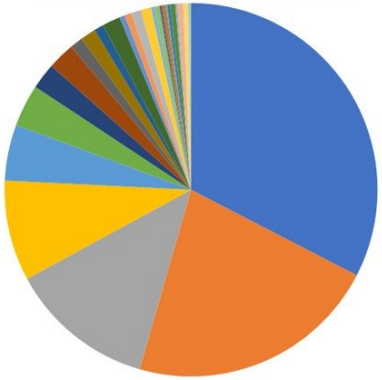
DPoS/Graphene Ecosystem



SO WHICH VALIDATORS ARE MORE DECENTRALIZED?

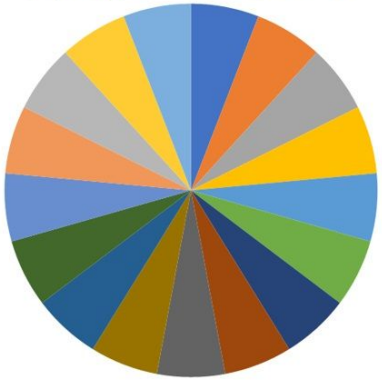
WAVES (LPOS) [a,d]

Forgers by Weight 2017-10-11
http://wavesgo.com/stats#tab-3



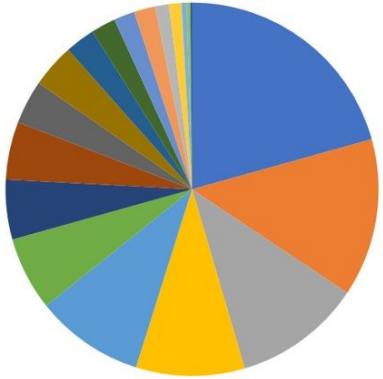
BITSHARES (DPOS) [a,c,e]

Active Witnesses (17, 73 Standby) 2017-10-11
http://cryptofresh.com/witnesses



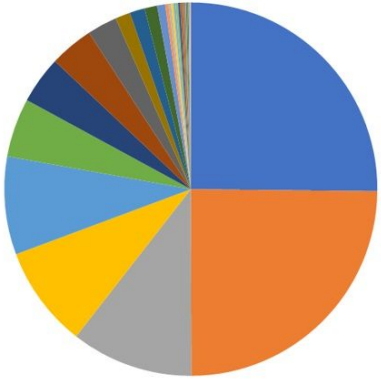
BITCOIN (POW) [a,b]

Mining Pools 2017-10-11
https://blockchain.info/pools



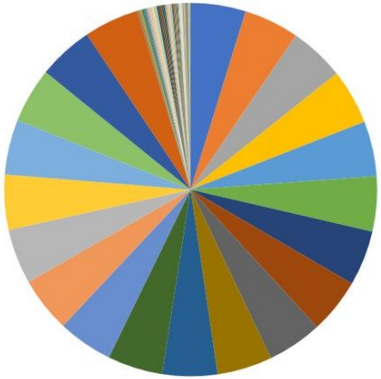
ETHEREUM (POW) [a,b]

Mining Pools 2017-10-11
https://etherchain.org/statistics/miners

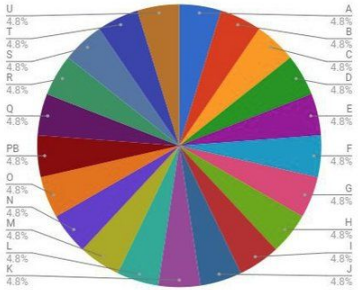


STEEM (DPOS) [a,c,e]

Active Witnesses (20, 68 Standby) 2017-10-11
https://steemd.com/witnesses

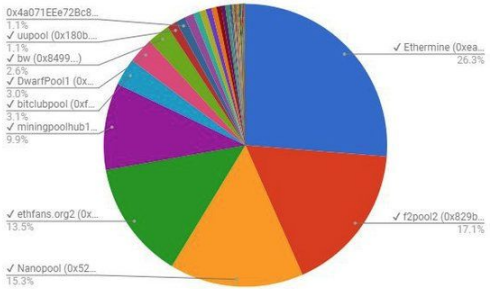


Validators (here meaning block producers) are limited by:
a. full node operators choose preferred version which reject invalid blocks
b. active miners can choose to contribute hash power to a preferred pool
c. stake holders choose up to 33 preferred delegates via approval voting
d. stake holders lease stake to a single preferred pool
e. requires more than 2/3 witnesses to agree to fork



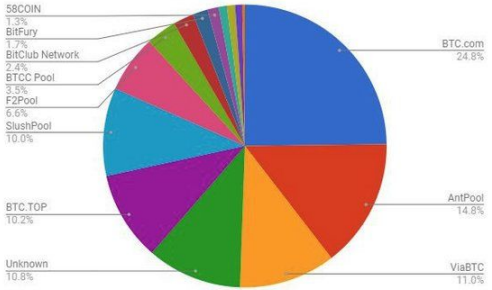
EOS

Source: EOS.IO WhitePaper
21 Block Producers



ETHEREUM

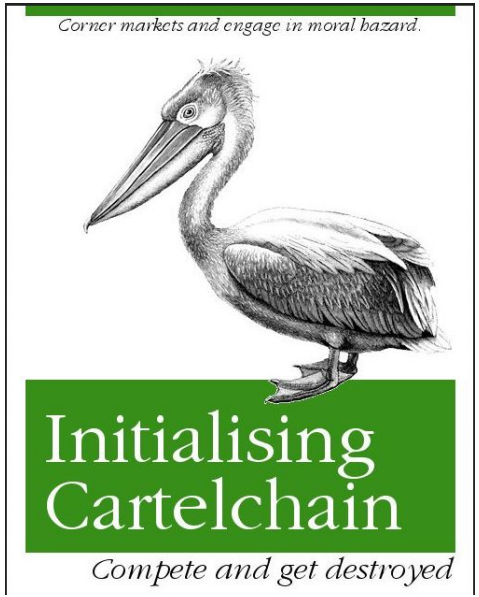
Source: etherchain.org
Top Miners over last 24 hrs

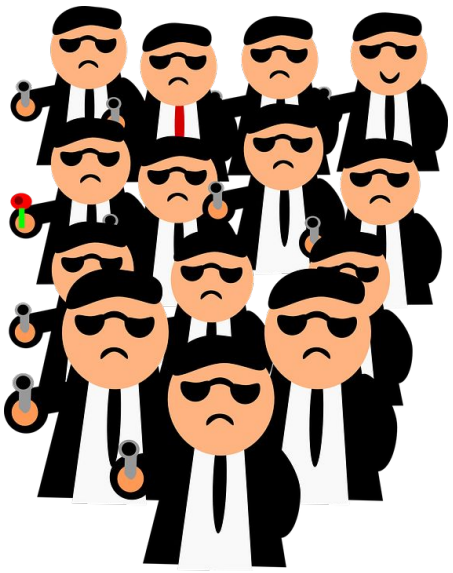


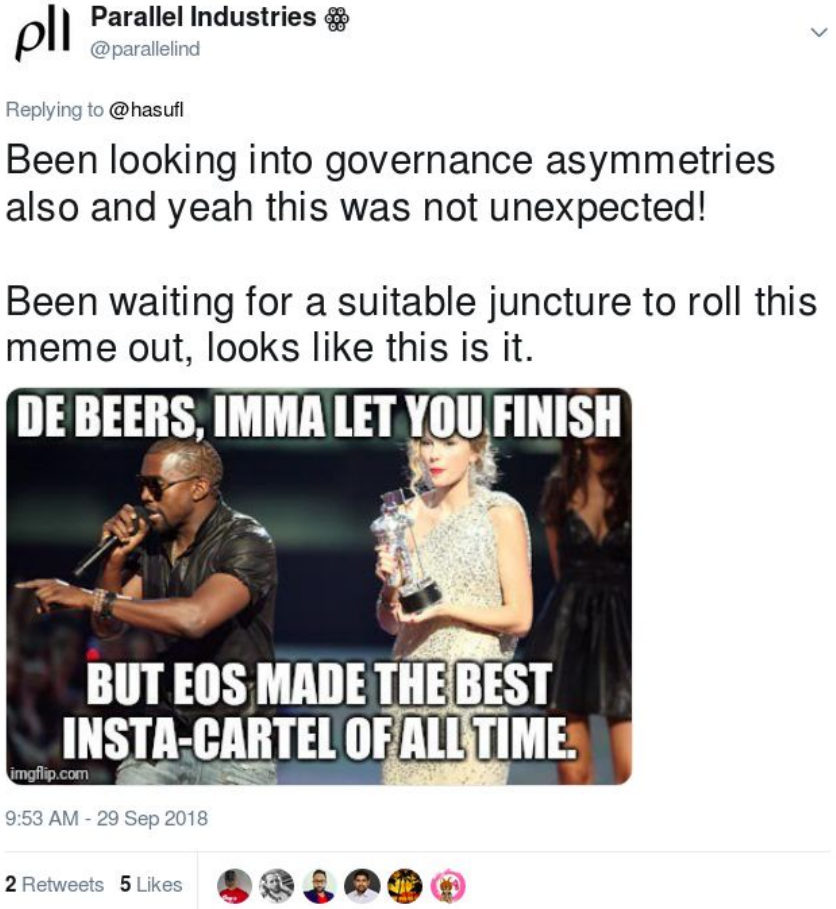
BITCOIN

Source: Blockchain.info
Hashrate Distribution - 4 Days

Hasu @hasufl · Sep 29
I am shocked, SHOCKED, to hear that another DPoS system has converged to mafia-like cartels with collusion and bribery.
Maple Leaf Capital @MapleLeafCap
Recently, an internal excel document from Huobi (one of the BPs) is circulating in the Chinese community. This file documents the collusion, mutual voting, and pay-offs that occur amongst the Chinese BP community. I' m working on getting the file.
Show this thread
15
73
301


Corner markets and engage in moral hazard.
Initialising Cartelchain
Compete and get destroyed




Parallel Industries
@parallelind
Replying to @hasufl
Been looking into governance asymmetries also and yeah this was not unexpected!
Been waiting for a suitable juncture to roll this meme out, looks like this is it.
DE BEERS, IMMA LET YOU FINISH
BUT EOS MADE THE BEST INSTA-CARTEL OF ALL TIME.
imgflip.com
9:53 AM - 29 Sep 2018
2 Retweets 5 Likes

THE DAO IS REVOLUTIONARY.|

Hacking, Distributed

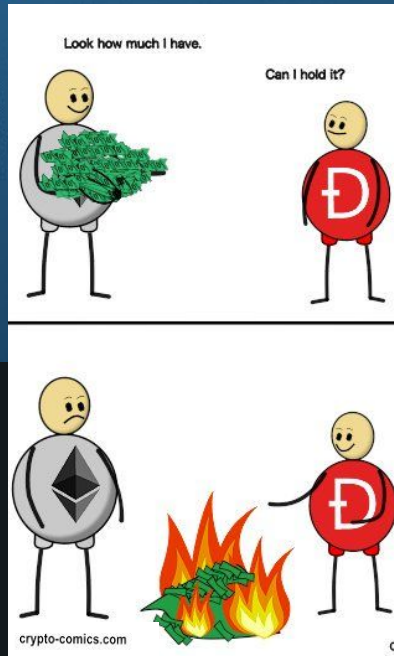
A Call for a Temporary Moratorium on The DAO

ethereum dao smart contracts

Dino Mark, Vlad Zamfir, and Emin Gün Sirer — May 27, 2016 at 01:35 PM

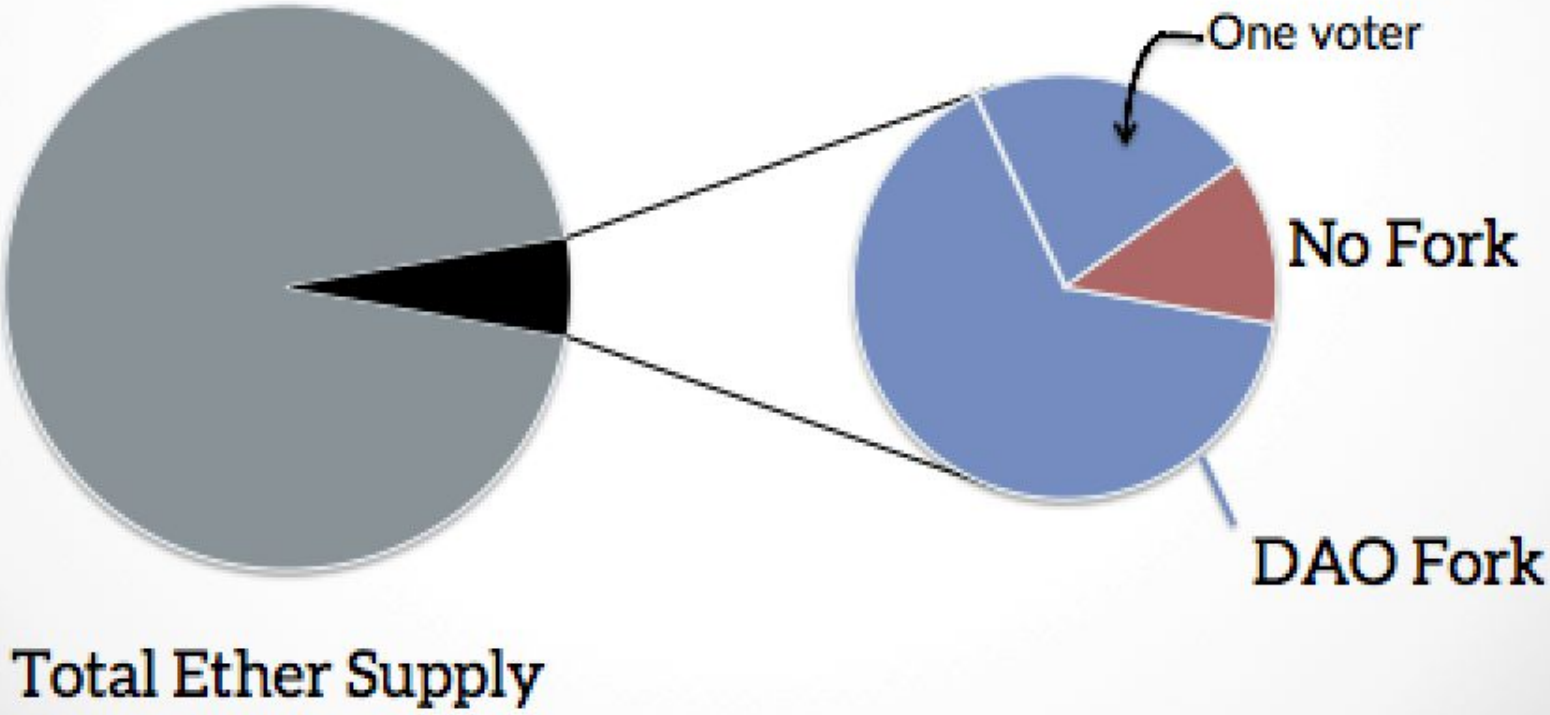
← Older Newer →

The DAO is an exciting new construct: an investment vehicle governed by a program, directed by investors' votes, to seek out and fund proposals.

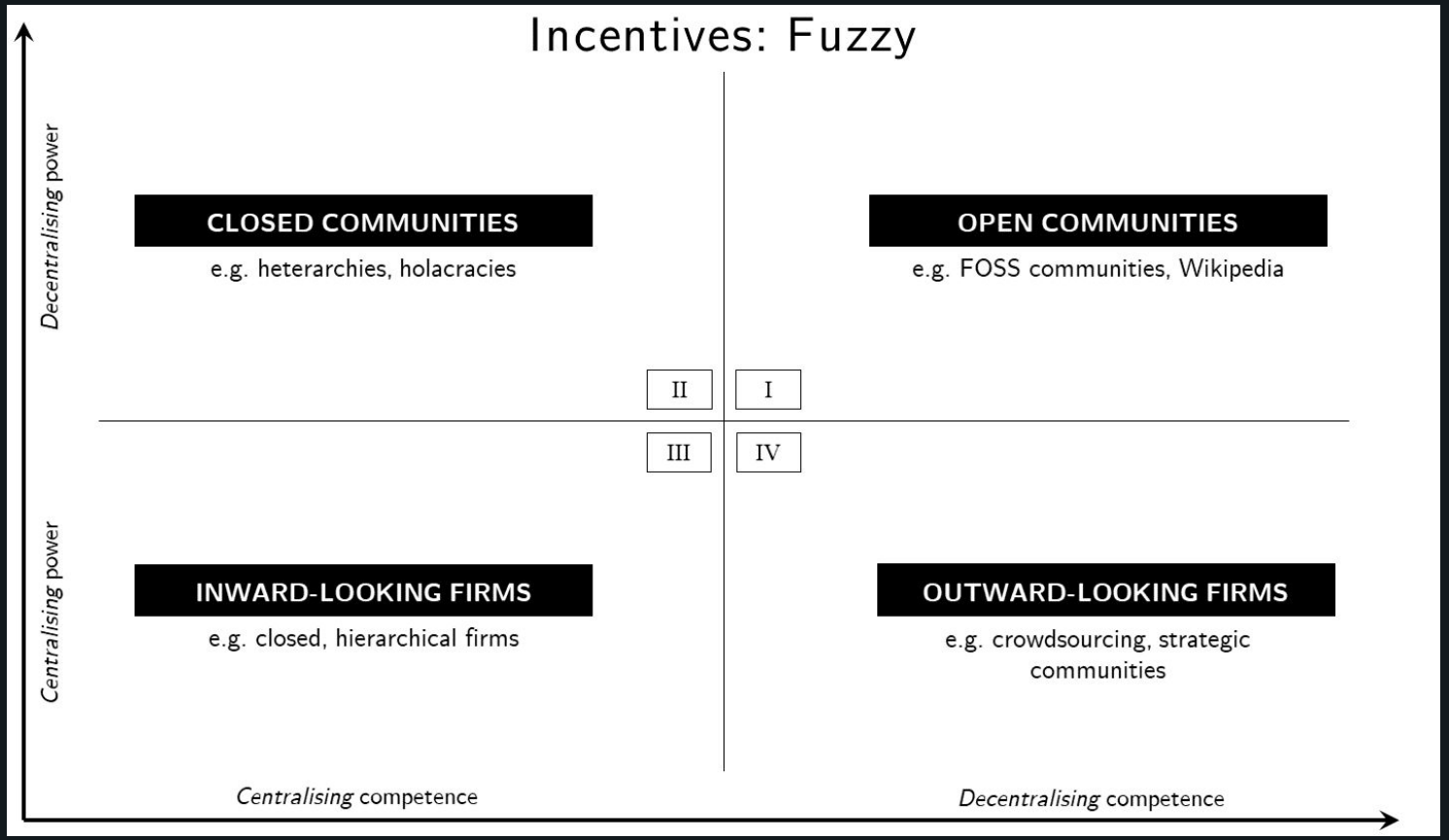


Credit: https://daohub.org, http://crypto-comics.com, http://www.ethereum.org, http://hackingdistributed.com

Credit: http://btcartgallery.com/ethereum-vitalik-yap-island-stone-money-by-biglambda/

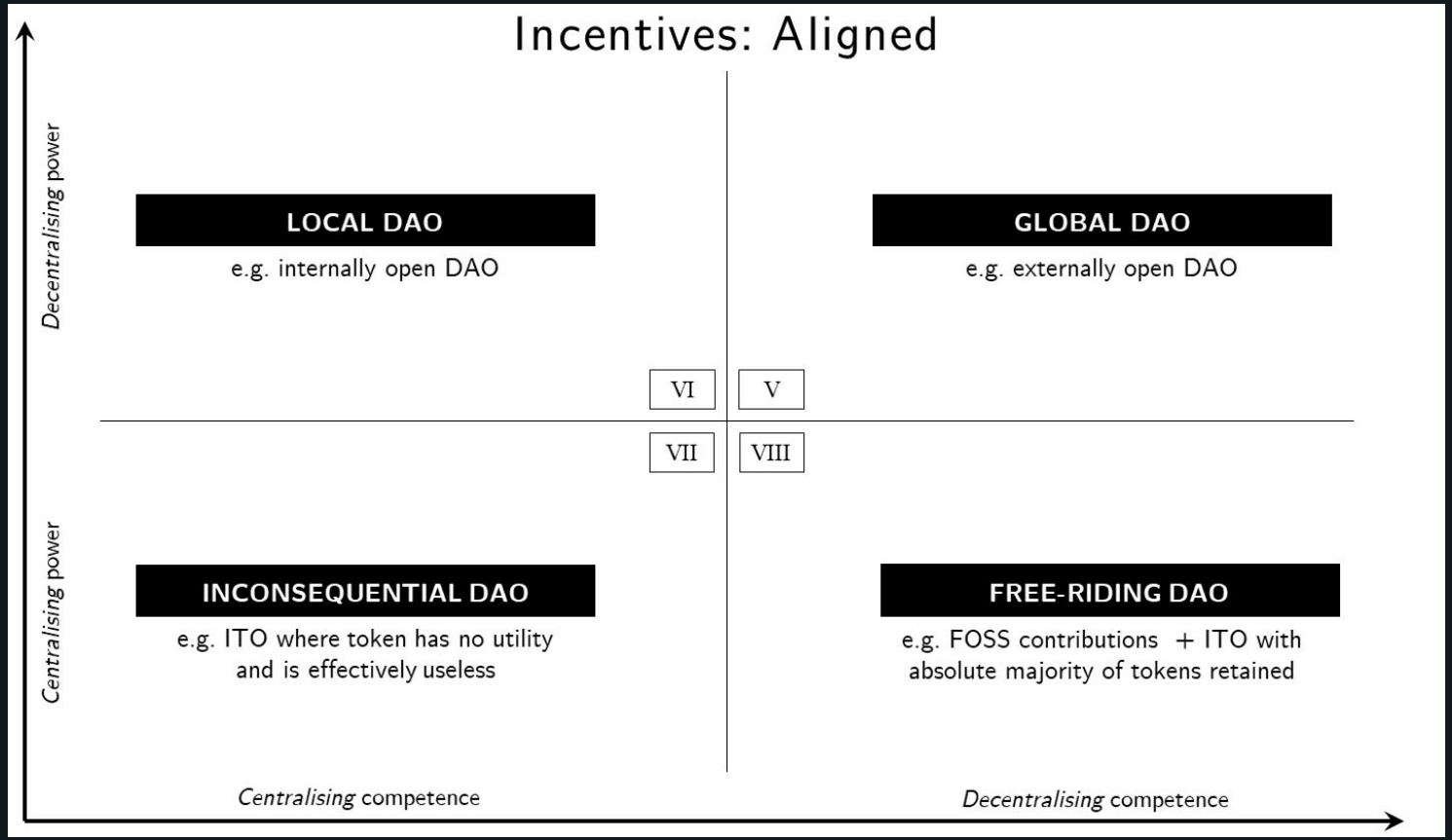

One voter
No Fork
DAO Fork
Total Ether Supply

DAOs STILL HAVE GREAT PROMISE, WHEN CAREFULLY DESIGNED & IMPLEMENTED



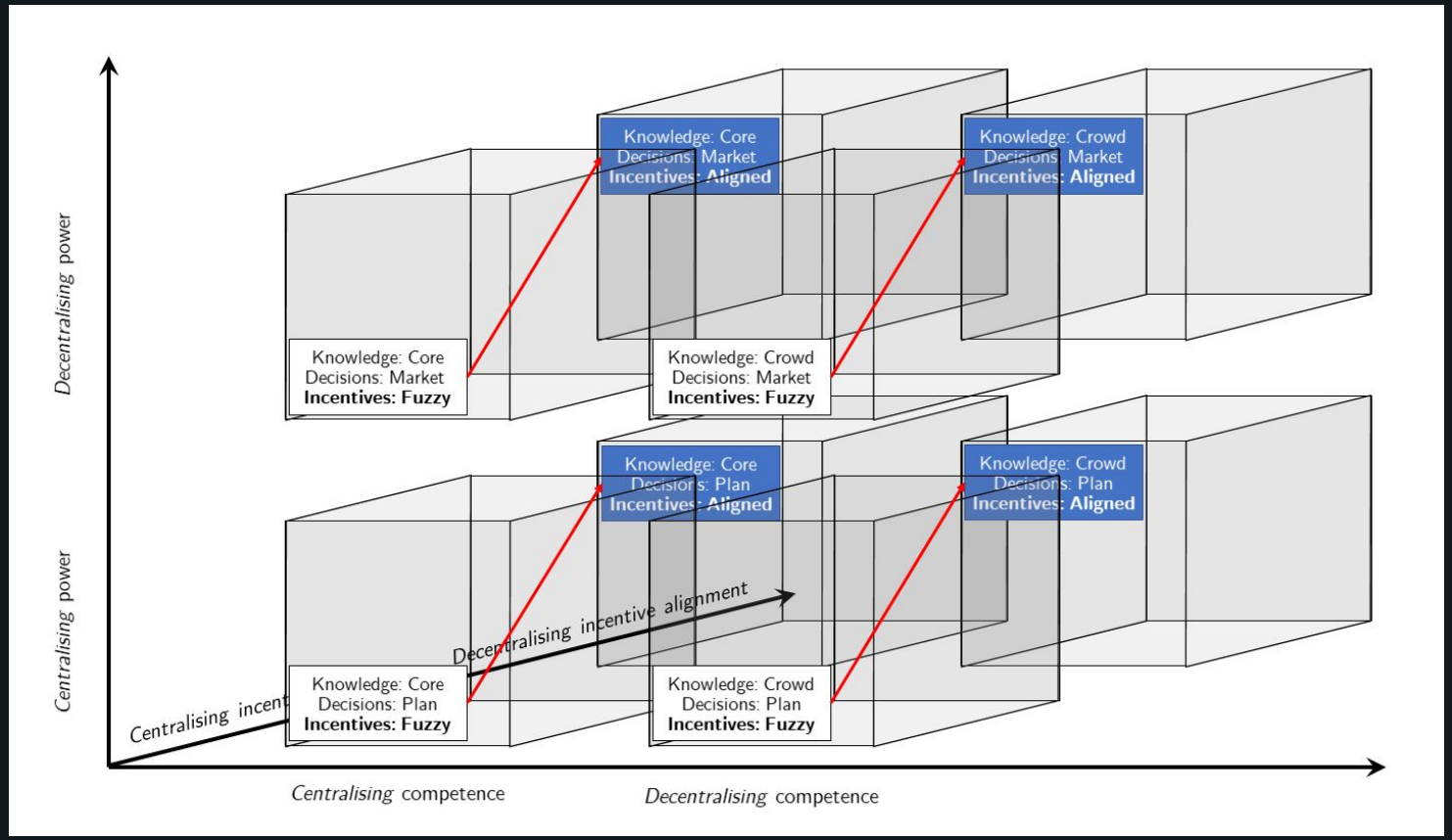
Credit: Theodor Beutel MSc Dissertation, University of Edinburgh, 2018.

DAOs STILL HAVE GREAT PROMISE, WHEN CAREFULLY DESIGNED & IMPLEMENTED



Credit: Theodor Beutel MSc Dissertation, University of Edinburgh, 2018.

DAOs STILL HAVE GREAT PROMISE, WHEN CAREFULLY DESIGNED & IMPLEMENTED



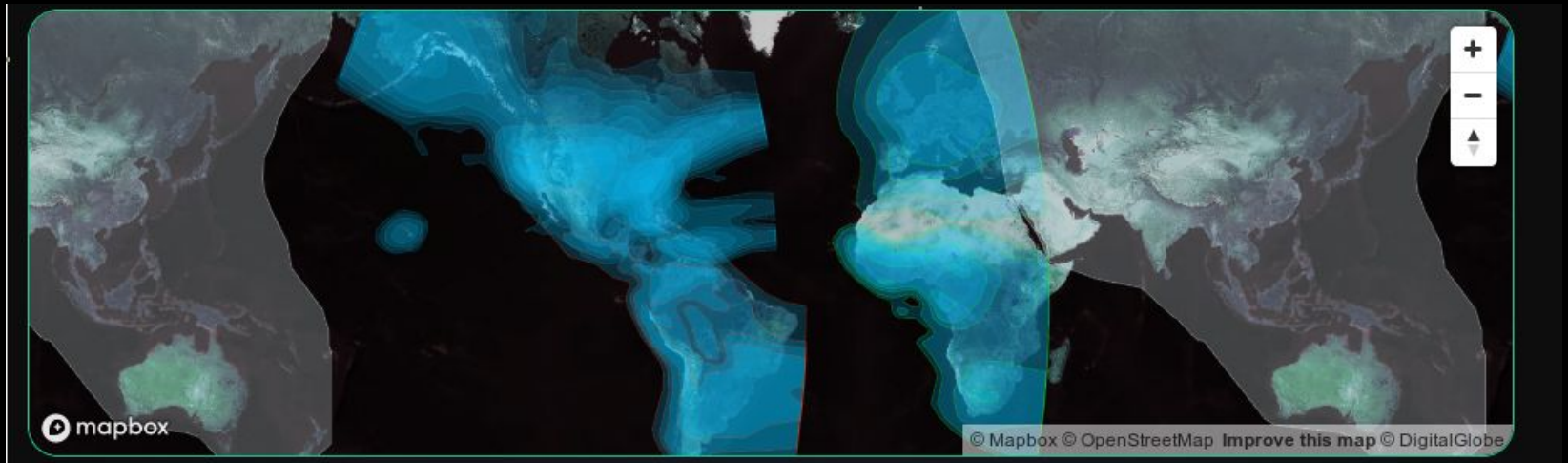
Credit: Theodor Beutel MSc Dissertation, University of Edinburgh, 2018.

THESE THINGS...DO NOT SEEM TO BE RELATED :)

- Why does Cryptocurrency Matter?
  Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

#ReachingEveryone
SHARED MODE
ACCESS POINT

Blockstream Satellite Network:
Receive offline / sync without censorship / verify!



GALAXY 18
North America
Long: 123W
Freq: 12022.85 MHz
Pol: Horizontal

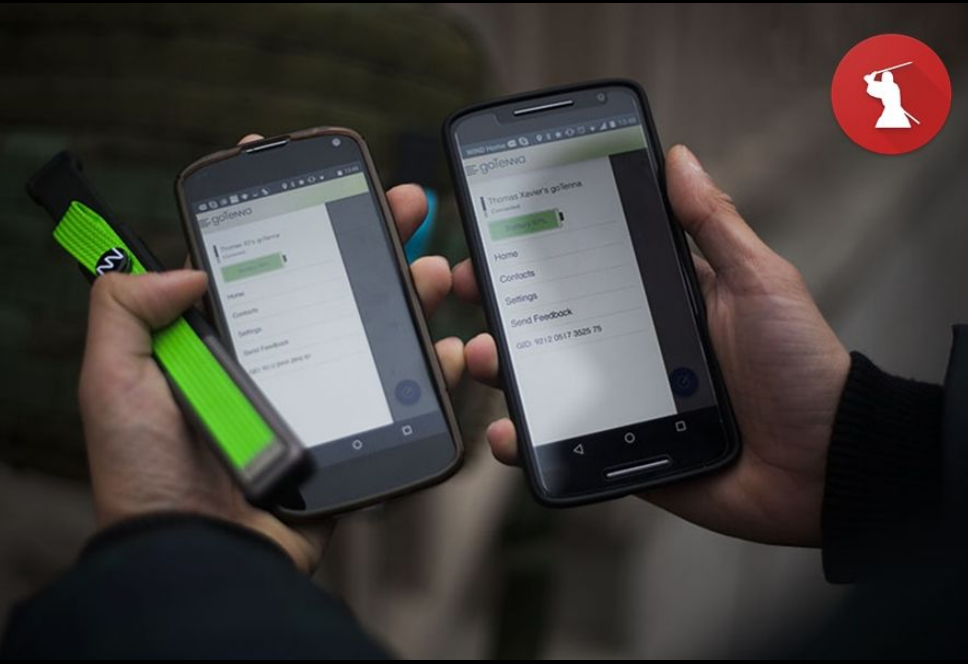
EUTELSAT 113
South America
Long: 113W
Freq: 12026.15 MHz
Pol: Vertical

TELSTAR 11N
Africa
Long: 37.5W
Freq: 11476.75 MHz
Pol: Horizontal

TELSTAR 11N
Europe
Long: 37.5W
Freq: 11504.02 MHz
Pol: Vertical

PHASE 2
Coming Soon
Long: TBD
Freq: TBD
Pol: TBD

goTenna MESH Networking + Samourai = txTenna

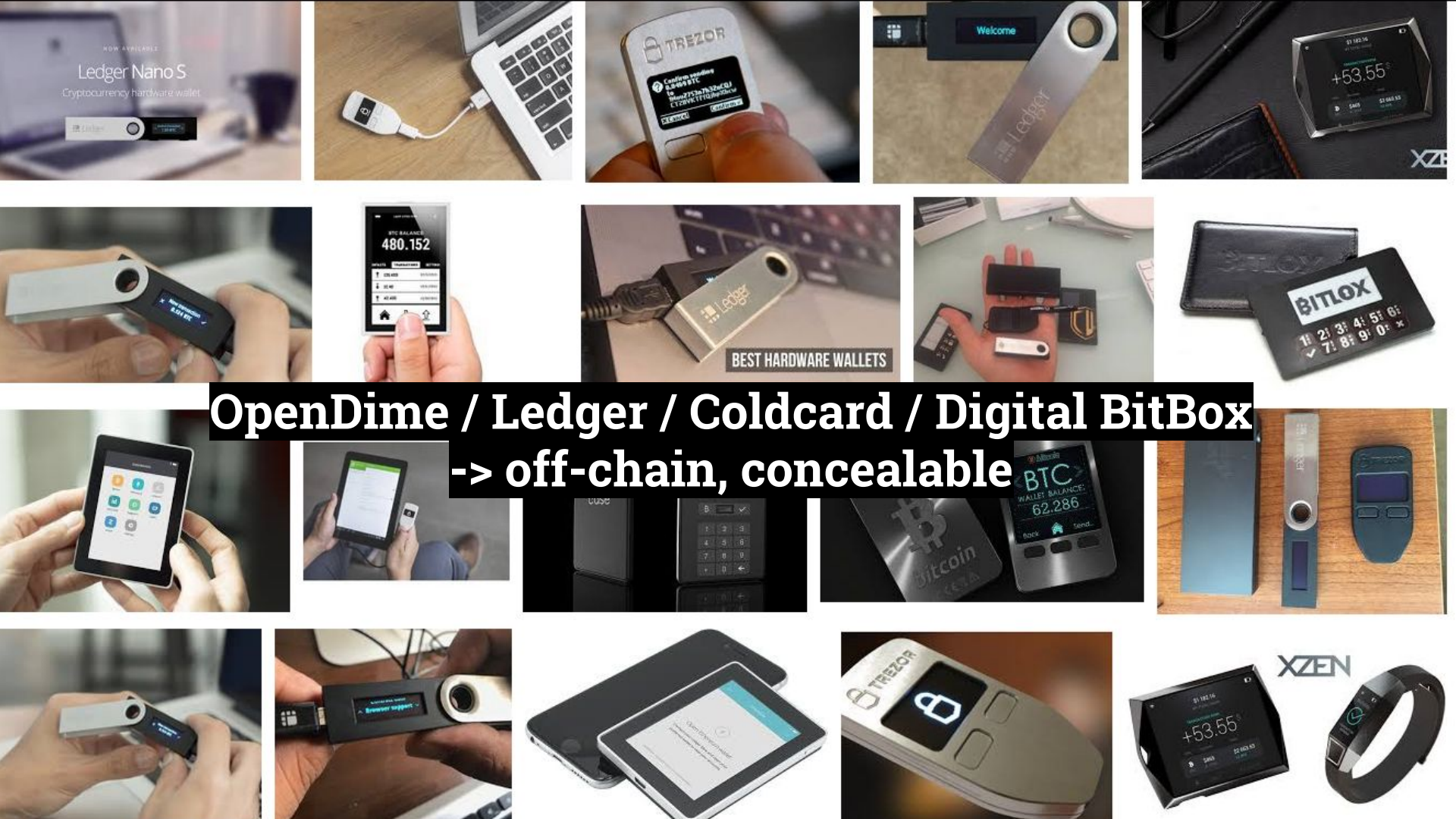


- SMS relay
- satellite hook-up
- fax or any form of hard copy to character recognition
- save to external support (USB)
- Portable Document Format (PDF)
- telex
- HF audio
- Morse code
- meshNets
- NFC
- BLE
- chat apps (especially encrypted)

(Umbrella Revn)

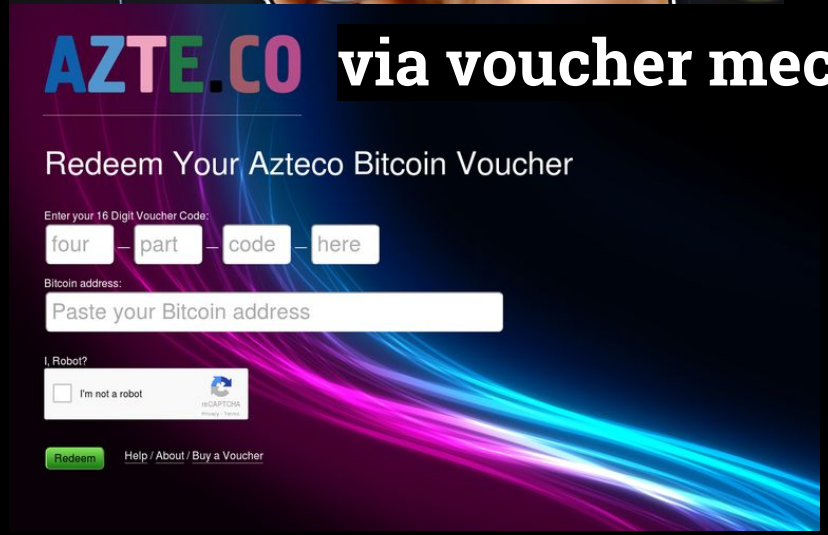
TxTema

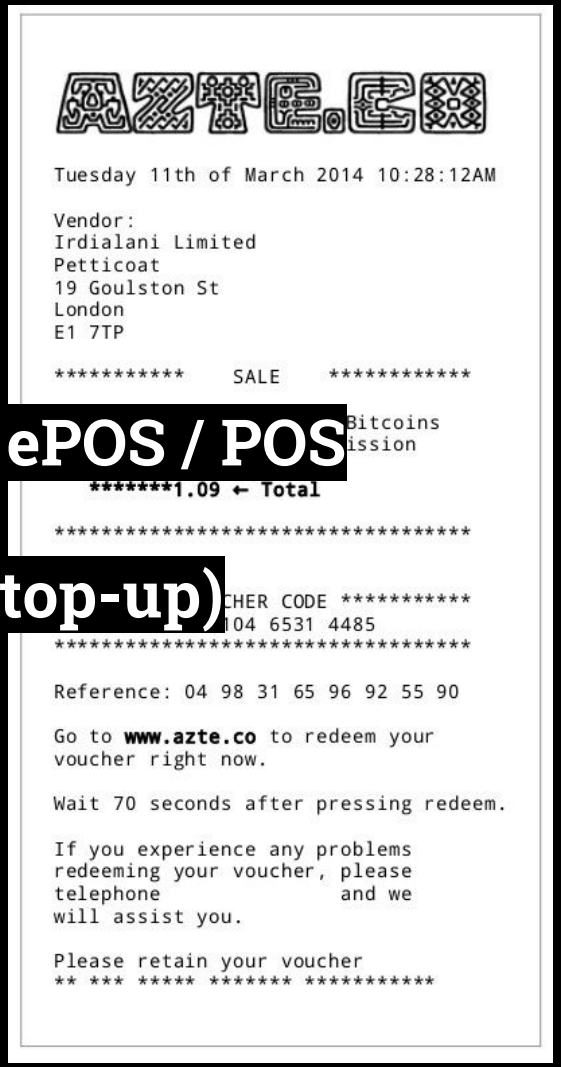
Polymerbit / Tangem / BitNotes
-> Printable, streaming top-up with Lightning
-> concealable, durable, offline



OpenDime / Ledger / Coldcard / Digital BitBox
-> off-chain, concealable

Azteco / Bitrefill - purchase crypto at ePOS / POS via voucher mechanism / mobile top-up)





AZTE.CO

Tuesday 11th of March 2014 10:28:12AM

Vendor:
Irdialani Limited
Petticoat
19 Goulston St
London
E1 7TP

********** SALE **********

Bitcoins
ission

*******1.09 ← Total

****

CHER CODE **********
104 6531 4485
****

Reference: 04 98 31 65 96 92 55 90

Go to **www.azte.co** to redeem your voucher right now.

Wait 70 seconds after pressing redeem.

If you experience any problems redeeming your voucher, please telephone and we will assist you.

Please retain your voucher
** *** ***** ******* **********

Parallel Industries @parallelind · Dec 9

They're really **#ReachingEveryone**

Josh Swihart @jswihart

The group @labitcoineta travels South America to teach people in small towns about Bitcoin. They even use a 📡 to connect to the @Blockstream 🛰️ where no internet is available. So incredibly cool. Grateful for them.

4

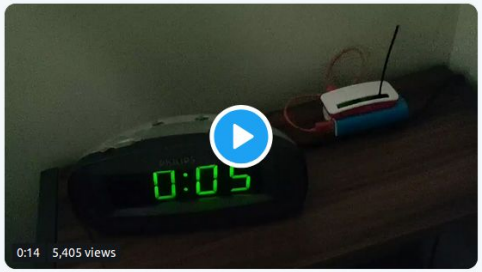
Samourai Wallet and 4 others Retweeted

Matt [Jan/3→🔑] @MattoshiN · Oct 20

Signed raw transaction broadcast over radio.

CC: @parallelind

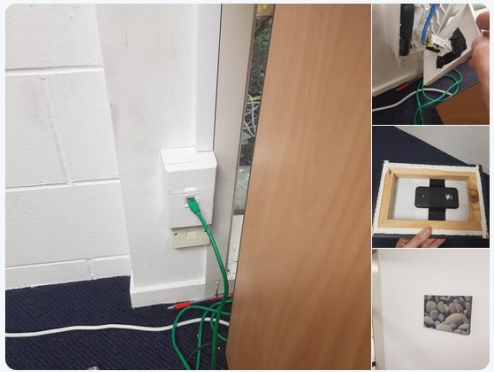
#ReachingEveryone



7 37 127

Coinsure @Coinsurenz · Oct 30

This in effect provides an open wifi access point for bitcoin transactions to anyone with a gotenna. A txtenna user who wishes to conceil their identity can then broadcast from potentially kilometeres away. Much greater distance and an extra degree of anonymity than via open wifi



Parallel Industries @parallelind · Nov 14

Get some range on your node.

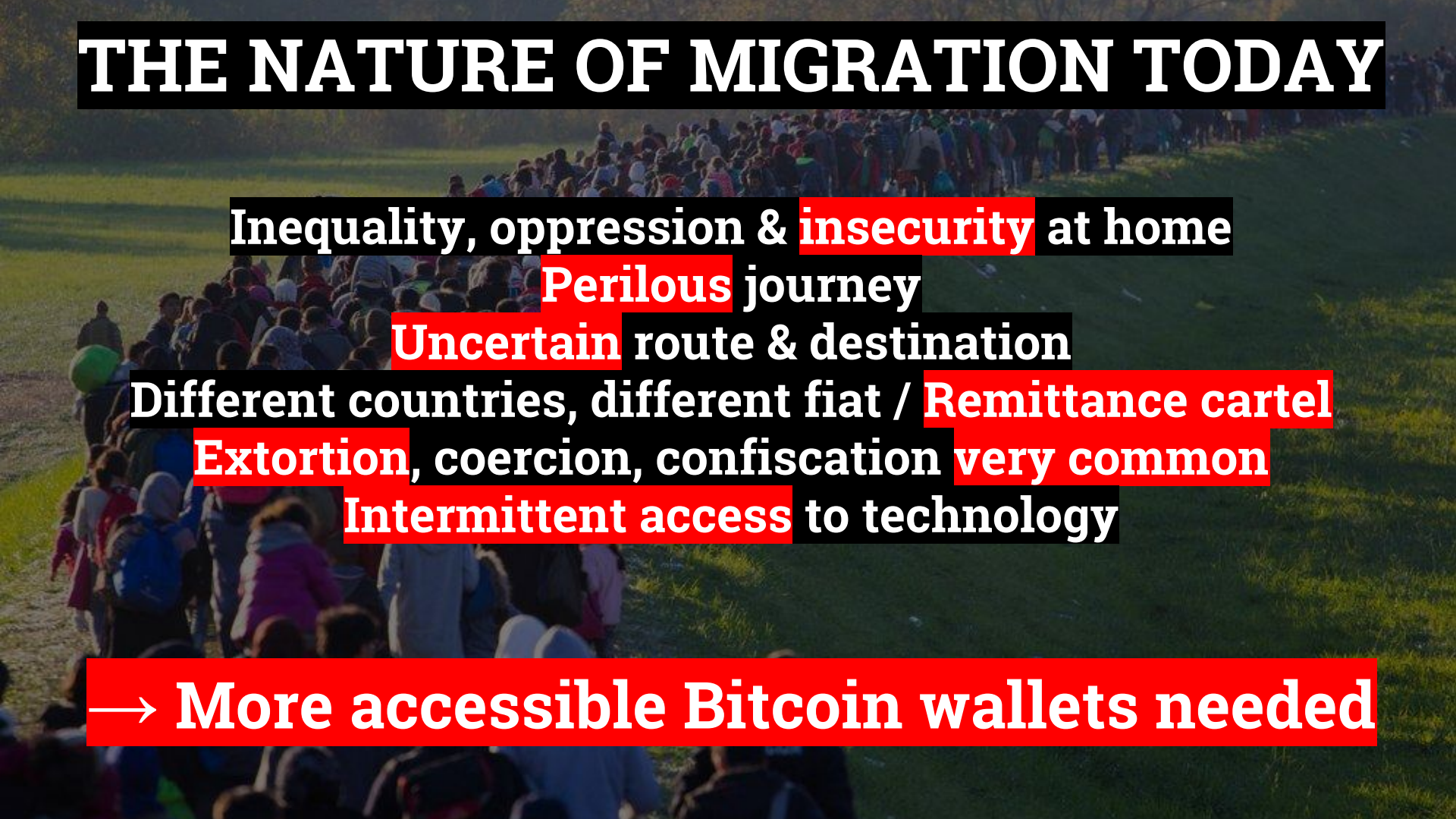
#ReachingEveryone

Pi Supply @PiSupply

Here's a few pictures of the beta boards of our IoT LoRa Gateway HAT for @Raspberry_Pi that we launched on @kickstarter. Packaging and boards looking great. Very pleased 🤗🤗🤗

1 1 5

Proof of Concept:
A Bitcoin wallet for migrants & their families with limited access to infrastructure & technology



THE NATURE OF MIGRATION TODAY

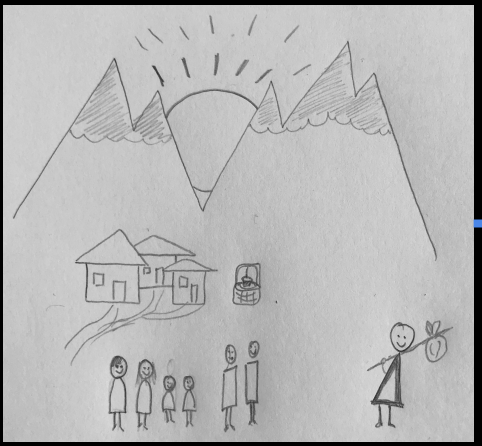
Inequality, oppression & insecurity at home
Perilous journey
Uncertain route & destination
Different countries, different fiat / Remittance cartel
Extortion, coercion, confiscation very common
Intermittent access to technology

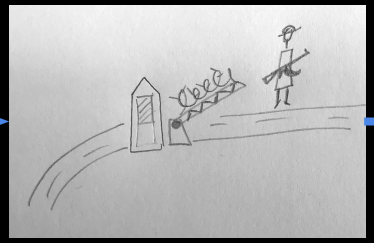
→ More accessible Bitcoin wallets needed

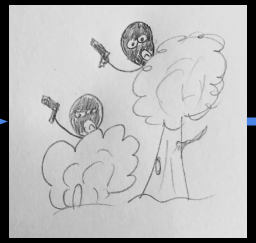
WHY BITCOIN?
DOES THIS NEED A BLOCKCHAIN?

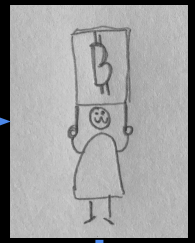
Political & Economic Oppression
Censorship / Extortion / Confiscation

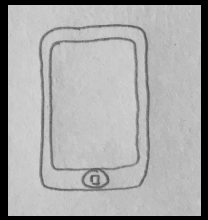
MIGRANT JOURNEY

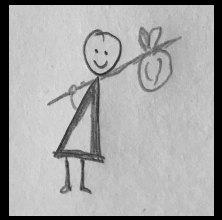


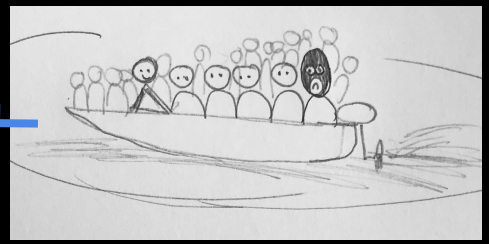


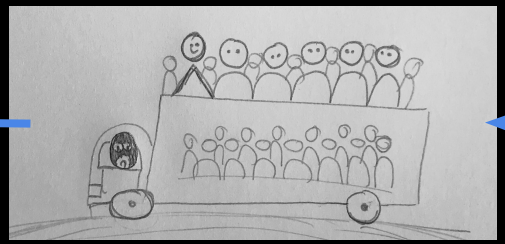


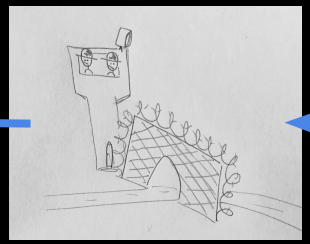


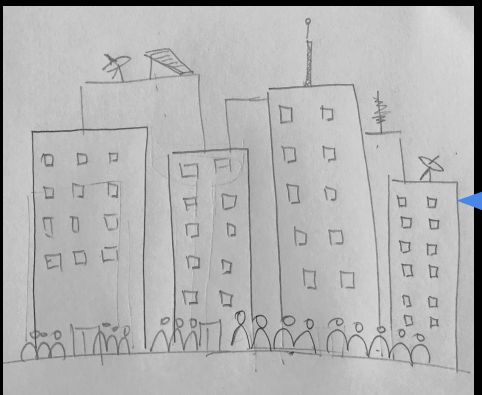




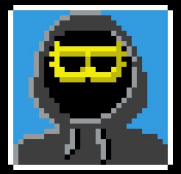








IT'S DANGEROUS TO GO ALONE! TAKE THIS.



BAYT

“BAYT” بيت (HOME)

A simple web wallet

Minimal technology requirements

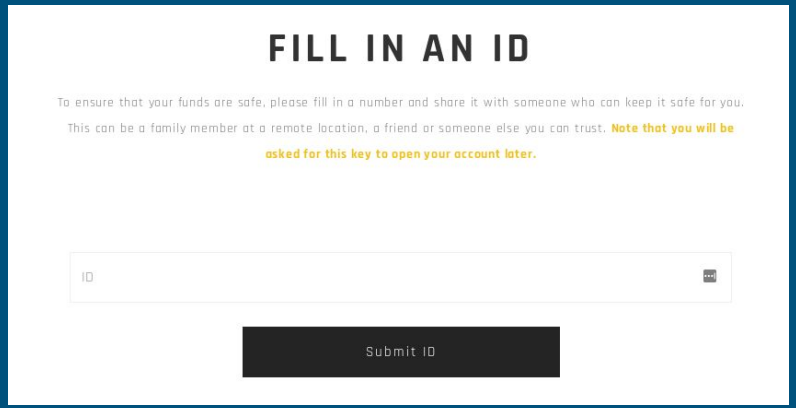
Personal Q&A generates privkey

Drip-feed funds to migrant

→ Minimise extortion / confiscation

(play with our demo @ Table 4 at the back of the room)
http://web.tecnico.ulisboa.pt/~ist186428/chainhack/

“BAYT” WEB APP SCREENSHOTS



(play with our demo @ Table 4 at the back of the room)
http://web.tecnico.ulisboa.pt/~ist186428/chainhack/

SECURITY / TRUST MODEL RELAXATIONS

Censorship Resistance > Security
Imperfect entropy in privkey gen
Hub & Spoke
Web wallet
Insecure devices

THESE THINGS...DO NOT SEEM TO BE RELATED :)

- Why does Cryptocurrency Matter?
  - Cryptocurrency, Decentralisation & the Network Stack
- Apples-to-Apples Comparisons in a sea of Fruit Salad
- Finding New Ways to Understand Asset Characteristics
- Hidden Power Structures in Monetary Networks
- Humanitarian and Political Hacks with Bitcoin
- What's Next?

THANKS FOR YOUR ATTENTION!

WANT TO HELP US DO MORE?

SPONSOR/COLLAB/DISCUSS:

info@pllel.com, www.pllel.com, @parallelind

BTC

BTC: 1GgUDrQvdycsr473eMJQZq4GYTgGUdJQfn
ETC: 0x9ec1e3aa7b7428dfa9d22685c33267d90afa2c80
ETH: 0x3c260b1b53dbc122068b98da7a7c196df4dc1211
DOGE: DKPYfbidZUqmcCa79rT5ZBh92RoqQNv4WR
LTC: LTGS78HRTJbSEo7Y5PxYXj1XE2ZYPh3NM5
ZEC: t1LktPAdT6bTuNTgQt97JZRRKXfq6cit3bt

2.2 Research Methods and Resources

This work has relied on numerous primary and secondary data sources as cited in the text. Blockchain analytics of BTC, BCH, ETH, ETC, XMR, MONA, ZCL and BTCP was achieved through the use of block explorers Blockchair.com, Blockchain.info, Etherscan.io, Etherhub.io, Bchain.info, Monerohash.com and Bitinfocharts.com with data exported in CSV or JSON formats. This was imported into the statistical computing suite RStudio (built upon R) for cleaning, treatment, analysis and visualisations. Network-wide observation and inference was conducted using publically available sources Coin.dance for node count and implementation versions for BTC and BCH, Crypto51.app for ZCL and BTCP network hashrates, Doublespend.cash for malleated transactions on BCH, Coinmetrics.io for high-level network heuristics and Onchainfx.com for networks' token price, supply issuance and monetary policy.