Blockchain-X

Blockchain Technology & Business Applications

Alexander Fred-Ojala
Research Director, Data Lab
SCET, UC Berkeley
afo@berkeley.edu

TiE inflect 2018

Pantas and Ting Sutardja Center for Entrepreneurship & Technology
Berkeley Engineering

May 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'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-X

OUTLINE

1. **Understanding Blockchains**

   A Comprehensive Overview of Bitcoin: Blockchain's PoC app

2. **Beyond Bitcoin**

   Ethereum, Smart Contracts, Dapps

3. **Blockchain Use Cases**

   Web3.0, Fintech, Supply Chain, Health Care, Government etc.

4. **Current State, Problems to solve & Future**

First:
QUESTIONS TIME!

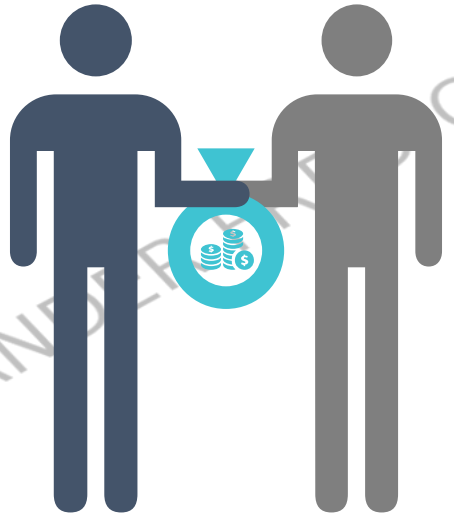
This is **Money**!

Medium of Exchange

Facilitate exchange of *value.*

Requires **Trust**

Everyone must agree that the money is valuable.



Scales the Economy

Speed up transactions.
Split value into parts.

Store of **Value**

Accumulate and store value over time. Requires trust!

This is a **Bank**!

Centralized **Trust Agency**

Private company regulated by governments.
Store resources.

Account **Managers**

Keeps account information. Only banks can verify the authenticity of balances etc.

Identity Management

Links a person to accounts.

Offers paid **services**

Loans, stocks, credit cards, mobile apps etc.

Image source: http://www.clker.com/clipart-bank-blue.html

History of Money

LET'S START at the beginning!

History of Money

Blockchain-X
Alexander Fred-Ojala

Prehistory, **Year < 10k BC**

Oldest technology? First abstraction of value: Shells, barely, feathers.

Metal coins, Lydia, **~500BC**

Merchant's in Lydia, today's Turkey. Adopted by Greece, Roman Empire etc.

Notes, China, **1200 AD**

Notes and first fiat currency introduced in China.

Banks, Italy, **15th Century**

Medici family. Double entry ledgers. Track deposits and withdrawals. Inspired Central Banks.

Gold Standard, England, **1821**

Bank of England promises to redeem notes for gold. Brought stability to prices.

Fiat Money, Global, **Post WW1**

Means to increase money supply. Fiat currency has value only because of the guarantee of the issuing authority /government.

Credit Cards, USA, **1950**

Diners Club Card, first CC to be introduced

2008: Enter Bitcoin

The Genesis (PoC) Application of Blockchains

Digital money!

History of Bitcoin

Blockchain-X
Alexander Fred-Ojala

Bitcoin Whitepaper, **2008**

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

10k BTC for a Pizza, **2010**

First real-world transaction: $25, 2 pizzas in Jacksonville, Florida for 10,000 BTC. ¼ cent.

First Altcoins, **2011**

Namecoin, Litecoin etc. fork and modify Bitcoin's code to create alternative currencies.

87% crash in price, **Nov 2013**

The bitcoin price falls 87% from one day to another. Largest crash ever.

Mt Gox hack, **2014**

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

Bitcoin enters the mainstream, **'16-'17**

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

FUTURE **2025**

What is **Bitcoin**?!

Decentralized & **Trustless**

Regulated by a community.
Trust in the technology protocols and rules set by the community.

Pseudo-anonymous **Identities**

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

Public ledger maintained by anyone

Full transaction history is public.
Incentive structures let you trust every node.

Transfer Money **P2P**

Transact money Peer-to-Peer, without intermediary or central authority that validates the transaction.

bitcoin / **Bitcoin**?!

- ***bitcoin*** *is the currency*

  (BTC = digital money)

- ***Bitcoin*** *is the technology / protocol*

  (almost like the infrastructure for a decentralized bank)

Bitcoin:
User Perspective

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

Private key signs transactions
Public key verifies signature

Private / Public **Keys**

Bitcoin Identity: *To send and receive bitcoins, unique private - public key pair.*

Private Key:

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

- Generated from random processes (BIP 39, mnemonic seed, 2048 words)
- Used to sign transactions and prove ownership.

Public Key:

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

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

The Bitcoin Network

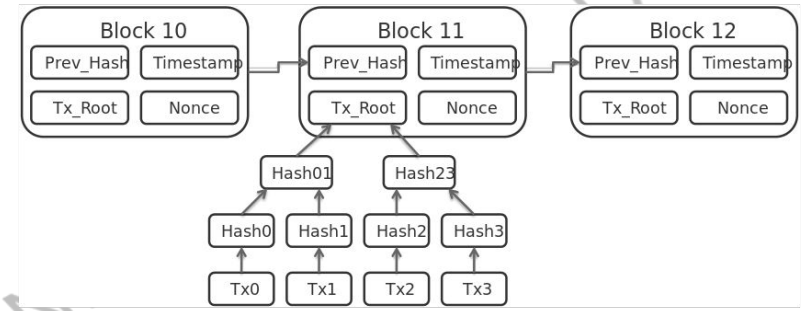
- **Decentralized P2P network of computer nodes** that keeps track of valid payments. Anyone can join, download a copy of the transaction history, and help maintain its validity. Nodes exist globally. **No central point of failure**, gets around the honey pot problem.

- Nodes validating transactions are called **miners**. They group transactions into blocks, and link blocks in an immutable chain. This is called the **Blockchain** -- a chain of blocks with the complete transaction history.

Blockchain: Record Keeping

Tracks every transaction since the Genesis block

- **Ledger, keeping track of transactions.** Like an append only spreadsheet.
- **Transactions are grouped together in blocks.** A new block is added every 10 minutes.
- **Immutable & Cryptographically Secured** by including the hash of the previous block to the current block
- Transparent, anyone can **audit**



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

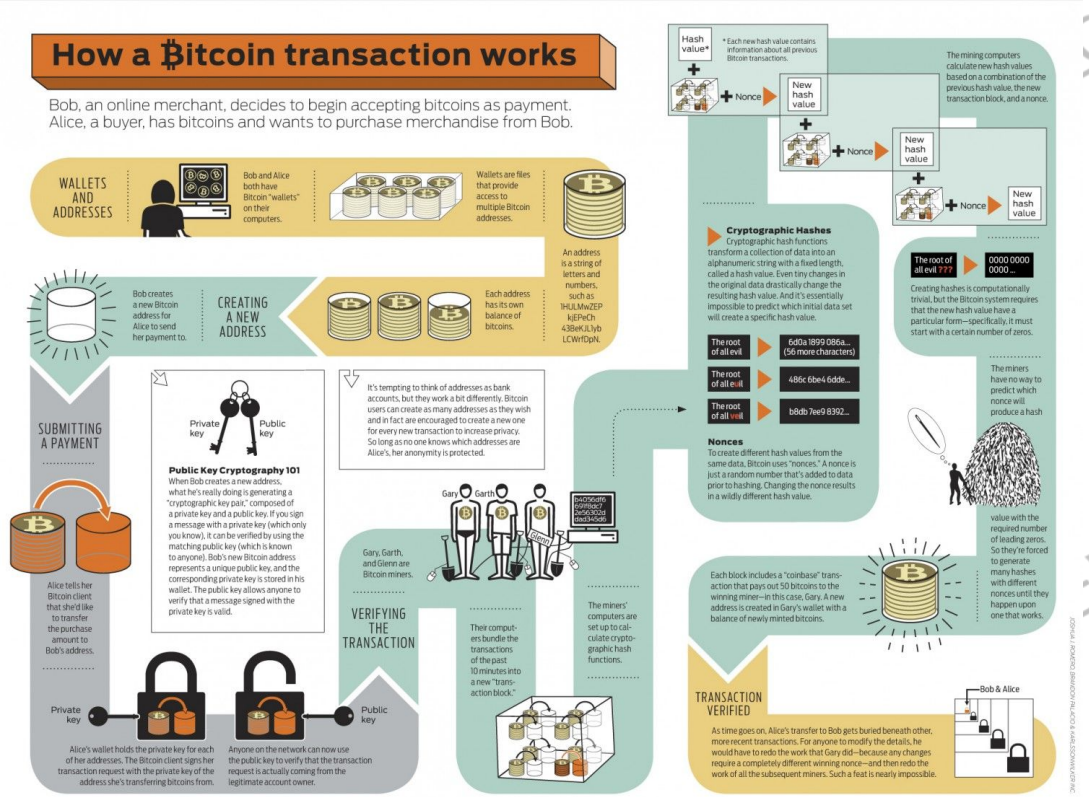
Bitcoin: Incentivizing Participation

Why do peers wanna join and set up mining rigs?

1. **Monetary incentive:** Every time the puzzle is solved a small reward is added to the solver's balance. Plus transaction fees.
2. Nodes are called **miners because they are rewarded money**, but their main task is to maintain the ledgers.
3. Convenient way to **distribute new money.**

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

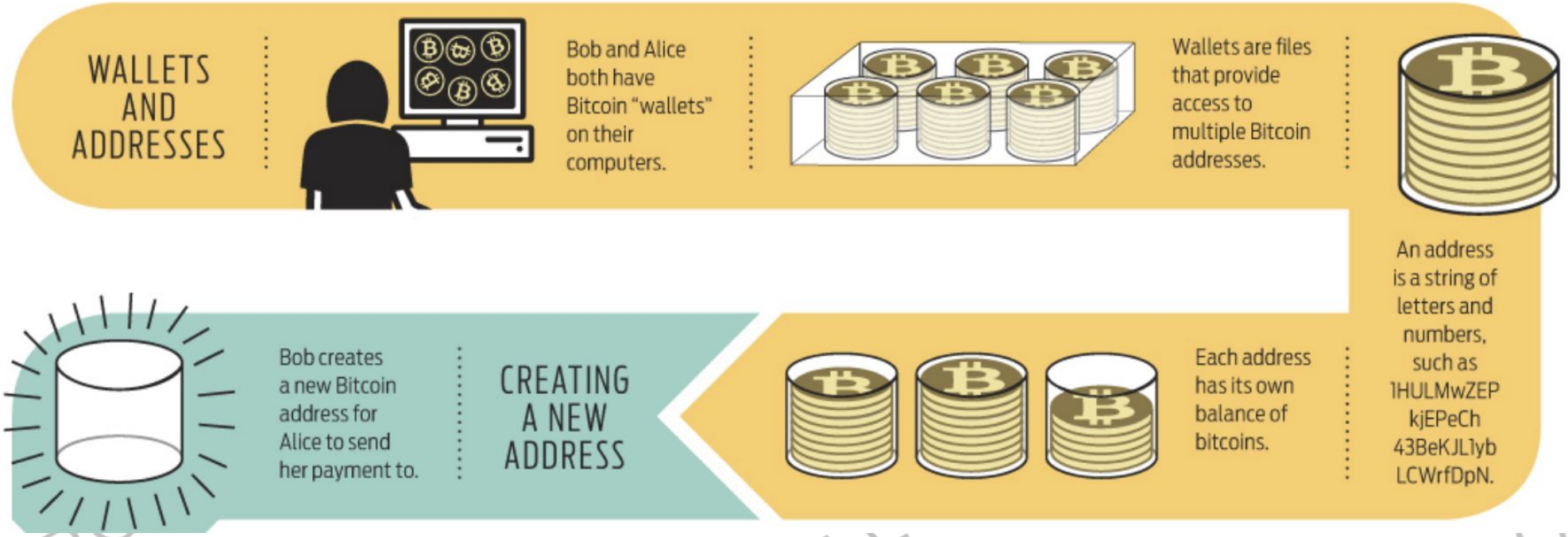
Bitcoin: System Overview



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.



Source: IEEE Spectrum

Source: IEEE Spectrum

Bitcoin: System Overview (2/4)

Submitting Payment

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

Private key

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.

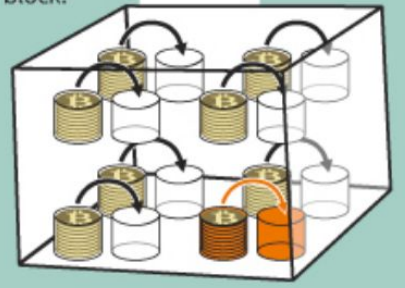
Public key

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.

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)

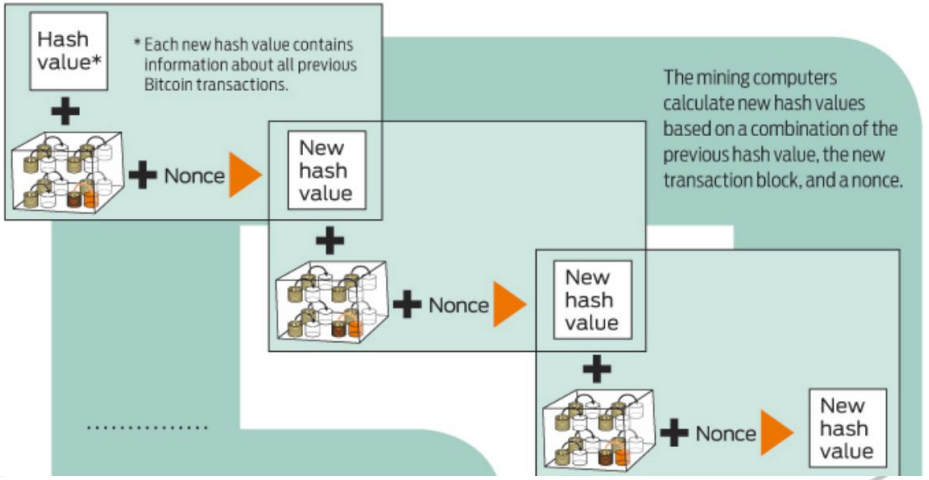
Cryptographic Hashes

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	6d0a 1899 086a... (56 more characters)
The root of all e**u**il	486c 6be4 6dde...
The root of all **ve**il	b8db 7ee9 8392...

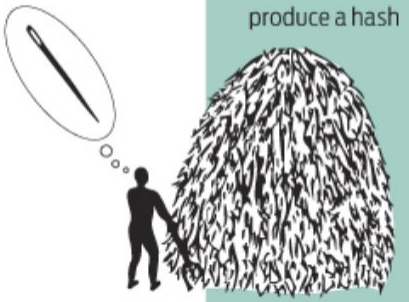
Nonces

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

Blockchain: Hashes

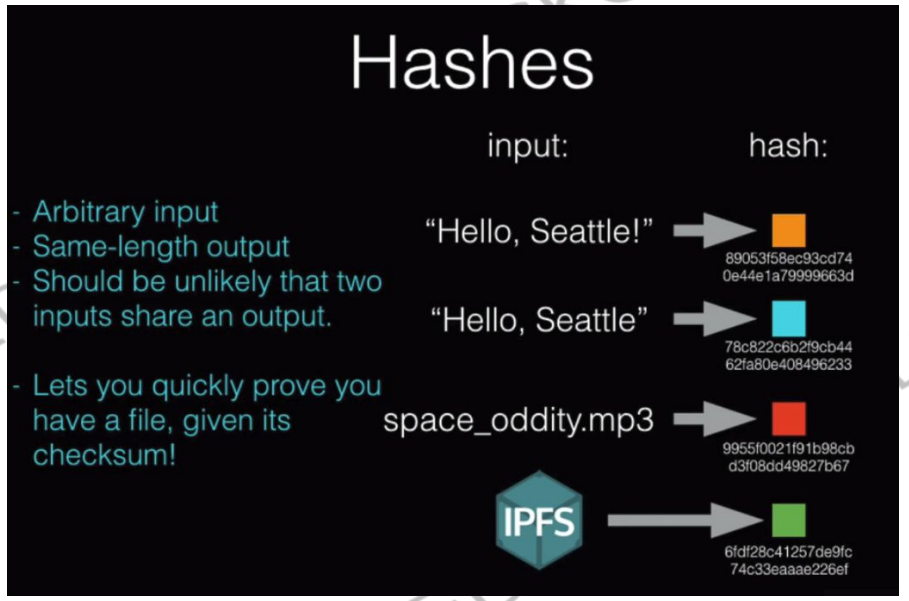
A hash is a **deterministic one way function with arbitrary input and an output of fixed length**, e.g 1gwv7fpx97hmavc6inruz36j5h2kfi803jnhg.

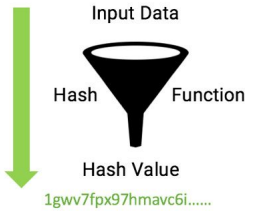
The same input will always create the same output.

Small change in input creates vastly different output

Given output y we cannot recreate input x

f(fruits+blender) = smoothie $f(x) = y$





Prove something without revealing the information beforehand.

Alice knows the answer to a math problem, wants to prove she knows it but not reveal the answer. Hash the answer. Bob can verify, when / if he finds the answer.

$$md5(\text{"hello world"}) = 5eb63bbbe01eeed093cb22bb8f5acdc3$$

Source: https://www.youtube.com/watch?v=-SMliFtoPn8

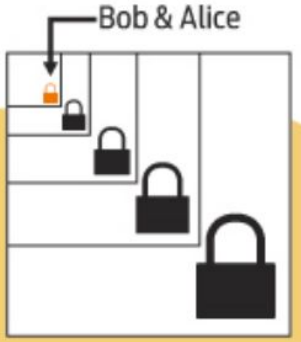
Source: learncryptography.com/hash-functions/what-are-hash-functions

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.



Source: IEEE Spectrum

Bitcoin: **Characteristics of a currency**

1. **Scarcity:** Finite units. Deflationary BTC. 21Mn in total. Mining reward halved every X years. After 2140 no more bitcoin will be created.
2. **Fungibility:** Interchangeable for identical units. Swap accounts should be OK.
3. **Divisibility:** Subunits for ease and precision of payments. 1 satoshi is 10^-8 BTC
4. **Durability:** Long-lasting units. Bitcoin cannot be destroyed physically.
5. **Transferability:** Liquidity, for ease of transacting. Bitcoin is a global infrastructure.
6. **Legitimacy:** Trust the Bitcoin protocol, it has not been hacked for 10 years

We pay thousand of dollars for hashes on a ledger. Network money!

User owned and managed

Post-Bitcoin

Bitcoin was one of the first to combine:

- **Cryptographic identities:** Public / Private. Reveal nothing about yourself. Prove claim ownership of assets.
- **Consensus protocol:** Nakamoto consensus. Tie voting power to specific external resource (computing power, resources). Majority decisions.
- **Blockchain:** Immutable source of truth. Append only. Decentralized database.

Post-Bitcoin: **Smart Contracts**

- **“Standard” Contract definition:**
  - Agreement with another party.
  - Some entity to enforce the contract and the terms (however, terms can be violated)
- **Smart Contract** (Nick Szabo, 1996):
  - Define terms of agreement in programmatic code.
  - Code that facilitates, verifies, and enforces both negotiation and execution of the digital contract.
  - Need trusted entity / tamper-proof computer to run code.


ethereum
HOMESTEAD RELEASE
BLOCKCHAIN APP PLATFORM

Enter Ethereum

- **Blockchain Smart Contract Platform:**

  Trustless environment to execute smart contracts

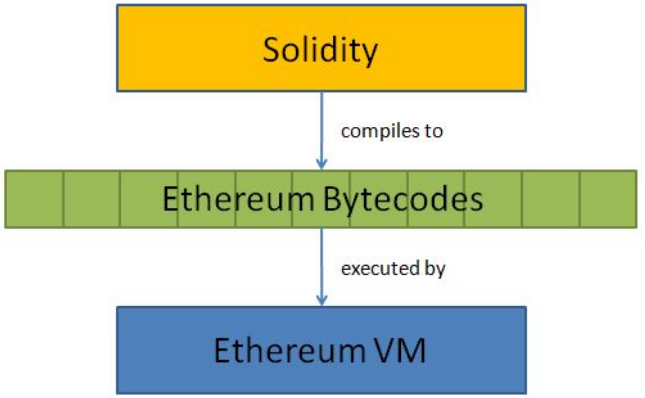
- **Distributed Computer to develop Dapps:**

- **The total network has a state**, not just transactions.
- Transactions and smart contract executions change global state (did I send email, vote etc?)

Etheruem

Native Asset: Ether (ETH)

- Basis of value in Ethereum ecosystem
- Needed to align incentives, and reward miners.



The Ethereum Virtual Machine

- Global distributed computer that runs smart contracts
- Smart Contracts require gas to be run (to not overload the network)
- Turing Complete (any programmatic code can run on the network)

Code in Solidity -> Ethereum Bytecodes -> EVM

scet.berkeley.edu Source: blog.oraclize.it/overcoming-blockchain-limitations-bd50a4cfb233

Ethereum Smart Contracts

Computer protocol to digitally facilitate, verify, or enforce a contract without 3rd parties.

- Stored as code on the Blockchain. Evaluated by all nodes.
- Transparent, distributed, and decentralized agreement.
- Smart Contracts can call other Smart Contracts -> Dapps

Altcoins / Cryptocurrency / Tokens

- *Digital currency, medium of exchange* and store of value
- Utility token or security
- Application-centric or general
- Based on new or existing blockchain
- Ether, Litecoin, Zcash, NEO, Dash…

ICO: Initial Coin Offering

- *The introduction of a new cryptocurrency / token*
- Incentivizes a community to buy into the idea -> Scale factors and network effects.

Today over 3000 coins have been introduced to the world, most of them on the Ethereum Blockchain using the ERC20 standard*.

List of inactive coins: *deadcoins.com*

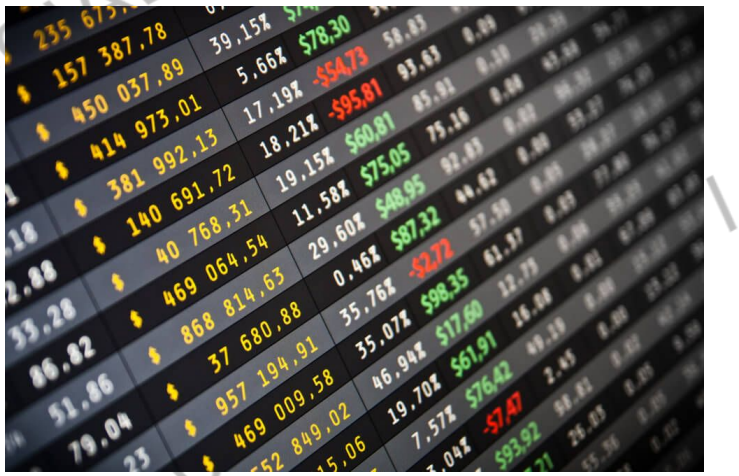
** coinranking.com (April 2018)*

Blockchain **Terminology**

Exchange

Platform where you can exchange and swap cryptocurrencies. Almost like FOREX.

Decentralized exchanges are possible with Blockchain technology.



dApp (Decentralized Application)

- Open source, decentralized applications cryptographically secured and stored on a public Blockchain.
- Often uses a **token that is native** to the Blockchain or the application in order to be used.
- **Miners will be rewarded in the native token** for running the application.

Ethereum: Powering Web 3.0

Web 3.0

- Distributed file storage
- 24hour stock markets
- Decentralized exchanges
- CryptoKitties (scarce items)
- Decentralized file storage
- Store sensitive data and records
- Smart grid solutions for energy
- Supply chain management
- Medical records
- Track goods
- Remittances
- Prediction markets
- Gitcoin
- Federated Learning
- Content creation automatic compensation
- Get paid to reply to emails

Blockchain

Examples of Industry Use Cases

FinTech

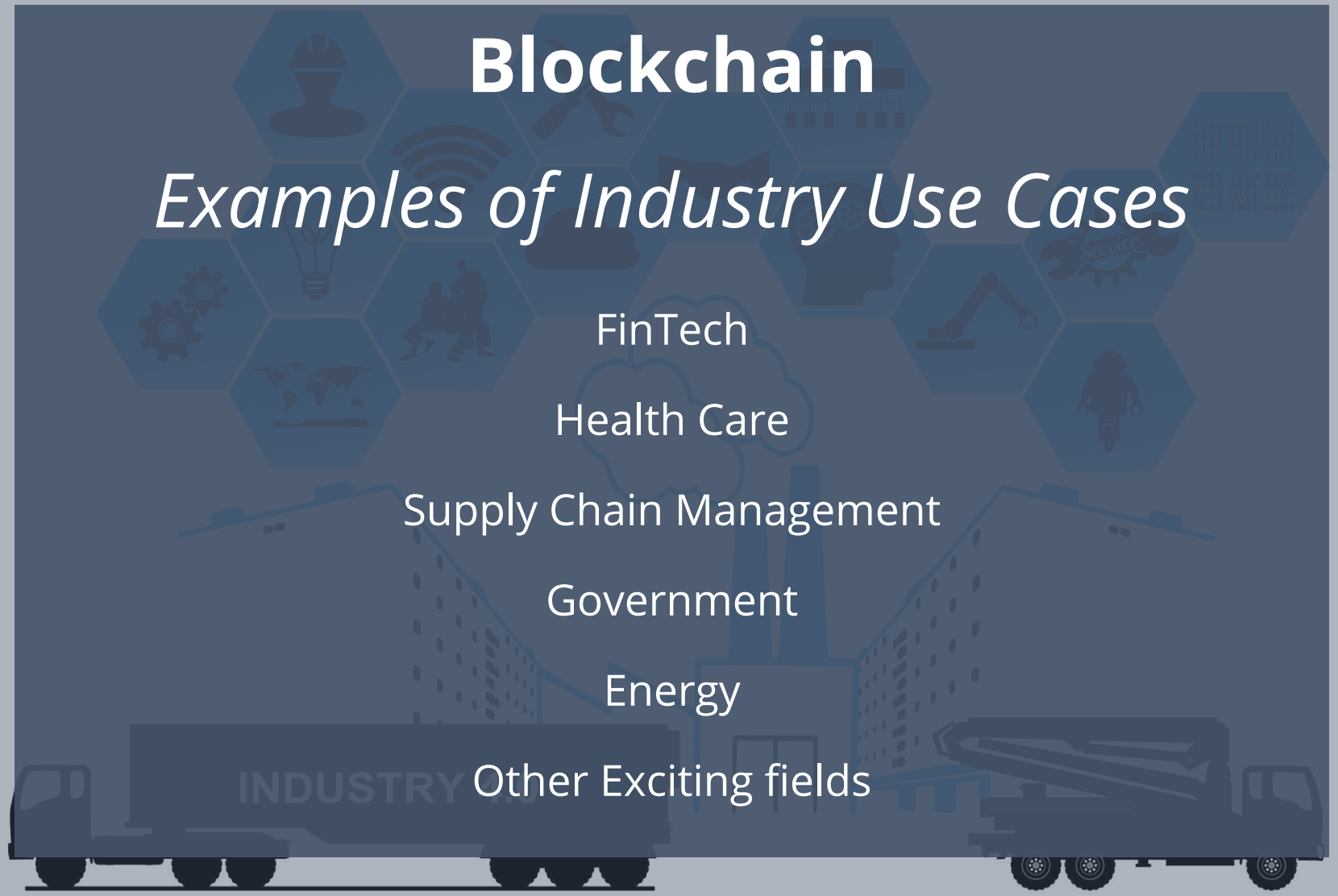
Health Care

Supply Chain Management

Government

Energy

Other Exciting fields



Blockchain Use Cases: **Fintech**

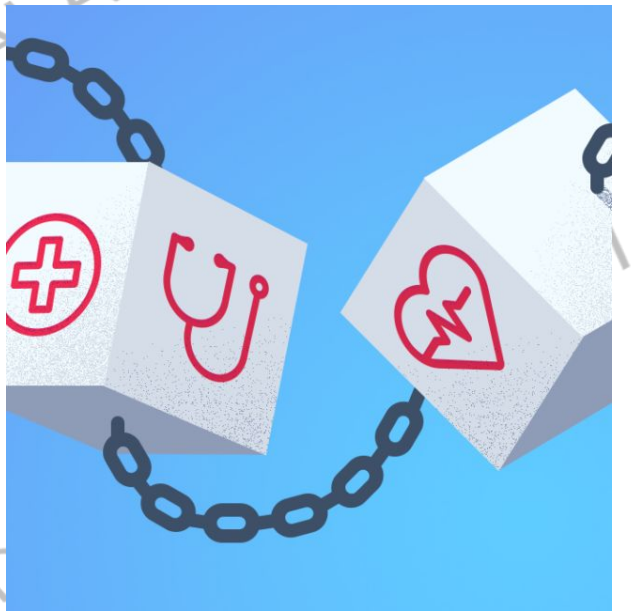
P2P Global Payments, P2P Loans and Financial Inclusion

- **Bank the 2Bn unbanked and 6Bn under-banked**. Anyone can join.
- Almost **instant verification and settlement of payments**
- **Lower transaction fees.** Improve remittances, no corruption for humanitarian aid
- **Efficient exchange of assets and securities.** Opens possibility of 24hr stock exchanges.
- **P2P Loans**
- **Collaborative KYC**

Blockchain Use Cases: **Health Care**

Safe and Shared Health Records, Tracked Pharmaceuticals

- **Store and share medical history and health records.** Pilot in Estonia running today!
- **Counter fragmented systems.**
- **Aggregate sensitive medical data** in secure repositories, enables researchers to do analysis
- **Patient owned and controlled data**
- **Compliance** with rules and regulations



Blockchain Use Cases: **Supply Chain**

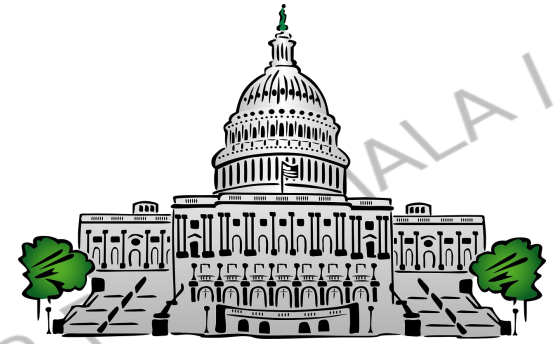
Track Goods w/ IOT, Limit Paperwork, Improved Security

- **Track goods, from origin to destination.**
  Simplify ownership transfer and automatic payments.
- **Food safety:** Let growers, regulators, consumers etc. gain permissioned access to information about origin state of food etc. Trace back source of bad food in the supply chain.
- **Track Pharmaceuticals:** Preserve drug integrity from production facility to consumer. Improve track-and-trace of serial numbers, to limit spread of fake drugs.
- **Maersk and IBM:** Limit paperwork for cargo shipments.

Blockchain Use Cases: **Government**

Open Government, Power to the People, Less Corruption

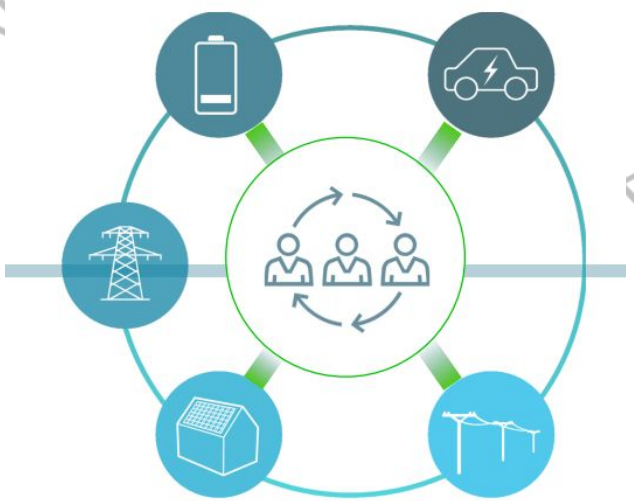
- **Self-sovereign identities:** Estonia has launched Blockchain based citizenship.
- **Blockchain-based voting.** Sierra Leone, blockchain based election. Diminish the likelihood of electoral fraud. (Also works for stock voting, NASDAQ)
- **Land records and titles:** Ukraine, Sweden
- **Refugee camps:** To help distribute food. Jordan.
- **Political spending, campaign contributions**



Blockchain Use Cases: **Energy**

Microgrids, Energy Certificates, Renewables

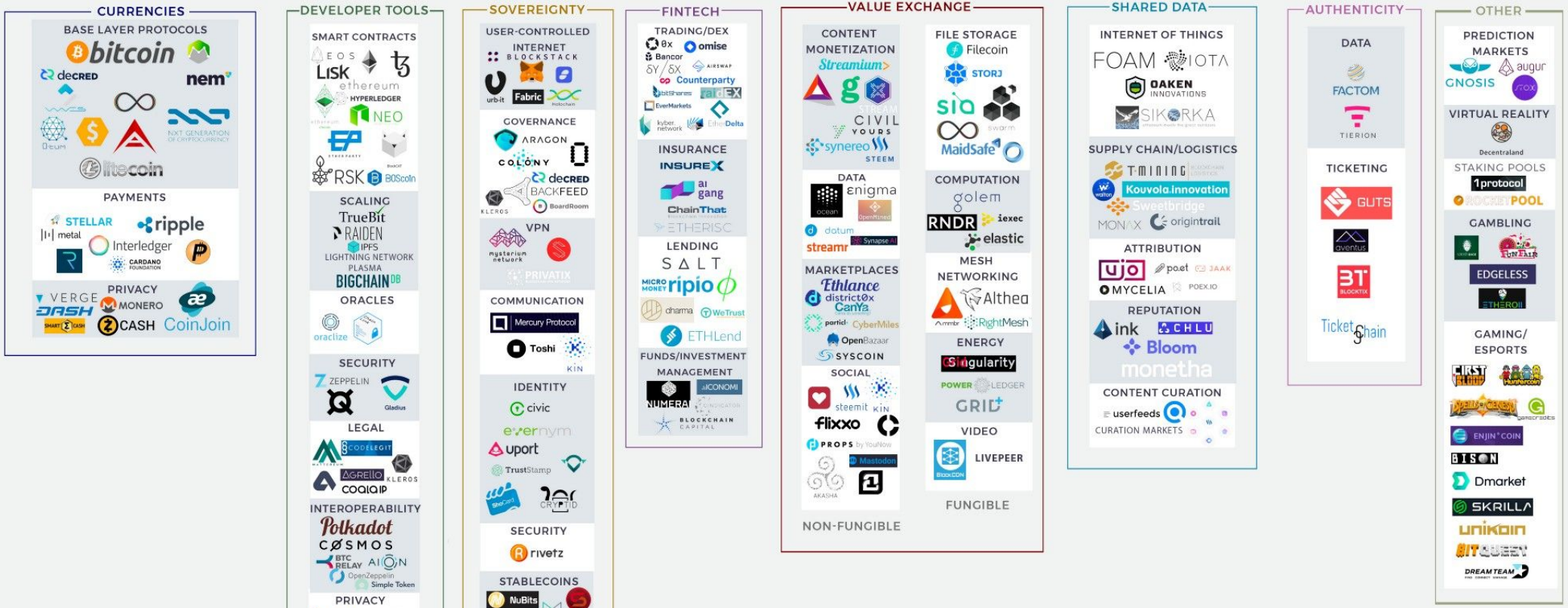
- **Microgrids:** Track consumption and production. Powerpeers in Netherlands and Exergy in Brooklyn.
- **Track clean energy:** Right now no one can really discern if it's generated by fossil fuels, solar energy or wind. **Organize the messy market of traded energy certificates**.



The New Energy Economy

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

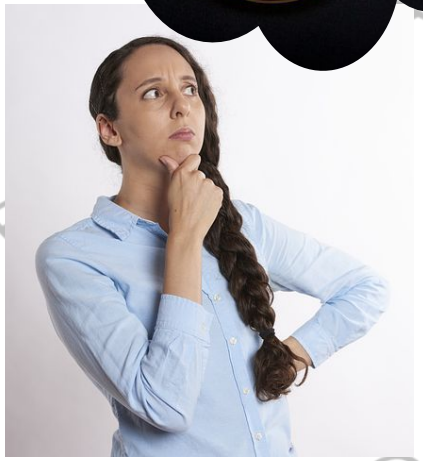
Overview: Exciting & Promising Blockchain Projects



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

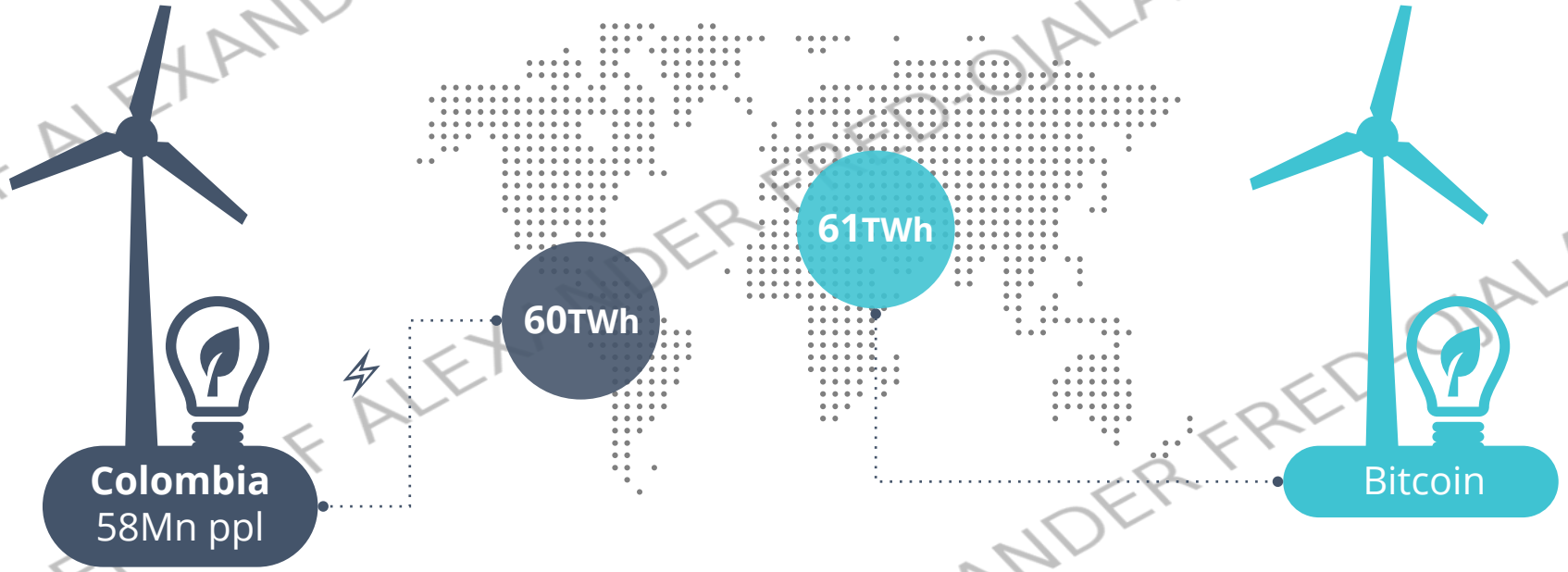
Beyond the Hype: Rational perspective

- **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

Blockchain 101: **Hard numbers**

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

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

3. Ratio of **Female Bitcoin Owners**

Only 5-7%

2. Number of **Total Unique Users of Blockchain tech**

2.9 - 5.8Mn

4. Blockchain **Disk Space**

Bitcoin: **164Gb**
Ethereum: **63Gb**

1. ttps://coinmarketcap.com/charts/
2. ttps://www.reddit.com/r/Ripple/comments/80hd4j/ripplexrp_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)

Approx numbers from April 2018

Positive outcomes

- **Data Privacy:** Blockchain tech has the potential for users to own their personal data, think of it as reversed user agreements. Services needs to sign how they can use data
- **Financial inclusion:** Today there are 2 billion adults without a bank account. Bitcoin and other cryptocurrencies are free for anyone to join. Most of them have a cellphone.
- **Sharing Economy:** Decentralize services, cut costs of middle men. True Airbnb, Uber.
- **Limit waste of resources and speed up services:** Limit use of paper work, store data in a more secure and auditable manner.
- **Open-source, free protocols, empowering individuals.**

Thanks!

Connect with me: https://alex.fo

E-mail
afo@berkeley.edu

LinkedIn
linkedin.com/in/alexanderfo

Twitter
@alexfroj

Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering