SOUNDCRYPTO

Seattle Estate Planning Council
May 16th 2018

Douglas Faust: faust@soundcrypto.com

Overview

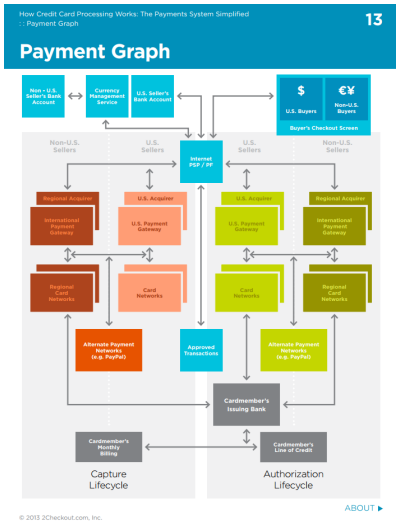
- What is cryptocurrency, Bitcoin, blockchain?
- Mythbusting; pizzas, Ponzis, pseudonymity
- Regulatory climate(s)
- Cryptoassets in a contemporary portfolio
- Beyond Bitcoin – the cryptoasset circus
- How blockchain technology may change contract law

A Payment Rail For The Internet?

- Automated Clearing House (ACH): slow
- Credit card payment networks: limited access, insecure, censorable
- David Chaum's "DigiCash" (1993)
  - Courted by Microsoft and Visa
  - Employed several key crypto-currency figures
- PayPal – essentially a nice user interface on credit card payment networks
- At least 20 more serious attempts starting in the late 1980's….

"How Credit Card Processing Works: The Payments System Simplified"

- Tens of billions of USD in fraud per year
- Small fraction of the internet-using population has access
- Fees offset by "data farming"



https://www.2checkout.com/upload/documents/wp_How_Credit_Card_Processing_Works.pdf

Bitcoin (2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

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

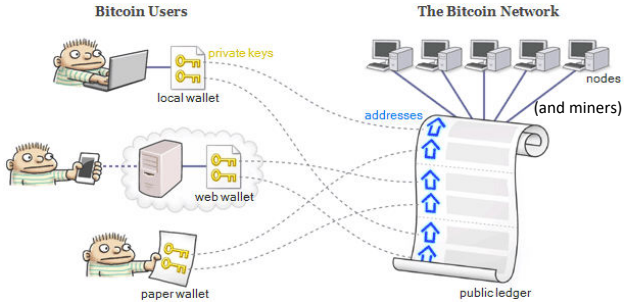
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

https://bitcoin.org/bitcoin.pdf

- Fully decentralized: No trusted 3rd parties!
- Uses a native asset, "bitcoin"

The Bitcoin Network Protocol:

1. Users broadcast new transactions to all connected nodes
2. Each node collects new transactions into a block
3. Each node works on finding the nonce to sign the block (proof of work)
4. When a node finds the proof of work, it broadcasts it to all the nodes
5. Nodes accept the block if all transactions are valid
6. Nodes express their acceptance by using the last block's hash to start the new block



http://preshing.com/20140127/what-is-a-bitcoin-really/

Current distribution of Bitcoin nodes

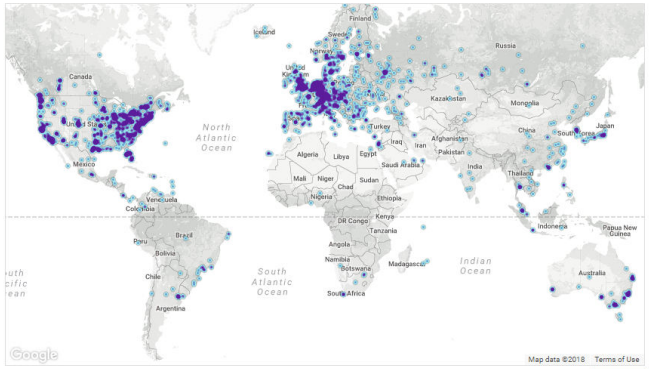
GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Wed Jan 17 2018 21:51:24 GMT-0800 (Pacific Standard Time).

11543 NODES
24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	3194 (27.67%)
2	Germany	1947 (16.87%)
3	China	825 (7.15%)
4	France	784 (6.79%)
5	Netherlands	516 (4.47%)
6	Canada	465 (4.03%)
7	United Kingdom	440 (3.81%)
8	Russian Federation	376 (3.26%)
9	n/a	304 (2.63%)
10	Singapore	252 (2.18%)

More (105) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

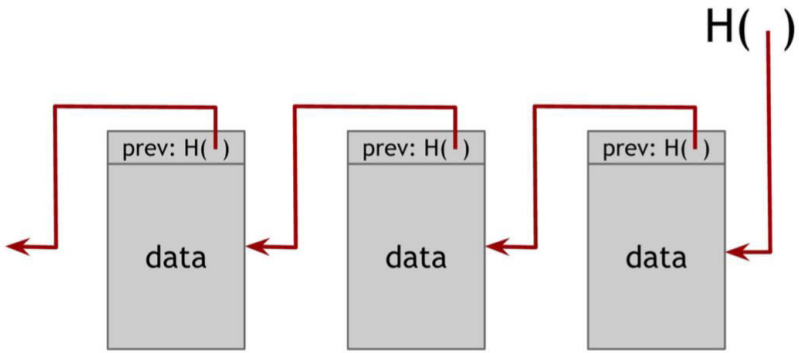
LIVE MAP

http://bitnodes.earn.com

The Bitcoin network has been running, uninterrupted, since 2009

The blockchain ledger of transactions replaces the trusted 3rd party

https://anders.com/blockchain/blockchain.html



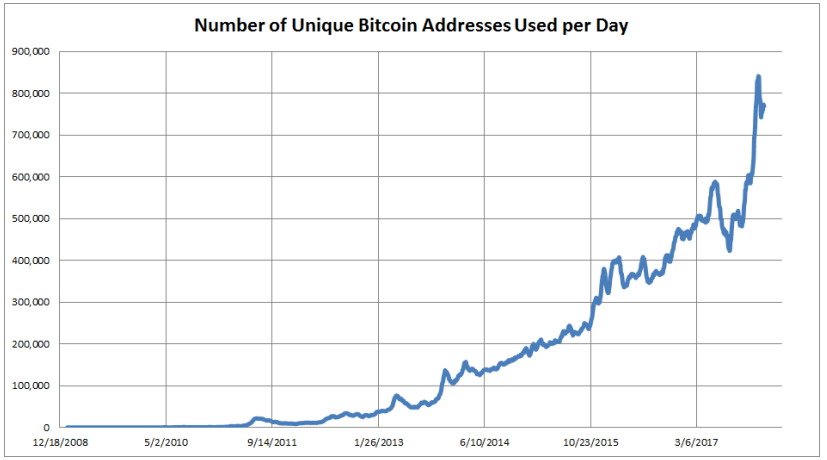
- ❑ Easy to check that the transactions are valid (digital signatures)
- ❑ Hard, by design, to assemble transactions into a valid block (Proof of Work)
- ❑ Operationally: Blockchain is an APPEND-ONLY ledger

Why are people and institutions all over the world so interested in using their computing resources to verify? (~250k transactions/day)

https://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic

1. **The successful miner of the most recent block gets a reward (12.5 BTC)**
2. **Users put extra BTC in their transactions to get them in the next block (~1%)**

User base is hard to track precisely, but all metrics indicate an exponential growth.



Data from blockchain.info

Cryptocurrency mythbusting

"The price went up by an astonishing rate, therefore Bitcoin must be a…"

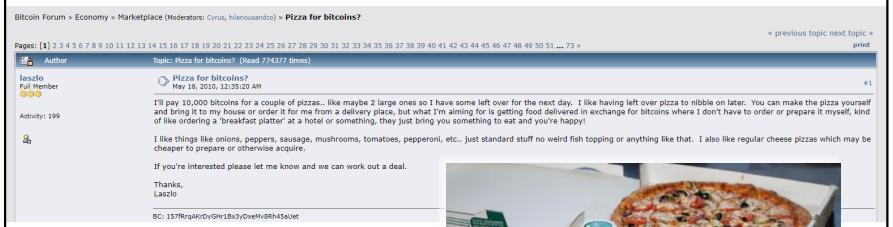
- **Ponzi scheme**
- **Tulipmania**
- **Other, completely new, type of scam**

"Bitcoin's anonymity makes its primary use case criminal activity"

"Bitcoin is immoral as the energy usage in mining is more than some small country"

"There is no basis for any solid valuation of bitcoin."

"The price went up by an astonishing rate, therefore Bitcoin must be a…"



https://bitcointalk.org/index.php?topic=137.0

The price appreciation, if you start from when the first large exchange opened (2011) is more like 250% annualized

"Fine. But I still think it's some type of scam…."

Who could possibly be doing any misleading?

Open source protocol:
https://github.com/bitcoin/bitcoin
https://bitcoin.org/bitcoin.pdf

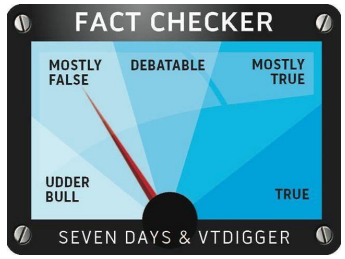
Based on cryptography published in academic journals in the 1970's and by the NSA in the 2000's
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
https://en.wikipedia.org/wiki/SHA-2

Open source wallet software

Public ledger
https://blockchain.info (for example)

"Bitcoin's anonymity makes its primary use case criminal activity"

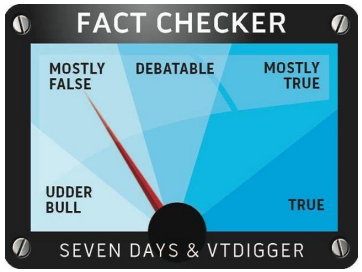
Much less true than it used to be.



- First large merchant, Silk Road
- First large exchange, Mt. Gox

"Bitcoin's anonymity makes its primary use case criminal activity"

Much less true than it used to be.



Bitcoin is not *anonymous*, it's *pseudonymous*. You're known only by your Bitcoin addresses, which can be linked to you.†

All address balances and every transaction EVER are on the blockchain

† Other cryptocurrencies are anonymous; Monero, Dash, Zerocoin, Zerocash….

Some blockchain exploring!

https://blockchain.info/address/3Q2KXS8WYT6dvr91bM2RjvBHqMyx9CbPMN

https://blockchain.info/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

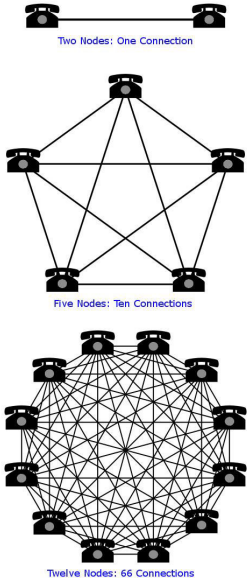
Cryptoasset (US) regulatory climate

- IRS: bitcoin is property
- CFTC: bitcoin is a commodity
- SEC: bitcoin is not a security (but other cryptoassets might be)
- FASB (GAAP): ¯_(ツ)_/¯

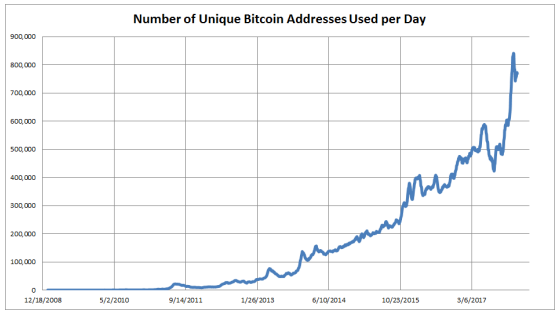
"There is no basis for any solid valuation of bitcoin."
aka Digital Tulip objection

- Networks have value: Metcalfe's law
- Permission to make a transaction has value: NVT ratio
- Currencies have valuation metrics: Quantity Theory of Money

CAVEAT: the first two are young ideas, the last one is descriptive not predictive.

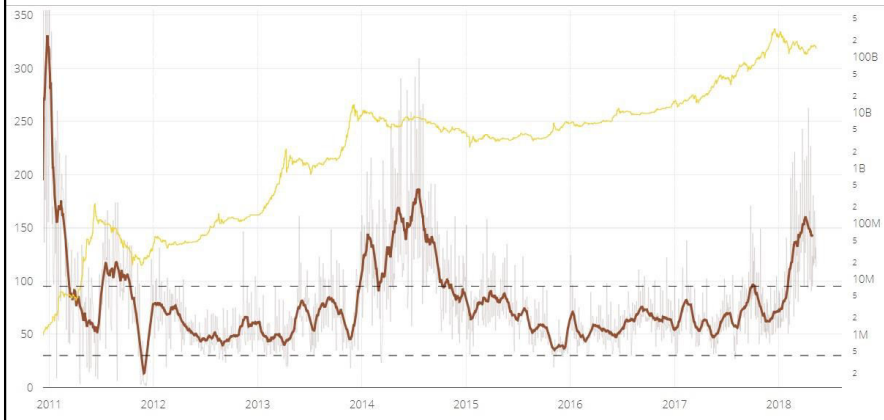


Metcalfe's Law (~1980, not Bob Metcalfe)



Data from blockchain.info

Network Value to Transactions (NVT) Ratio:
value of network / value flowing through network
"Bitcoin's P/E ratio"



(Ratio has been smoothed using moving averages, 14 day forward and 14 day backward facing)

http://charts.woobull.com/bitcoin-nvt-ratio/

Hey, it's a currency!

Quantity Theory of Money / Fischer's Equation of Exchange

$$MV = PQ$$

M = Money Supply

V = Velocity of Money

P = Price Level

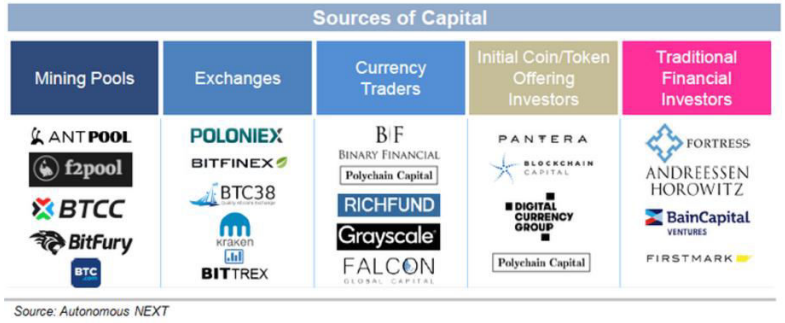
Q = Quantity of Goods and Services

Example: "Remittances market is $600B. If half is transacted in bitcoin, 75% of bitcoin are being held or lost, and the rest have velocity of v=5, then the price of 1BTC = $13,000"

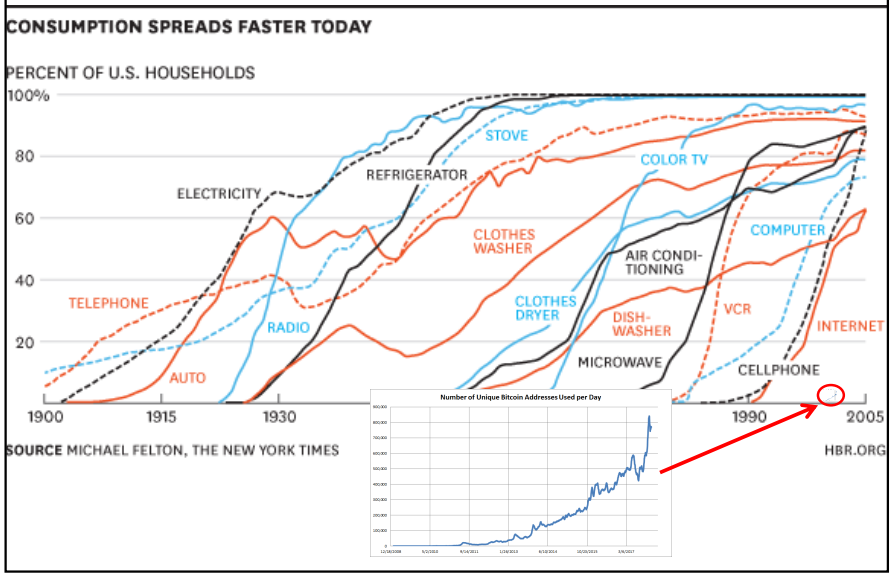
Cryptocurrency as an investment/speculation

Individuals buy crypto to transact or to invest in roughly equal amounts https://lendedu.com/blog/investing-in-bitcoin

Institutions are barely represented in the cryptoasset space

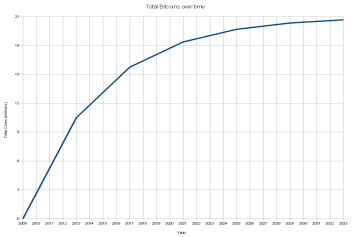


Cryptocurrency investment thesis: GROWTH



Cryptocurrency investment thesis: HEDGE

- PBoC (aggressive devaluation)
- India (demonitization)
- Venezuela (hyperinflation)
- Zimbabwe (hyperinflation)
- Capital flight (>250 million people not living in county of birth)



The hedge thesis supports the zero/anti-correlation with especially fixed income assets.

As a hedge, less time value erosion than options or futures

Bitcoin has a hard-coded inflation schedule (21 million BTC total)

Cryptocurrency in a “classical” portfolio

Portfolio with 1% bitcoin, rebalanced quarterly, January 2013-18

Metric	Basic Portfolio (70% VOO, 30% AGG)	Crypto-augmented Portfolio (69% VOO, 30% AGG, 1% BTC)
Monthly Volatility	1.95%	2.36%
Sharpe Ratio	1.72	1.77
Compound Annual Growth Rate	12.2%	15.3%

VOO: Vanguard 500 Index Fund
AGG: iShares Core U.S. Aggregate Bond ETF
BTC: bitcoin

Data from Bloomberg and CoinDesk

Worst Case Scenario . . .

Portfolio with 1% bitcoin, rebalanced quarterly, November 29th, 2013 – January 1st 2018

Metric	Basic Portfolio (70% VOO, 30% AGG)	Crypto-augmented Portfolio (69% VOO, 30% AGG, 1% BTC)
Monthly Volatility	1.92%	1.96%
Sharpe Ratio	1.47	1.50
Compound Annual Growth Rate	10.3%	11.4%

Data from Bloomberg, coinmarketcap.com and CoinDesk

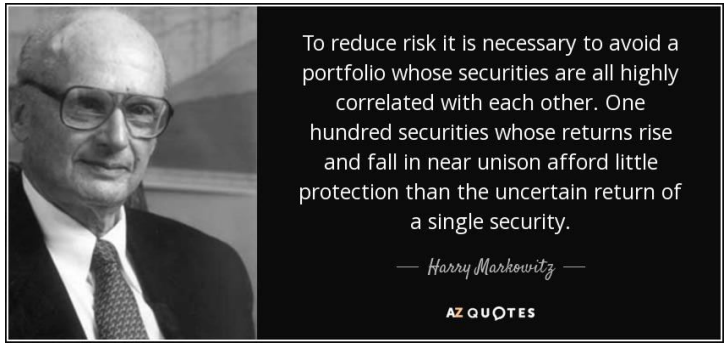
Cryptocurrency can be Markowitz’s “free lunch!”

Portfolio with 1% bitcoin, rebalanced quarterly, January 2015-17

Metric	Basic Portfolio (70% VOO, 30% AGG)	Crypto-augmented Portfolio (69% VOO, 30% AGG, 1% BTC)
Weekly Volatility	1.24%	1.22%
Sharpe Ratio	0.54	0.61
Compound Annual Growth Rate	4.7%	5.3%

Data from Bloomberg and CoinDesk

Cryptoassets have offered true diversification (thus far)

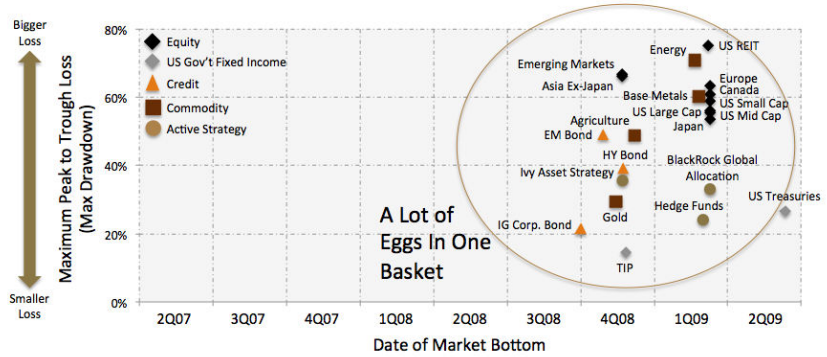


Contemporary recommendations include around 20% “alternative investments” post 2008 crash

http://www.morganstanley.com/wealth/investmentsolutions/pdfs/altscapabilitiesbrochure.pdf

http://www.aaii.com/journal/article/the-alternative-portfolio-diversifying-away-from-a-traditional-allocation

Cryptoassets have offered true diversification (thus far)

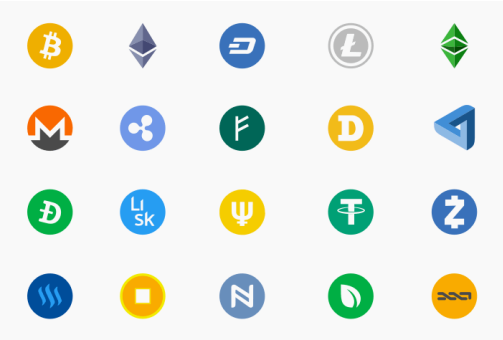


https://blog.thinknewfound.com/2013/03/visualizing-increased-correlation-during-market-crases/

Bitcoin has some features that are not ideal for all parties

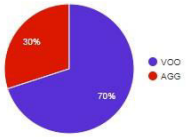
- **Proof of Work**
- **Anonymity**
- **Scalability**
- **Bitcoin script is limited**

….also, no good idea goes uncopied.



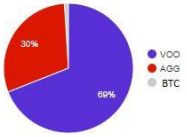
Cryptoassets have offered true diversification (thus far)

Ticker	Name	Allocation
VOO	Vanguard S&P 500 ETF	70.00%
AGG	iShares Core US Aggregate Bond ETF	30.00%



US Mkt Correlation 0.98

Ticker	Name	Allocation
VOO	Vanguard S&P 500 ETF	69.00%
AGG	iShares Core US Aggregate Bond ETF	30.00%
^BTC	Bitcoin Market Price USD	1.00%

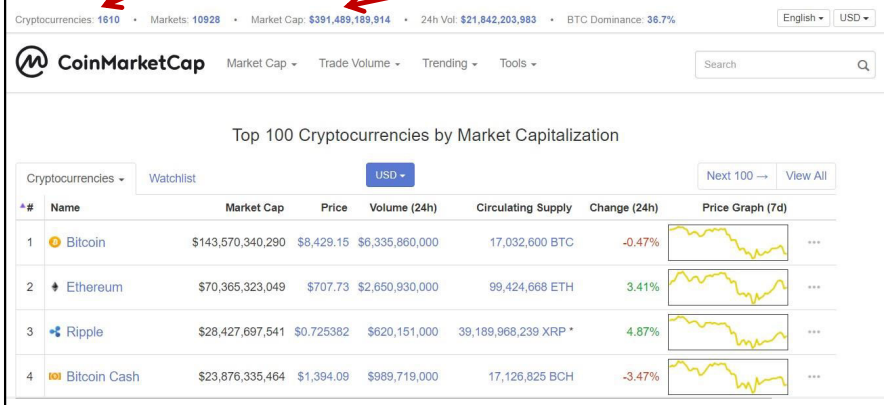


US Mkt Correlation 0.86

https://blog.thinknewfound.com/2013/03/visualizing-increased-correlation-during-market-crases/

>1,600 cryptocurrencies

~$400 billion



The Cryptoasset Ecosystem

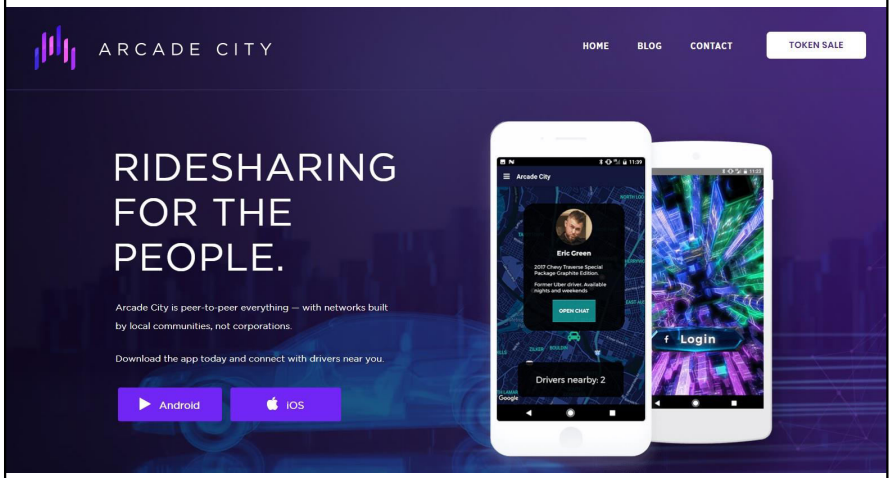
Cryptoassets: Blockchain-based protocols with exchangeable tokens

Which trusted third party is being dis-intermediated?
(is there value for it to capture?)

What information is being written to the blockchain?
(does it need its own ledger?)

Cryptoassets: Blockchain-based protocols with exchangeable tokens

https://arcade.city/

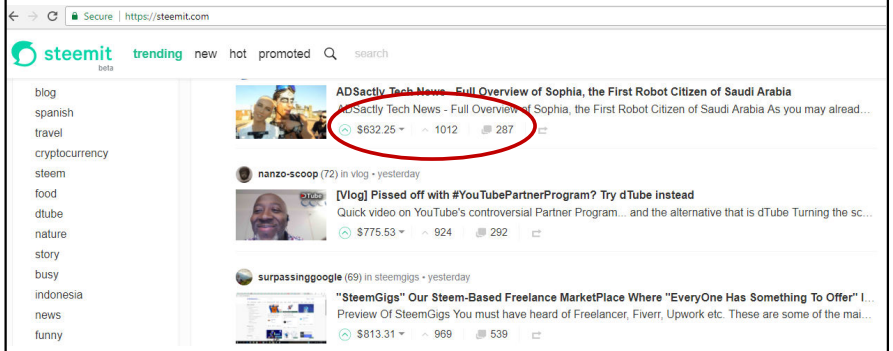


† These are included as examples not endorsements

steemit

Content creation on media platforms, transparent curation and advertising

https://steem.io/



https://steemit.com/

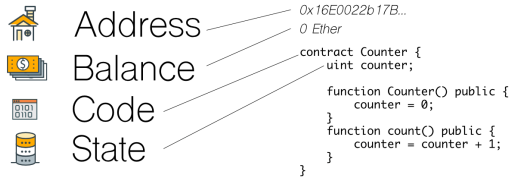
ethereum

https://www.ethereum.org/

nodes execute code to execute conditional transactions

Smart Contract

Ethereum Account Type (Just like User Account)

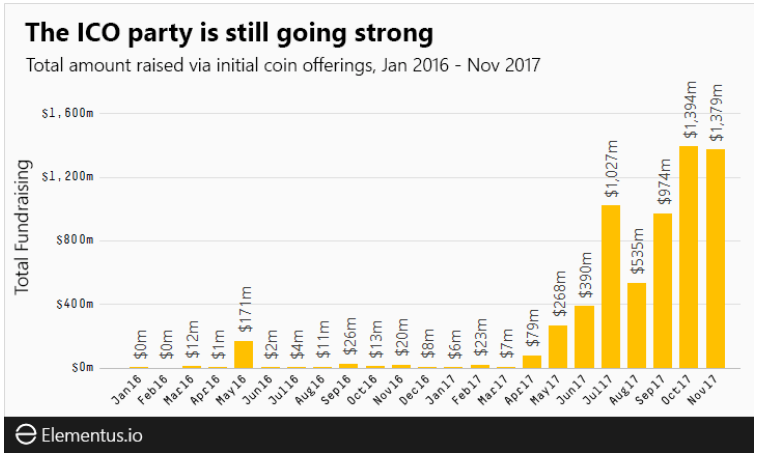


http://www.gjermundbjaanes.com/understanding-ethereum-smart-contracts/

† These are included as examples not endorsements

Ethereum's killer app of 2017, the "Initial Coin Offering" (ICO)

IPO as an smart contract on the Ethereum blockchain



https://thenextweb.com/hardfork/2017/12/15/cryptocurrency-token-sale-visualization/

Ethereum's killer app of 2017, the ICO

In general, many more scams and vaporware companies than substantive projects right now.

Most ICOs are "illegal securities" under SEC v. Howey (1946)

(1) An investment of money (2) in a common enterprise, with the (3) expectation of profits (4) based on the work of others.

https://www.sec.gov/ICO
https://www.coinbase.com/legal/securities-law-framework.pdf

Blockchains provide "digital scarcity" more than just Money over IP

(Bitcoin : Blockchain :: Email : Internet)

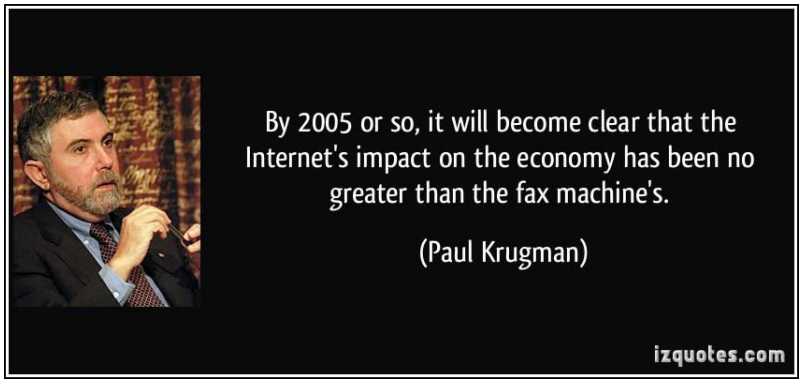
- Escrow services (1-2% vs. $50 flat?!)
- Notary services (document timestamping)
- Publicly auditable voting systems
- "Smart contracts"
  - Titles and deeds
  - Probate
  - Trusts

Smart contracts recognized state law in AZ
Bill to do the same proposed in FL
Blockchain data sufficient to authenticate data in VT

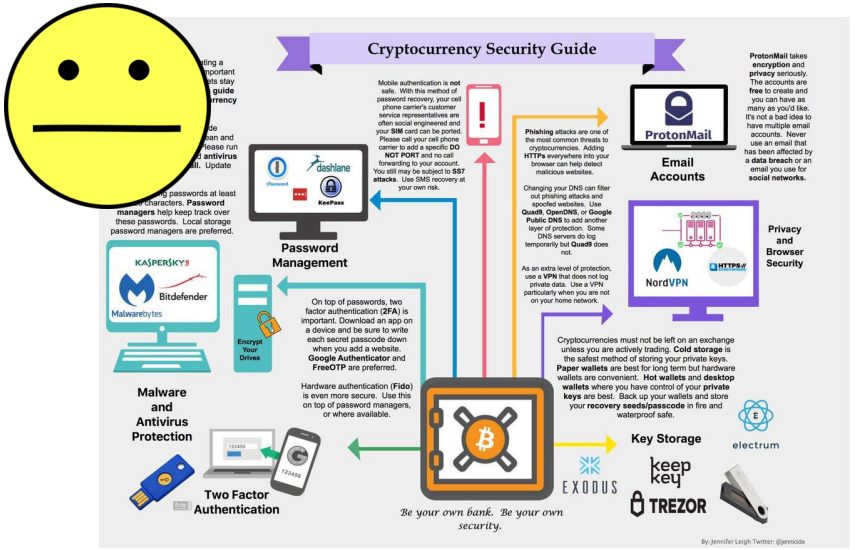
https://legiscan.com/FL/text/H1357/id/1676376

Conclusions

- Invest some time in researching cryptoassets
- Make your own conclusions



Last caveat! Lots to learn: Allocation, Buying, Custody



Thank you!

Doug Faust: faust@soundcrypto.com
General questions: info@soundcrypto.com