

SCET Blockchain Lab

Introduction to Blockchain tech & Use Cases

Alexander Fred-Ojala

Research Director, Data Lab
SCET, UC Berkeley
afo@berkeley.edu

Ikhlaq Sidhu

Founding Director, SCET
Professor, IEOR, UC Berkeley
sidhu@berkeley.edu



Pantaz and Ting

Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering

2018

Alexander Fred-Ojala

- Research Director
Data Lab, SCET, UC Berkeley
- Co-creator of Data-X
UC Berkeley class: Applied Data Science w Venture Applications
- Co-founder
UC Berkeley / SCET's Blockchain lab
- Founding Team of 3 companies
InnoQuant (COO), Auranest (CMO),
Wheely's (YCombinator alumni)
- Degree in Mathematical Statistics
UC Berkeley & Lund University, Sweden



Co-founder Blockchain Lab

OUTLINE

1. Quick Blockchain Overview

History and statistics

2. Bitcoin

The First Blockchain application

3. Ethereum & Smart Contracts

Decentralized Apps, Web3.0

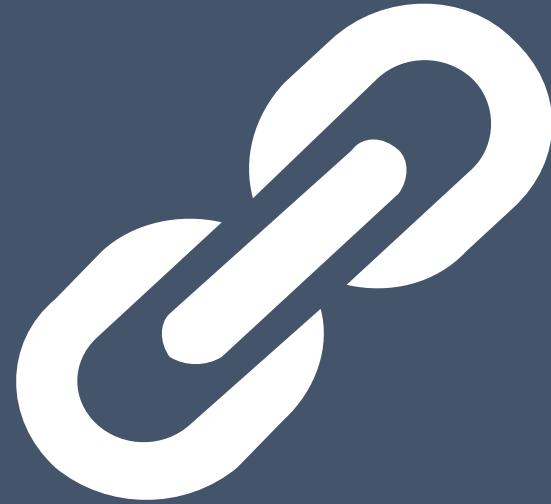
4. Blockchain Applications

Fintech, Healthcare, Government, Energy





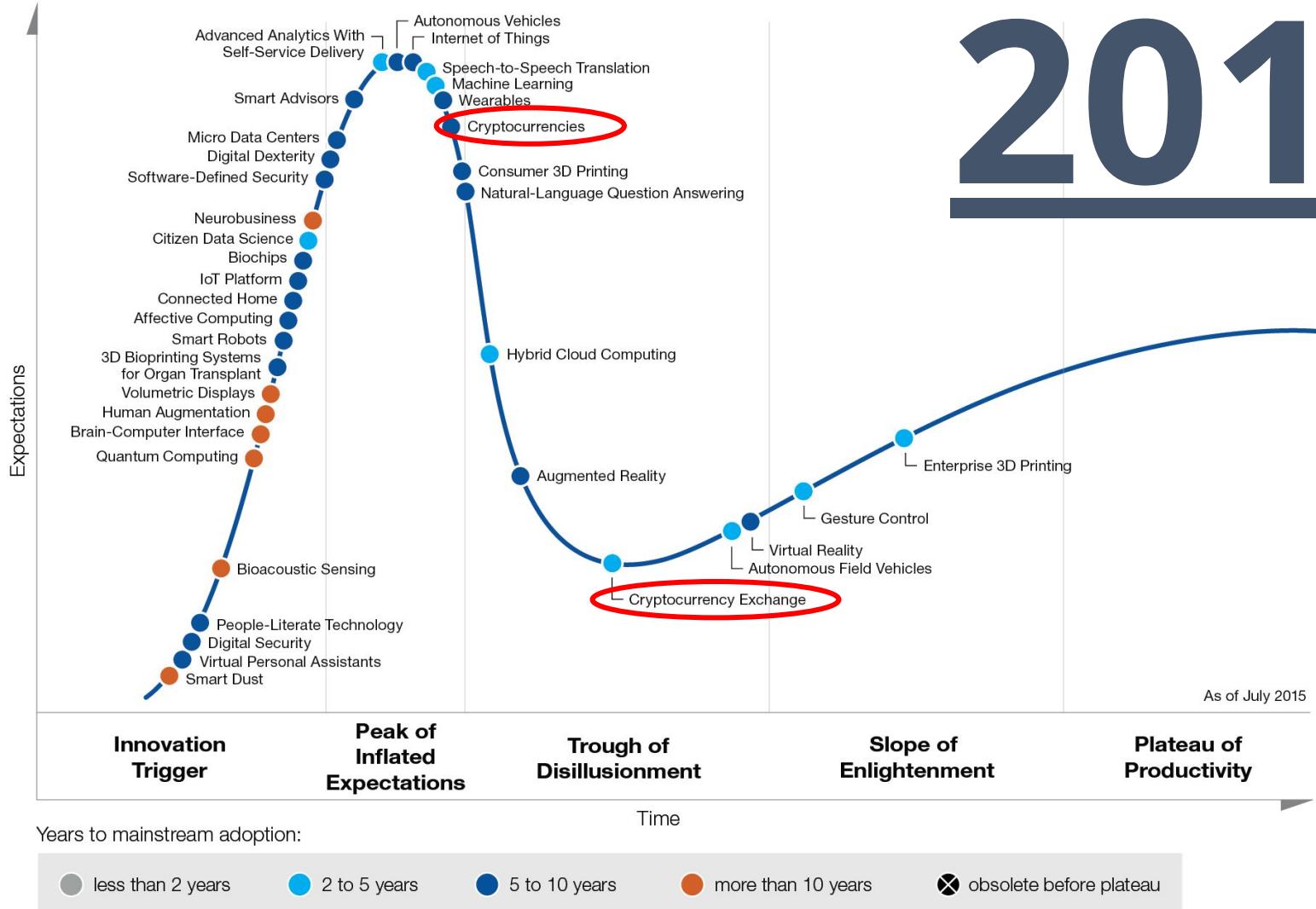
**First:
QUESTIONS TIME!**



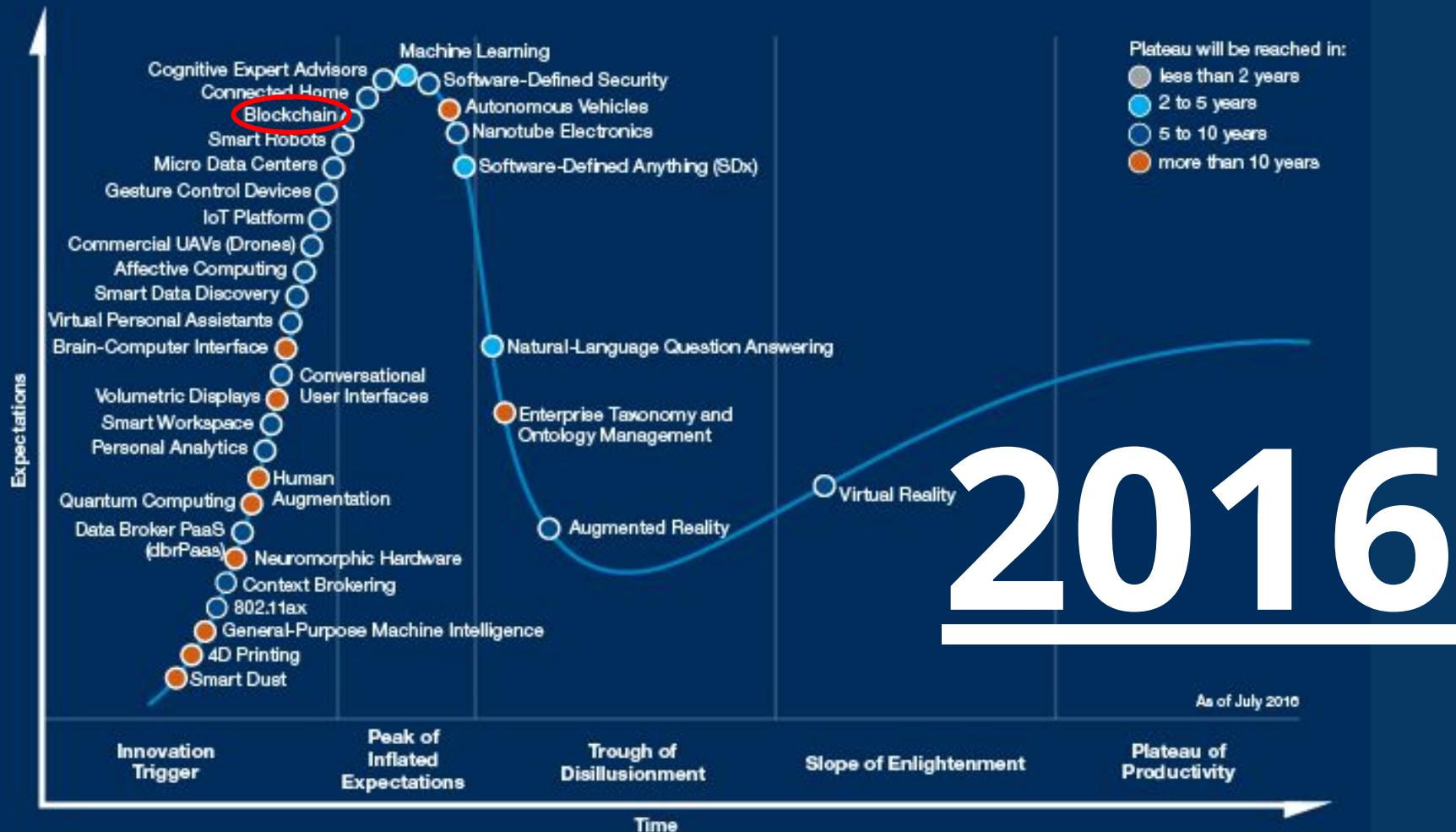
Blockchain Hype & History

Emerging Technology Hype Cycle

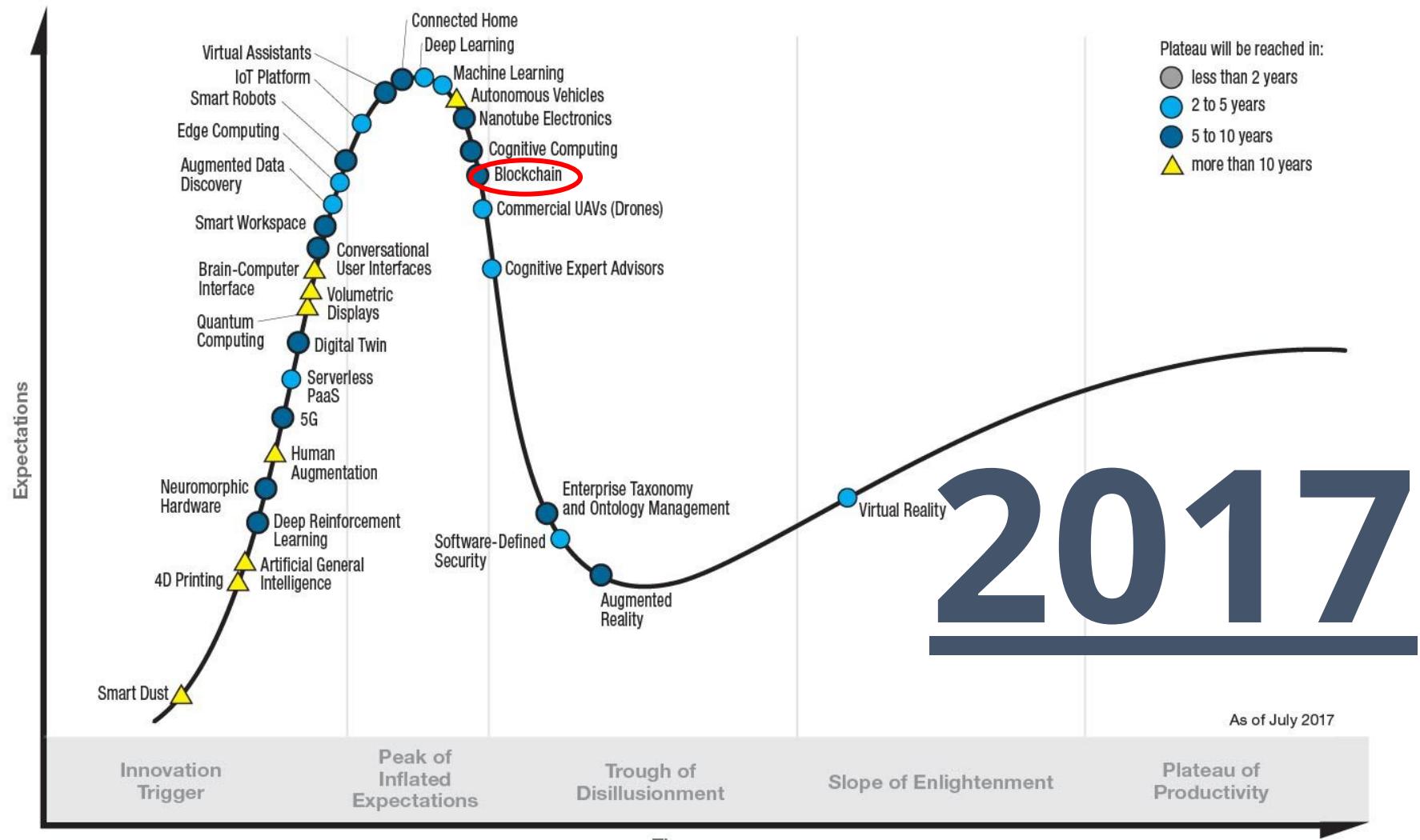
2015

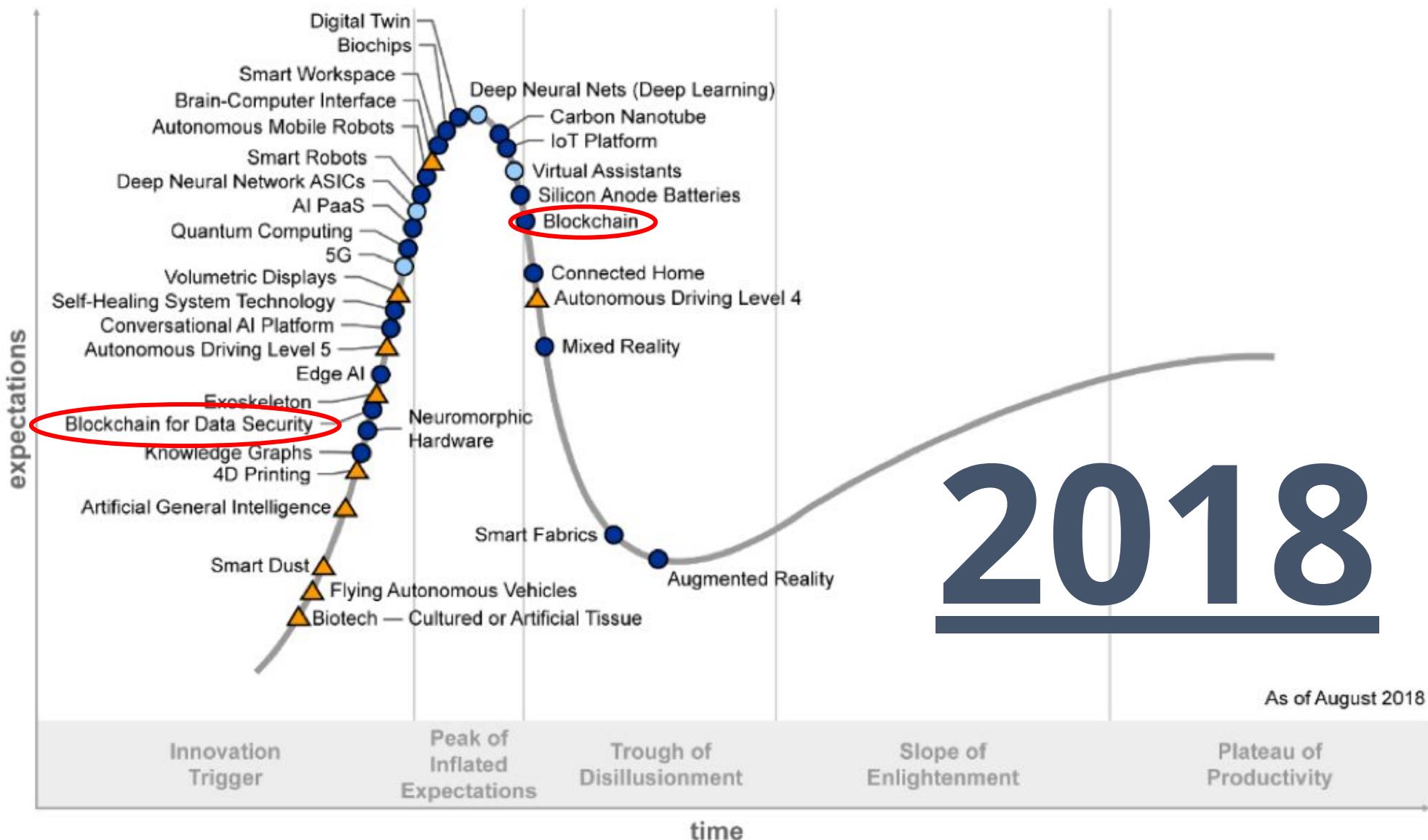


Gartner Hype Cycle for Emerging Technologies, 2016



Gartner Hype Cycle for Emerging Technologies, 2017

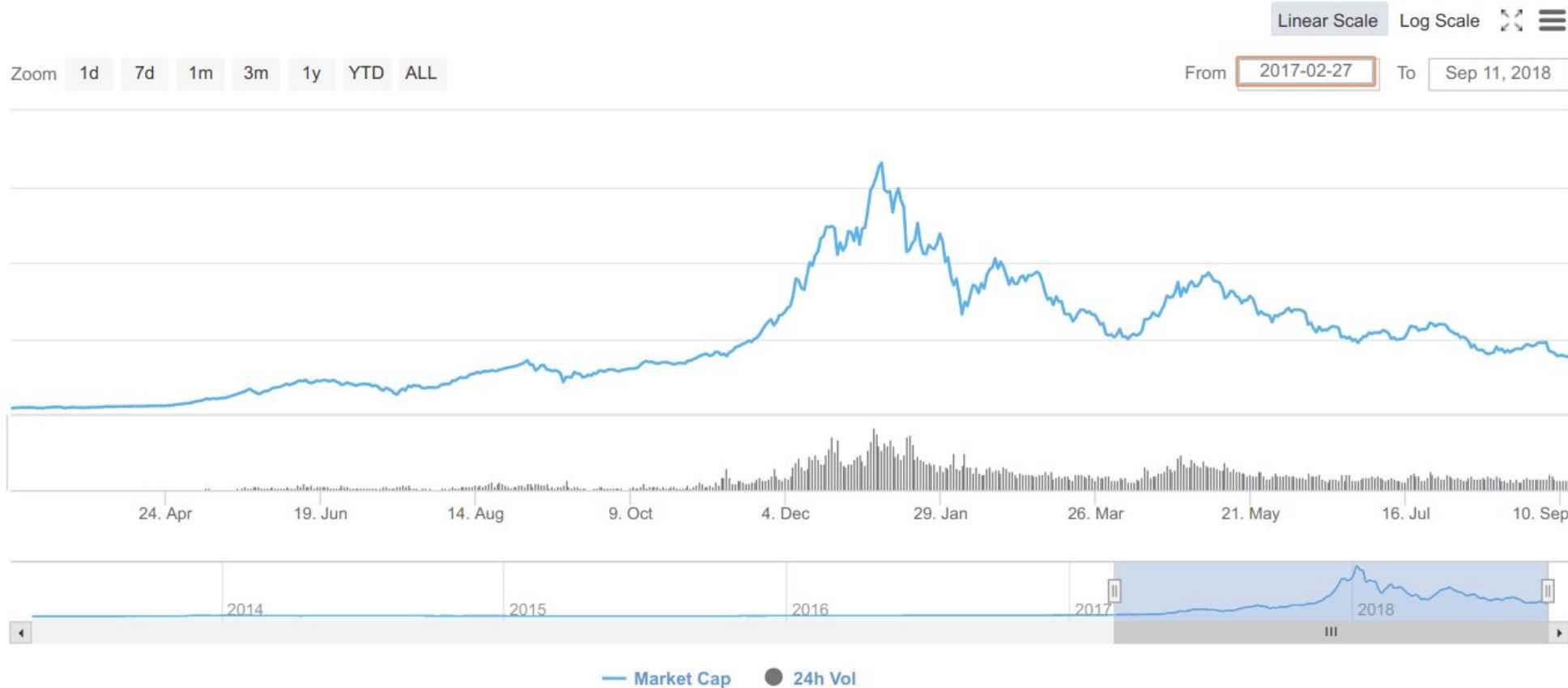


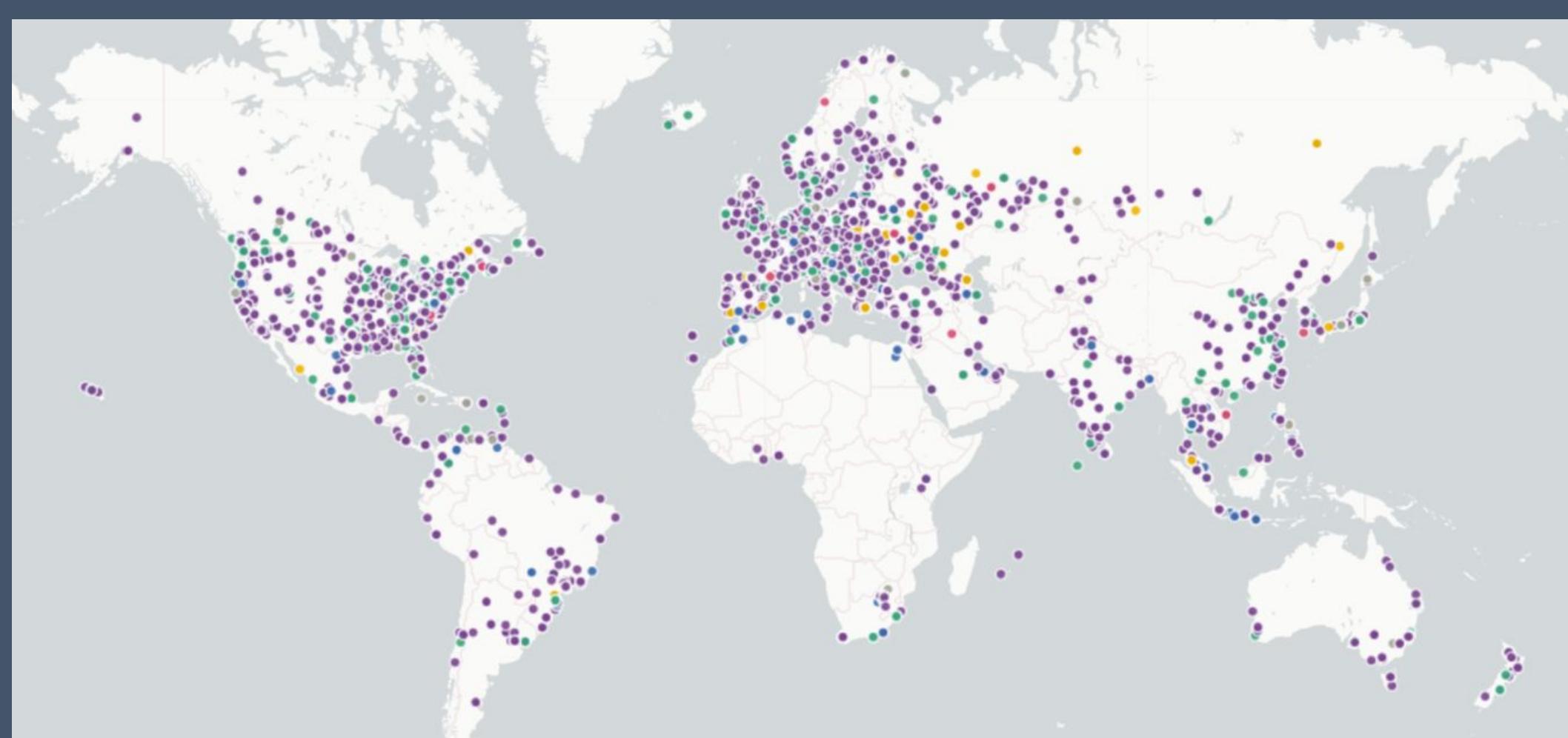


Market Cap for all cryptocurrencies

Peak: \$820Bn (today \$190Bn)

Total Market Capitalization



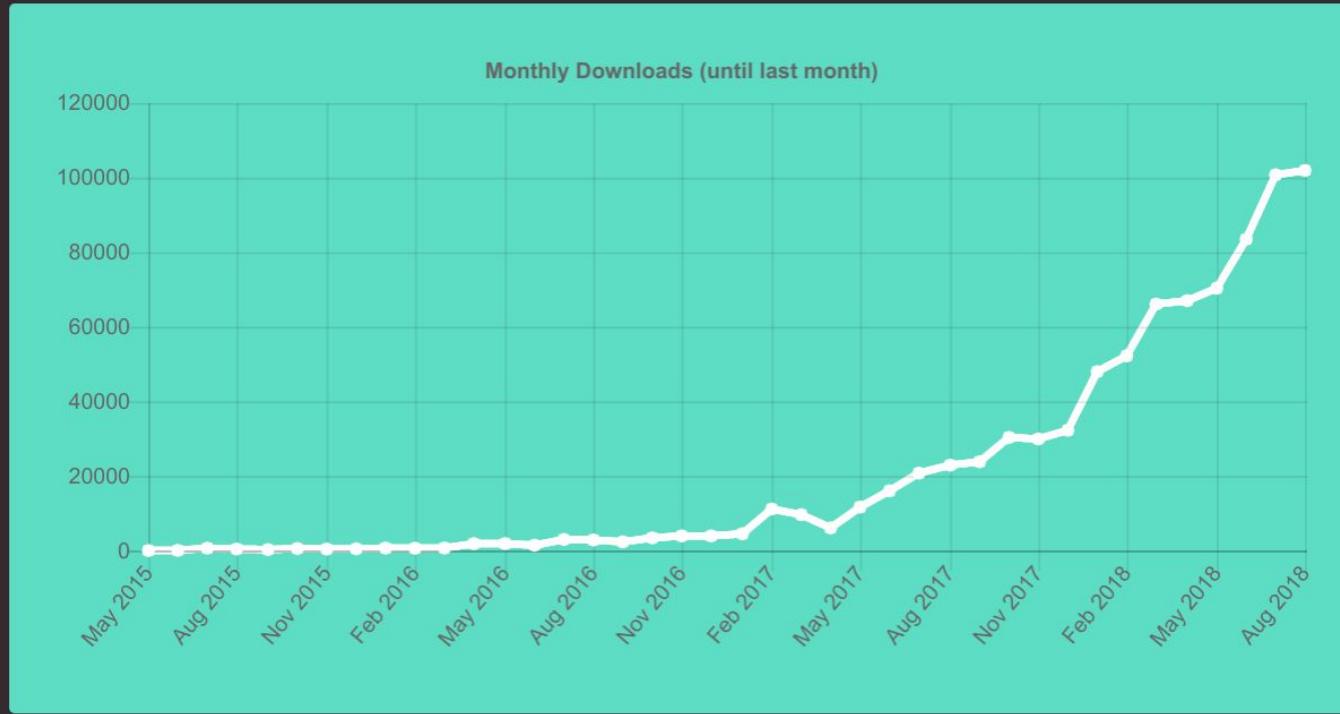


World map of Ethereum nodes according to
https://team.carto.com/viz/e70677d5-1111-40a8-9e19-f27da227a55c/public_map

Downloads

Over the lifetime of each product in the Truffle Suite, from inception to now.

TRUFFLE



Downloads of Blockchain Development Kit

Lifetime Downloads

869,911

Last Three Months

UP 40%

* excludes current month

<https://truffleframework.com/dashboard> &

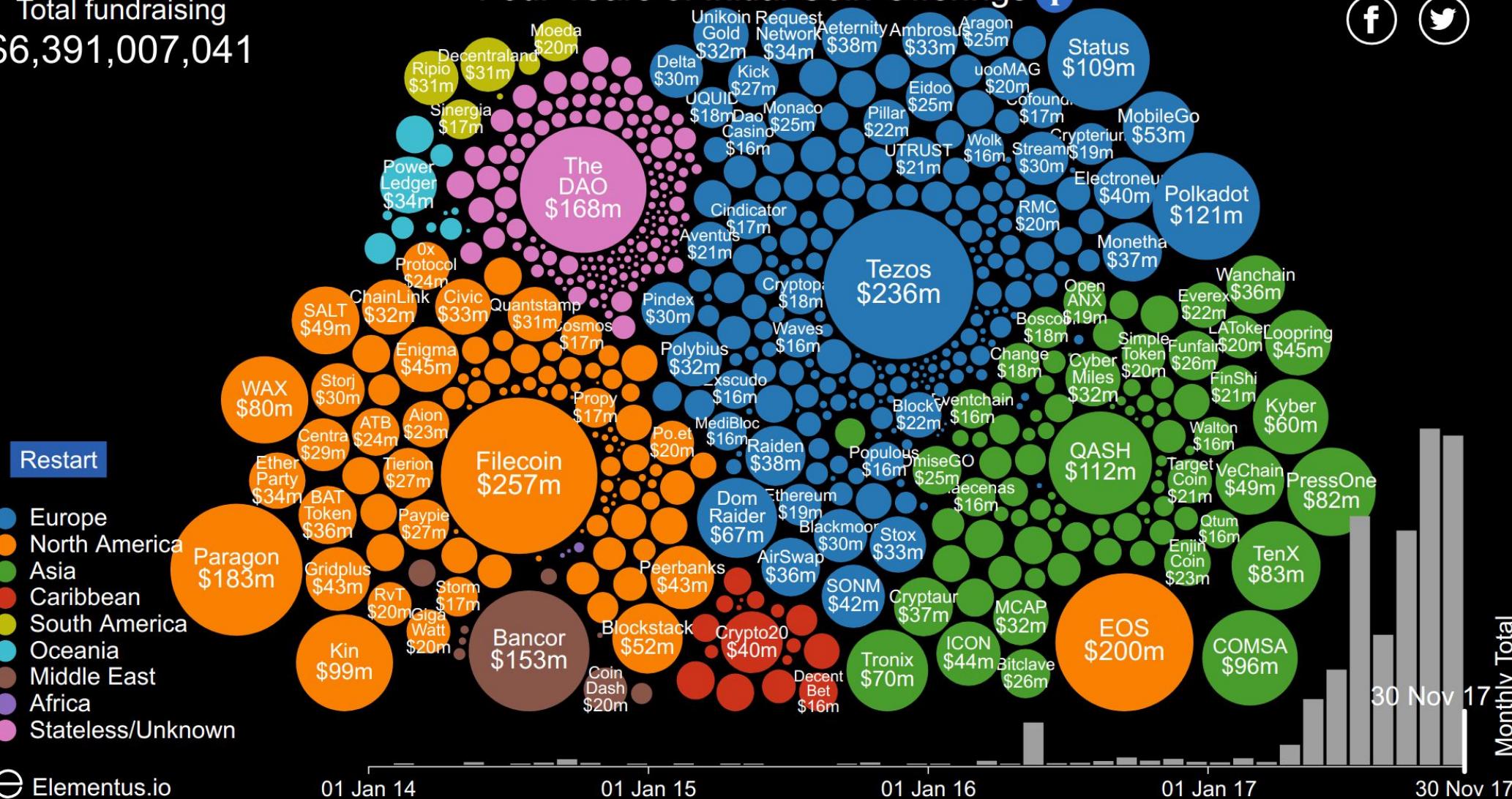
<https://medium.com/loom-network/ethereum-will-be-the-backbone-of-the-new-internet-88718e08124f>

Four Years of Initial Coin Offerings

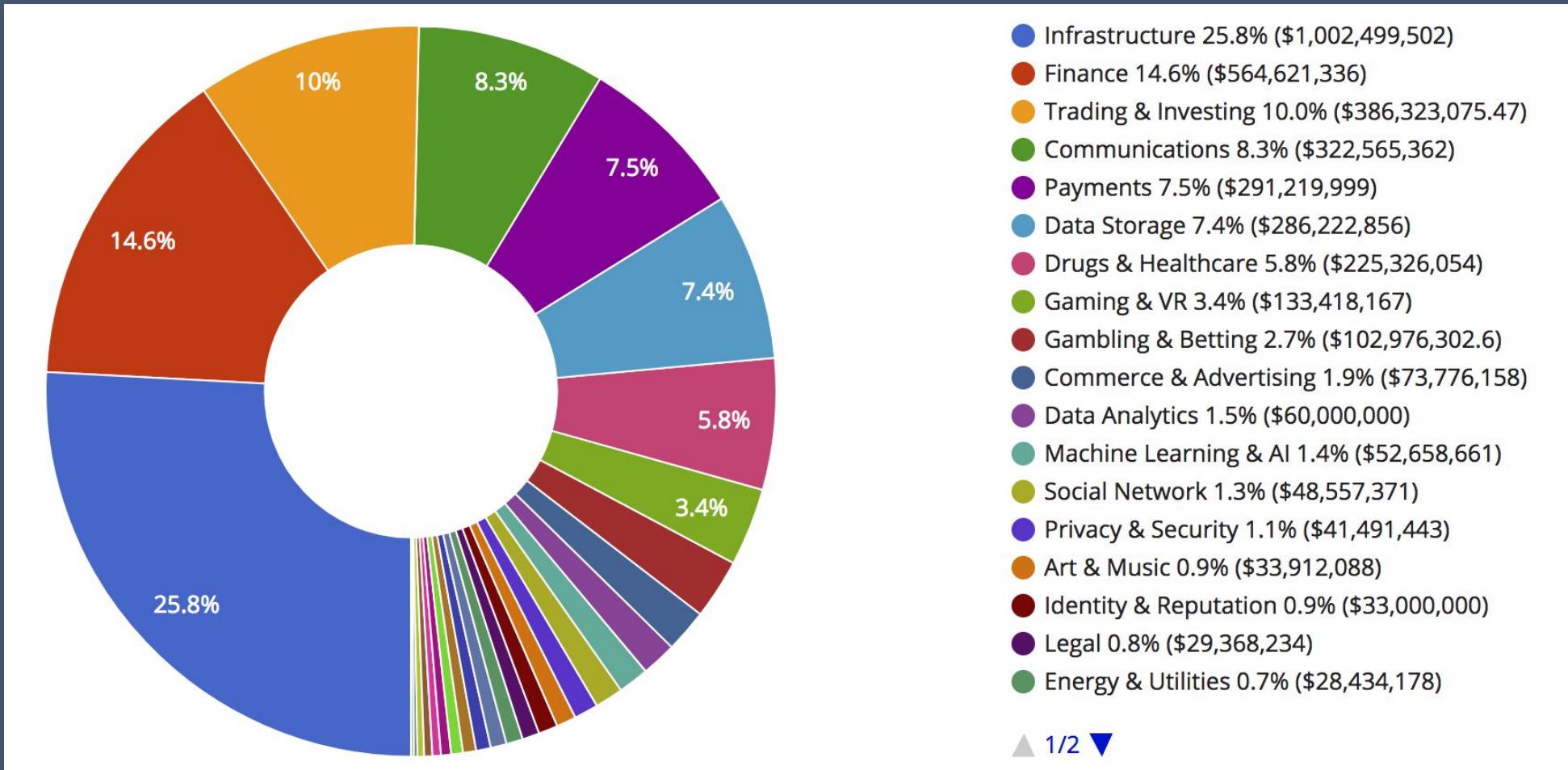


Total fundraising

\$6,391,007,041



Industry agnostic - ICOs by category in 2017



Blockchain Hard numbers

1. Global **Market Cap**:
Blockchain tokens

\$820Bn (Jan 2018)
0.9% of World GDP

2. # of **Blockchain users**
~ 30 million users.



3. Ratio of **Female Bitcoin Owners**
Only 5-7%

4. Blockchain **Disk Space**
Bitcoin: **184Gb**
Ethereum: > **1Tb**

5. **Price** Oct 30th 2018
\$6300 / BTC
\$200 / ETH

Approx numbers from Sep 2018

1. <https://coinmarketcap.com/charts/>

2. https://www.reddit.com/r/Ripple/comments/80hd4j/ripple_xrp_price_and_the_total_number_of_t/

3. <https://www.forbes.com/sites/lamjackie/2017/12/10/where-are-the-women-in-the-blockchain-network/>

4. <https://blockchain.info/charts/blocks-size> (Bitcoin) <https://etherscan.io/chart2/chaindatasizefast> (Ethereum)

5. <https://coinmarketcap.com/>

How Do Blockchains work

A Bitcoin case study



2008: Enter Bitcoin

First Blockchain Application
Digital money!



10k BTC for a Pizza, 2010

First real-world transaction: \$25, 2 pizzas in Jacksonville, Florida for 10,000 BTC. $\frac{1}{4}$ cent.

Bitcoin enters the mainstream, '16-'18

ICOs, blockchain technology, and the price of bitcoin are ever present in the news. The hype takes the price to ~\$20k / BTC. Market correction in 2018.

Bitcoin Whitepaper, 2008

Satoshi Nakamoto releases Bitcoin in the wake of the financial crisis. Owns 1Mn BTC.

Largest bitcoin crash, 2013

The bitcoin price fell 75% over the course of 24hrs in April 2013.

Mt Gox hack, 2014

6% of all bitcoin ever created stolen from the largest exchange. \$500Mn.

FUTURE

Bitcoin (USD) Price

Closing Price OHLC

1h 12h 1d 1w 1m 3m 1y All

Jul 18, 2010 to Sep 5, 2018 [Export](#)

Week from Monday, Dec 18, 2017 UTC
CoinDesk BPI: \$15 852.28

\$15000
\$10000
\$5000
\$0



: coindesk

CoinDesk BPI in effect

2012 2014 2016 2018

What is Bitcoin?

Digital, Decentralized & Trustless Currency

First widely adopted digital currency. Regulated by a community that anyone can join.



Public ledger with transactions

Full transaction history is public, anyone can audit.

Financial Inclusion: Pseudonymous identities

Anyone can join w/o revealing identity. Transactions are public but identities are not linked to accounts / keys.

Transfer Money Globally P2P

No need for trusted 3rd party or intermediary to validate transaction.

bitcoin / Bitcoin?!

- ***bitcoin*** is the currency
(BTC = digital money)
- ***Bitcoin*** is the technology / protocol
(almost like the infrastructure for a bank)

Bitcoin: User Perspective

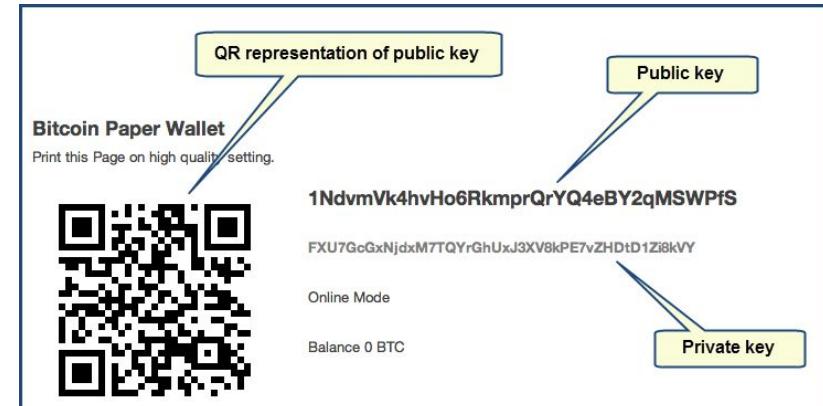
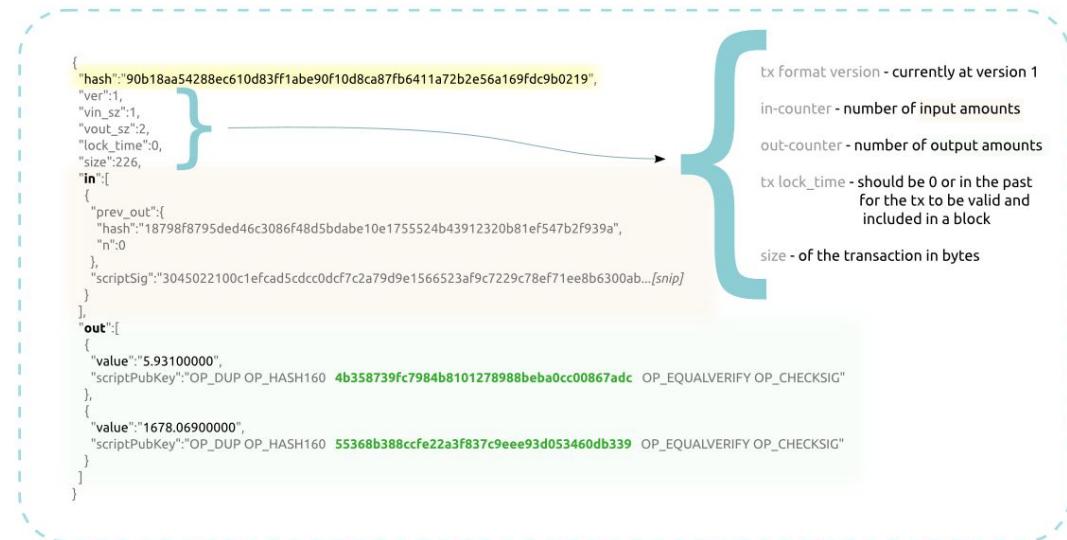
1. First system to enable **simple transactions** with a digital currency.
2. User's use a wallet with Public and Private keys to send and receive bitcoin.

Private key signs transactions

Public key verifies signature

Bitcoin Transaction Example

`txid 90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219`



Private / Public Keys



◇ Private Key:

Secret. Like a password. Keep it safe. No recovery option.

- Generated from random processes
- Used to sign transactions and prove ownership.

5K8BwE76VsatQiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn

◇ Public Key:

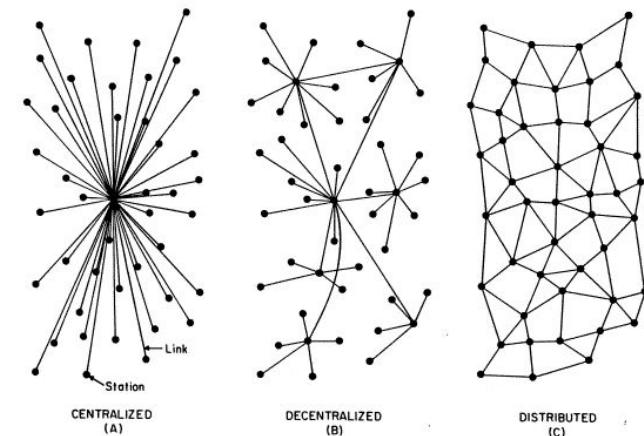
External. Like a username. Generated deterministically from Private key.

- Private key will always generate same public key (ECDSA: Elliptic Curve Digital Signature Algorithm)
- Public address for receiving bitcoin.

1M3RLrXve5wcT2ZcJu8WXoXjh4WXcWQA9

Bitcoin: Network Perspective

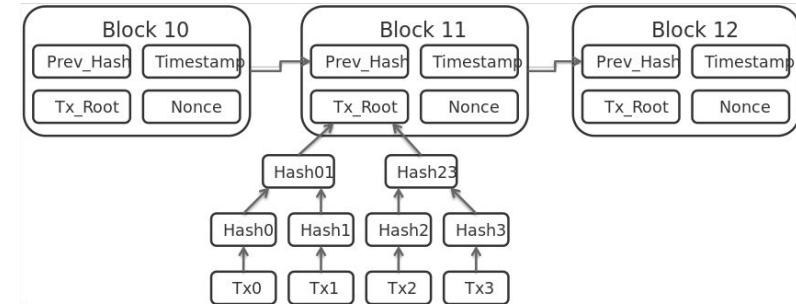
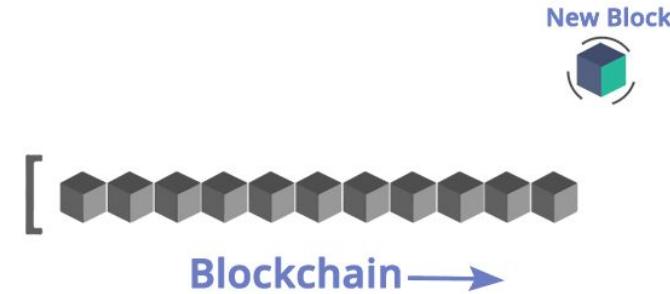
- Users broadcast transactions to **decentralized P2P network of computer nodes** that validates payments and keeps track of transactions.
- Anyone can setup a node and join the Bitcoin network. Nodes exist globally. **No central point of failure**, gets around the honey pot problem.
- Nodes validating transactions are called **miners**. They group transactions into blocks, and link blocks in an immutable chain. This data structure is called a **Blockchain**.



The Bitcoin Blockchain

Shared Database: Tracks every transaction since the Genesis block

- ◊ **Ledger:** Like an append only spreadsheet.
- ◊ **Immutable: Cryptographically Secured** by including the hash of the previous block in the current block.
- ◊ **Transactions are grouped together in blocks.** A new block is added every 10 minutes.
- ◊ **Consensus protocol:** Majority decide valid chain. Tie voting power to resource. Proof of work.



Source: <https://www.edureka.co/blog/blockchain-technology/>

Bitcoin: Incentivizing Participation

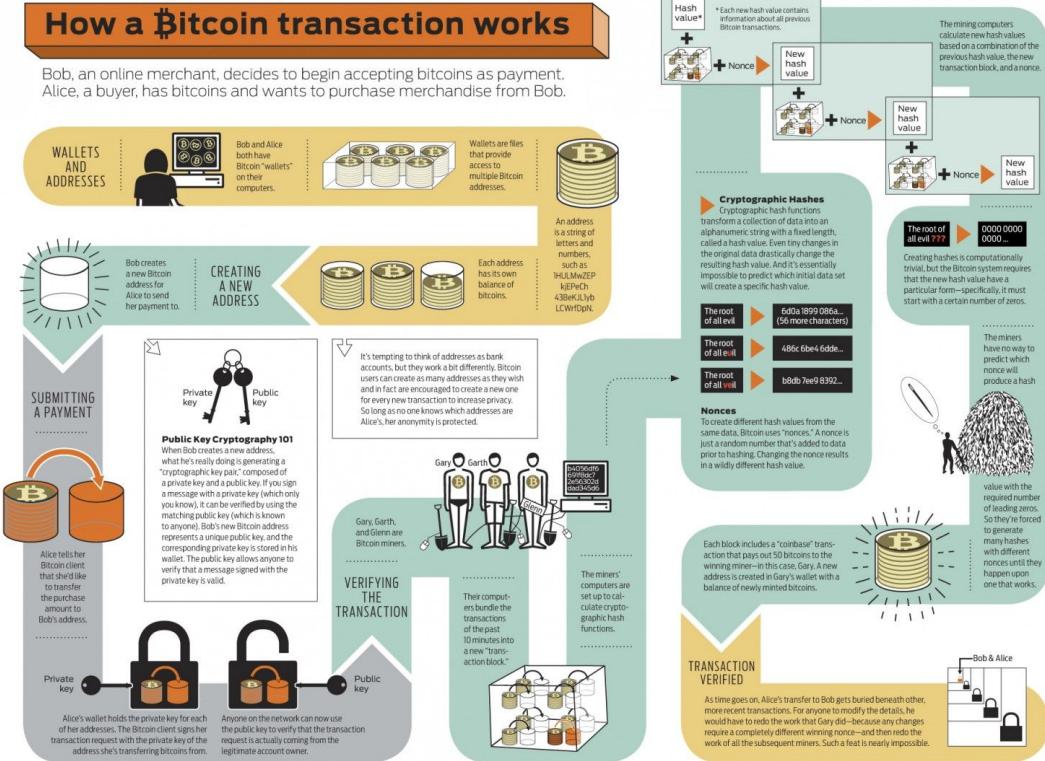
Why do peers wanna join and set up mining rigs?

1. **Monetary incentive:** Every time a node validates a block of transactions they get a reward. Plus transaction fees.
2. Convenient way to **create and distribute new money.**



Source: <https://www.cnbc.com/2018/01/12/what-it-looks-like-inside-an-actual-bitcoin-mining-operation.html>

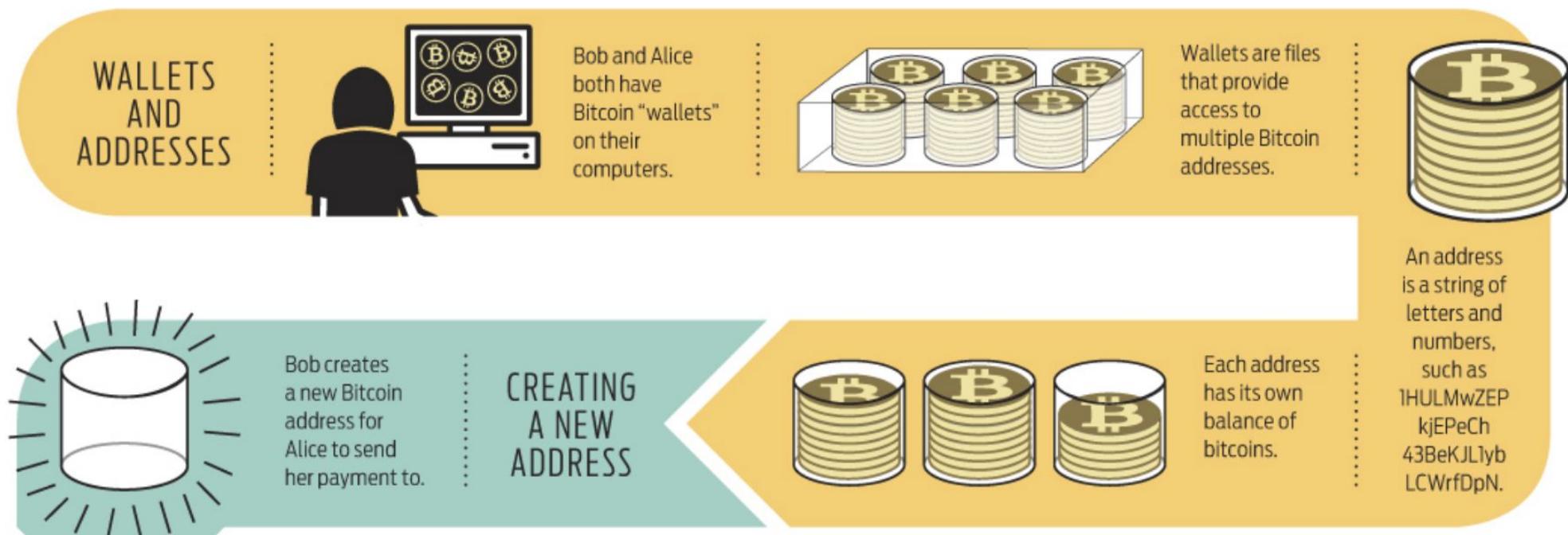
Bitcoin: System Overview



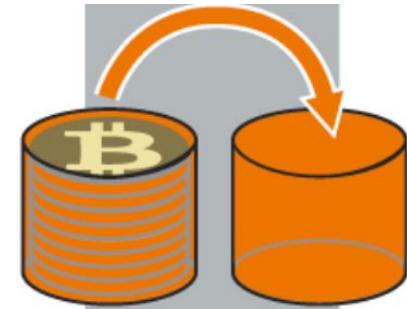
Source: IEEE Spectrum

Bitcoin: System Overview (1/4)

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.



Bitcoin: System Overview (2/4)



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Submitting Payment



Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

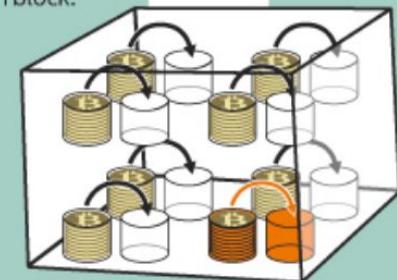
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.



b4056df6
691f8dc7
2e56302d
dad345d6

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.

Bitcoin: System Overview (3/4)

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root
of all evil

6d0a1899086a...
(56 more characters)

The root
of all evil

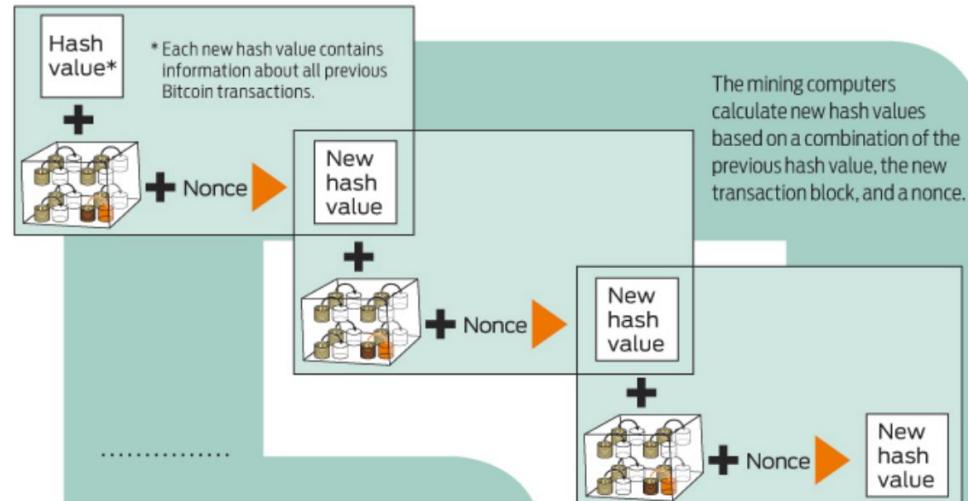
486c6be46dde...

The root
of all veil

b8db7ee98392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.



The root of
all evil ???



0000 0000
0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners
have no way to
predict which
nonce will
produce a hash



value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Source: IEEE Spectrum

Bitcoin: System Overview (4/4)

Each block includes a “coinbase” transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary’s wallet with a balance of newly minted bitcoins.

TRANSACTION
VERIFIED

As time goes on, Alice’s transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

Bob & Alice



User owned and managed

Digital, Network Money!

(Wow, we pay thousand of dollars to claim hashes on a ledger!)



Around 2013: *How to improve Bitcoin?*

Smart Contracts

◆ “Standard” Contract definition:

- Agreement with another party.
- Some entity (courts, banks, escrow agents) enforces the agreement and the terms so that they are not violated.

◆ Smart Contract (Nick Szabo, 1996):

- Define terms of agreement in programmatic code.
- Code that facilitates, verifies, and enforces execution of the digital contract.
- Code becomes law!



Satoshi Nakamoto



Vitalik Buterin



VS.



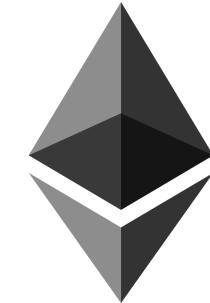
ethereum

HOMESTEAD RELEASE

BLOCKCHAIN APP PLATFORM

Enter Ethereum

- **Blockchain Smart Contract Platform:**
 - Total network has a state
 - Transactions and smart contract executions change state.
- **Distributed World Computer (EVM)**
 - Turing Complete (allowing loops)
- **Native Asset: Ether (ETH)**



ethereum

Blockchain Terminology

Ethereum Smart Contracts

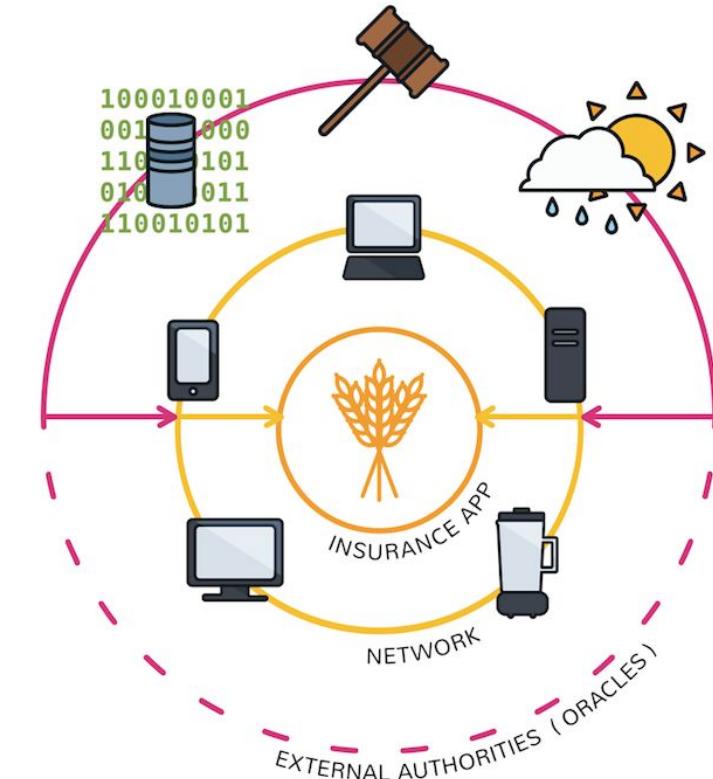
Computer protocol to digitally verify and enforce a contract without 3rd parties.

- ◇ Stored as code on the Blockchain. Evaluated by all nodes.
- ◇ Transparent, distributed, decentralized, deterministic agreement.



Decentralized Application (dApps)

- **dApps:** “Normal” applications that use smart contracts (smart contracts can also call other smart contracts)
- Sometimes has a **token that is native** to the application.
- Can be based on their own Blockchain or existing one.



Initial Coin Offering

ICO

- ◇ Introduction of a new Altcoin / Cryptocurrency / Token
- ◇ **Incentivizes a community to buy into the idea**
-> Scale factors and network effects.

Over 4000 cryptocurrencies exist, most use ERC20 standard*.



List of inactive coins: deadcoins.com

* coinranking.com (April 2018)

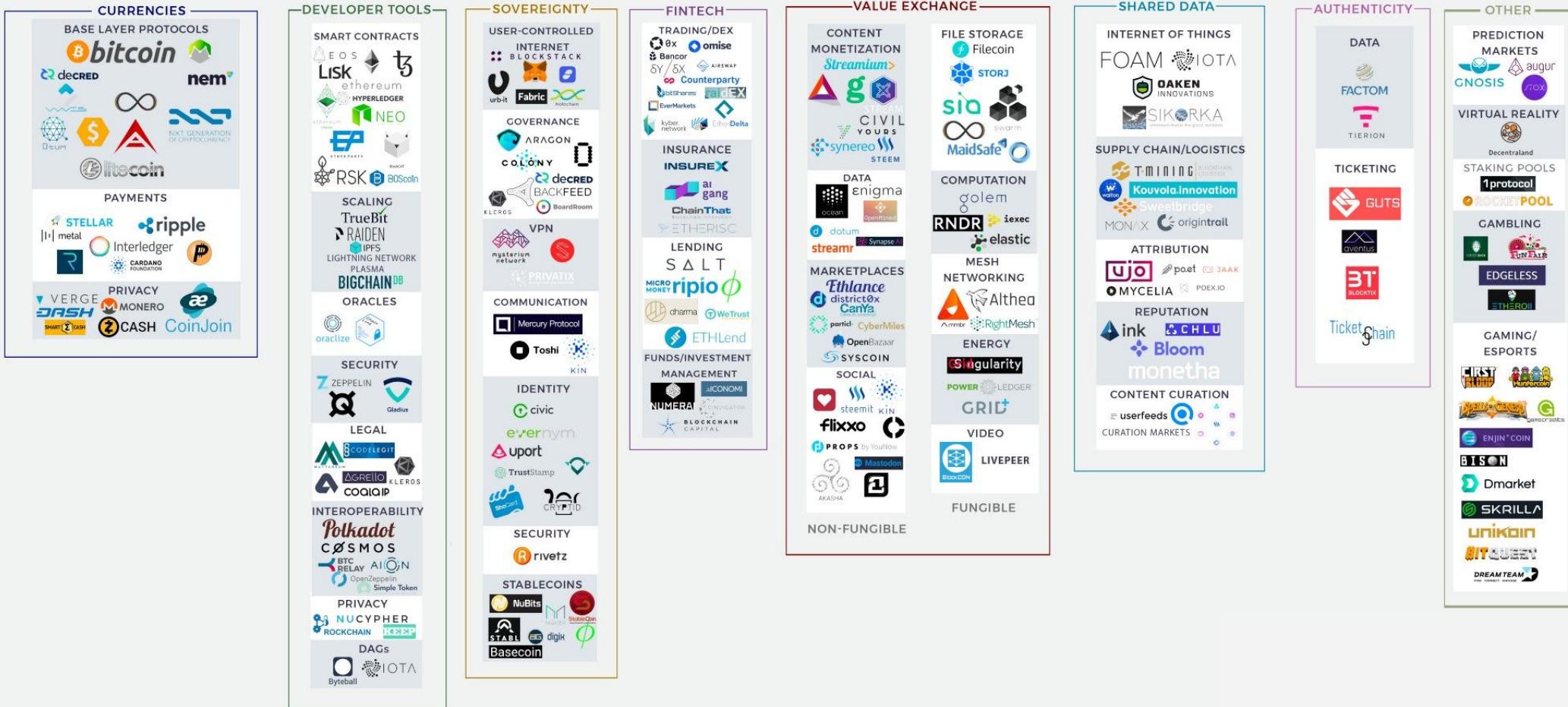
Ethereum: Powering Web 3.0

Web 3.0

- Distributed file storage
- 24 hour stock markets
- Decentralized exchanges
- Unique and scarce items (CryptoKitties)
- Digitize assets
- Store sensitive data and records
- Smart grid solutions for energy
- Supply chain management
- Medical records
- Track provenance of goods
- Remittances
- Prediction markets
- Open source incentives (Gitcoin)
- Federated Learning / Homomorphic enc.
- Content creation automatic compensation
- Get paid to reply to emails (Earn.com)
- Self sovereign identities



Overview: Exciting & Promising Blockchain Projects



Source: Josh Nussbaum, https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27

Blockchain

Examples of Industry Use Cases

FinTech

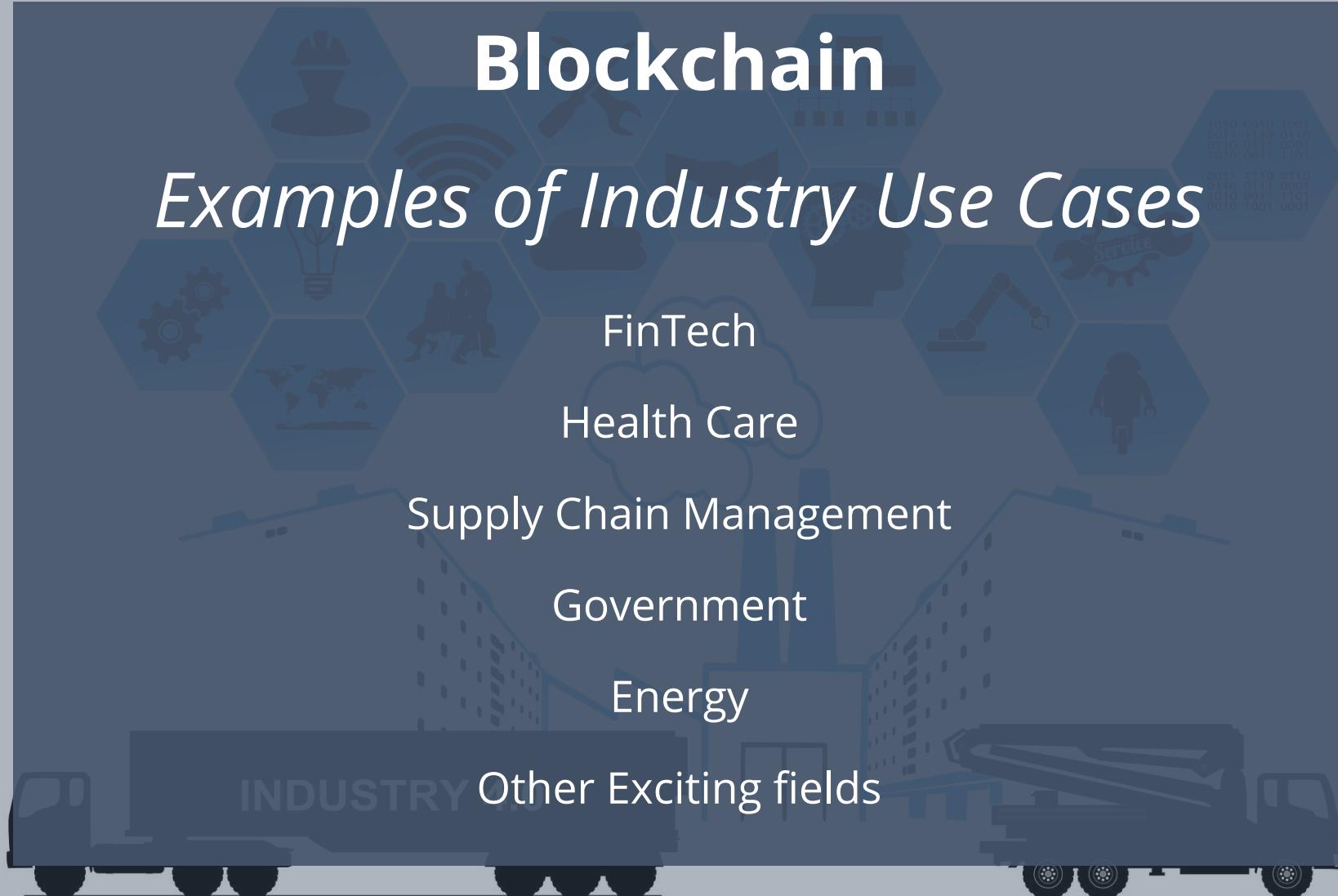
Health Care

Supply Chain Management

Government

Energy

INDUSTRY Other Exciting fields



Blockchain Use Cases: Fintech

P2P Global Payments, P2P Loans and Financial Inclusion

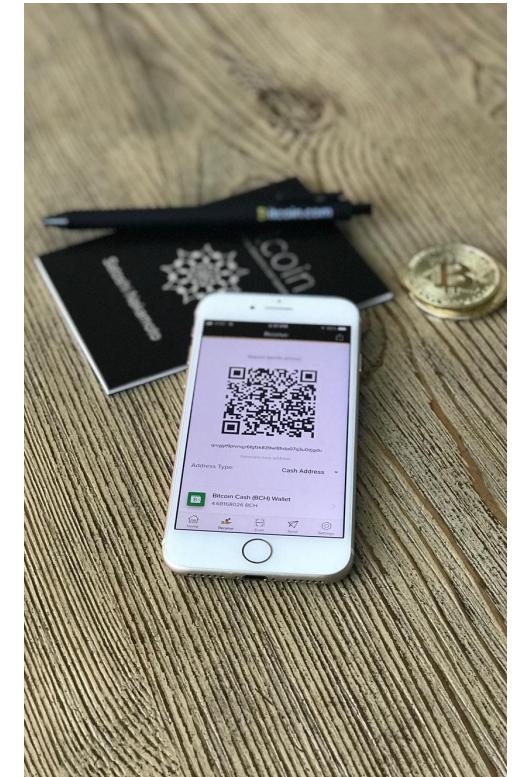
- ◊ **Bank the 2Bn unbanked** and 4Bn under-banked
- ◊ **Improve remittances and prevent corruption for humanitarian aid**
- ◊ **Automatic P2P exchange** of assets, stocks, bonds or securities. 24hr stock exchanges.
- ◊ **P2P Loans**



Blockchain Use Cases: Fintech pt. 2

Financial instruments and services

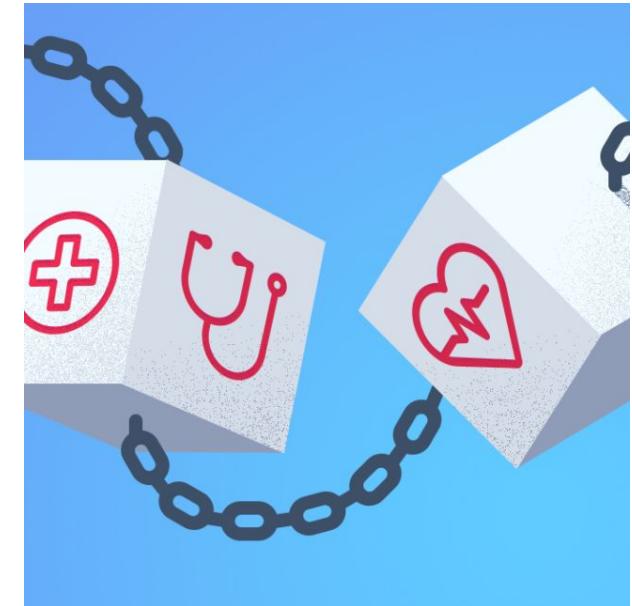
- ◇ **STO = Security Token Offering** (tokenize assets)
- ◇ Improved and simplified **KYC process**
- ◇ **Private Blockchain Consortiums** (R3, Corda, Quorum) to reduce settlement times and paper trails
- ◇ **Corporate cross border payments** with instant settlements.



Blockchain Use Cases: Health Care

Safe and Shared Health Records

- ◊ **Store and share medical history and health records.** Pilot in Estonia running today!
- ◊ **Aggregate sensitive medical data** in secure repositories. Empower researchers to extract insights.
- ◊ **Patient owned and controlled data**



Blockchain Use Cases: Supply Chain

Track Goods w/ IOT, Limit Paperwork, Improved Security

- ◆ **Track goods, from origin to destination.** Limit documentation. Simplify ownership transfer and automatic payments.
- ◆ **Food safety:** Let growers, consumers etc. gain permissioned access to food information. Trace back source of bad food in the supply chain.
- ◆ **Track Pharmaceuticals:** Preserve drug integrity from production facility to consumer. Track serial numbers, limit spread of fake drugs.



Blockchain Use Cases: Government

Open Government, Power to the People, Less Corruption

- ◇ **Individually Controlled Identities:** Estonia has launched Blockchain based citizenship.
- ◇ **Blockchain-based voting.** Sierra Leone, blockchain based election. Diminish the likelihood of electoral fraud.
- ◇ **Land records and titles:** Ukraine
- ◇ **Trace political spending, campaign contributions**



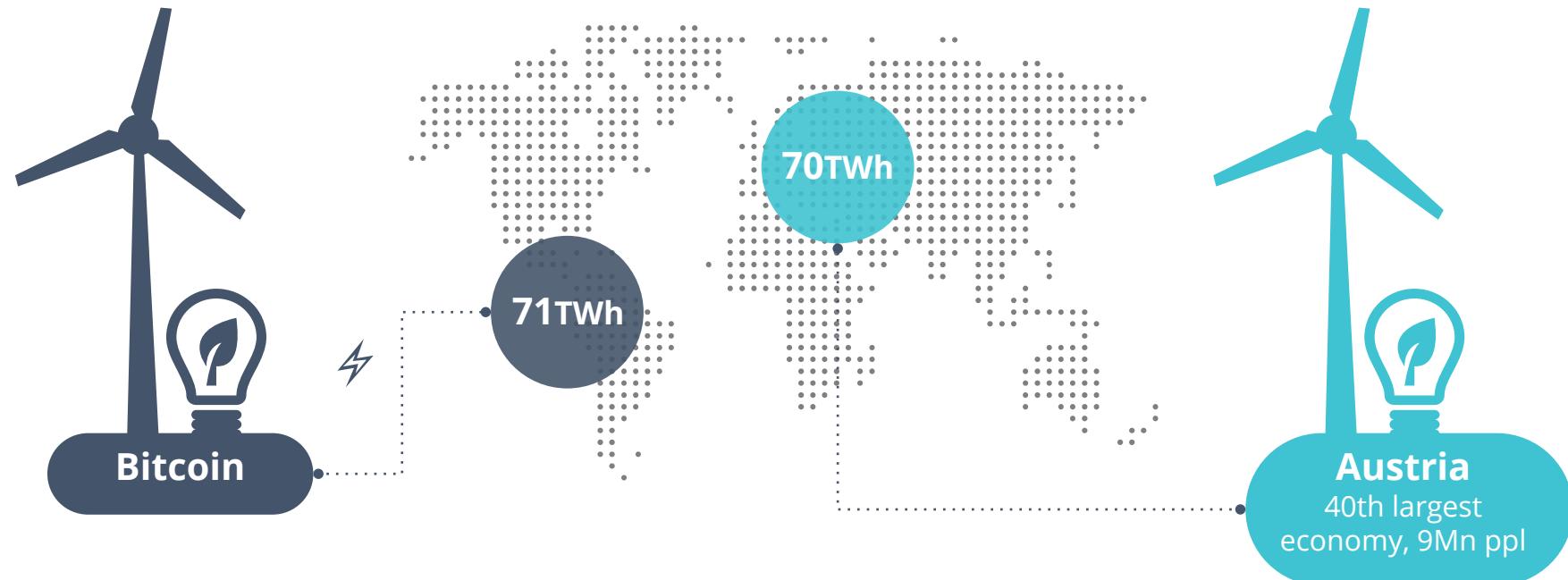
Beyond the Hype: Rational perspective

- ◇ **Maturity:** Right now the technology and fundamental protocols still need to be refined before global adoption.
- ◇ **Speculation:** The field is very hyped right now and beware of frauds, scams. Always do thorough due diligence.
- ◇ **Policy & Regulation:** Many policy frameworks have to be created and implemented before wide scale adoption can become a reality.



Scalability Issue: Energy Consumption

Bitcoin, Ethereum and many other Blockchain Technologies currently utilize Proof of Work as their consensus algorithm. Scalability problem and waste of resources. It is estimated that



Source: <https://digiconomist.net/bitcoin-energy-consumption>

Positive Global Outcomes & Opportunities

- ◇ User Owned Data
- ◇ Financial inclusion
- ◇ Sharing Economy: True decentralized services, cut costs of platform owners.
- ◇ Limit Corruption, add transparency
- ◇ Open-source, free technology, empowering individuals.





Thanks!

Let's stay connected:

<https://alex.fo>



E-mail
afo@berkeley.edu



LinkedIn
linkedin.com/in/alexanderfo



Twitter
@alexanderfo



Thanks!

Let's stay connected:

<https://scet.berkeley.edu>



E-mail
afo@berkeley.edu



LinkedIn
[linkedin.com/in/alexanderfo](https://www.linkedin.com/in/alexanderfo)

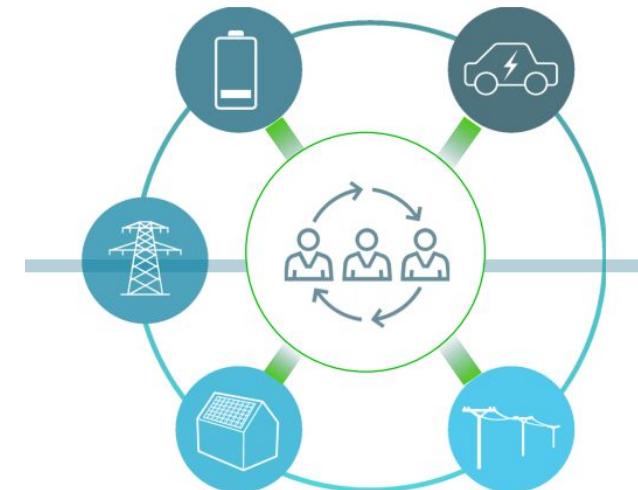


Twitter
@alexanderfo

Blockchain Use Cases: Energy

Microgrids, Energy Certificates, Renewables

- ◊ **Microgrids:** Automatic transactions between producers and consumers. Powerpeers in Netherlands and Exergy in Brooklyn.
- ◊ **Track clean energy:** See if it's generated by fossil fuels, solar energy or wind. **Organize the messy market of traded energy certificates.**



The New Energy Economy

Source: https://www.eniday.com/en/technology_en/blockchains-energy-market/

company that handles tokenization sells the property? Token owners just own tokens. They have no legal rights of the property and thus are not entitled to certain properties, such as houses or gold.

The same applies to gold and other assets are needed to accommodate these new business models.

Another problem is that this system jurisdiction is prohibited to sell fractional parts of company shares. Centralization through clearing.

Again, legal changes are necessary to successfully implement contracts. To create a trustless tokenization of company stocks environment. While this is possible

to achieve when tokenizing digital assets, this is not the case.

Therefore, we have to accept a traditional asset such as real estate, equity, bonds, and VC funds.

Why is this beneficial? Tokenization makes the issuance and trading of assets more efficient by cutting out the middle person. This cuts out administrative fees, cuts down the time of issuance (getting rid of timely IPOs), and

Blockchain Use Cases: Fintech pt. 3

Security Token Offering / Tokenizing Assets

When you buy a stock you need to trust: You are trusting: Brokers; Transfer Agents; Registrars;

Clearing Firms; Custodians; and more

If that same share was tokenized, the only entity

have to trust is the issuer.

