Blockchain-X

Blockchain Technology & Business Applications

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

Ikhlaq Sidhu
Founding Director, SCET
Professor, IEOR
UC Berkeley

Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering

May 2018

OUTLINE

1. **Understanding Blockchains**

   A Comprehensive Overview of Bitcoin

2. **Beyond Bitcoin**

   Ethereum, Smart Contracts, Dapps

3. **Blockchain Use Cases**

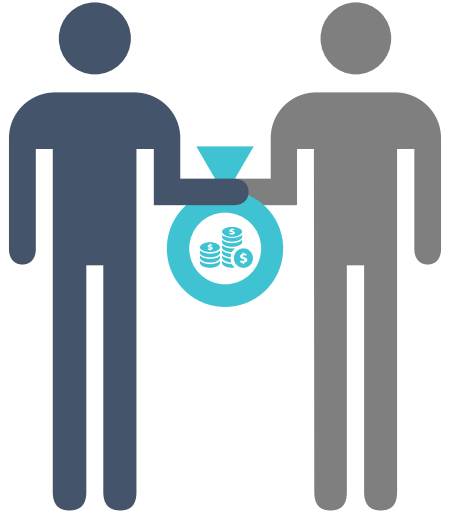
   Web3.0, Fintech, Supply Chain, Health Care, Government etc.

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

First:
QUESTIONS TIME!

What is **Money**?

In order to understand Bitcoin you have to understand money



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!

What is a **Bank**?

In order to understand Bitcoin you have to understand banks

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

This is a **Bank**!

Centralized **Trust Agency**

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. 800 Mn % increase in value.

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**

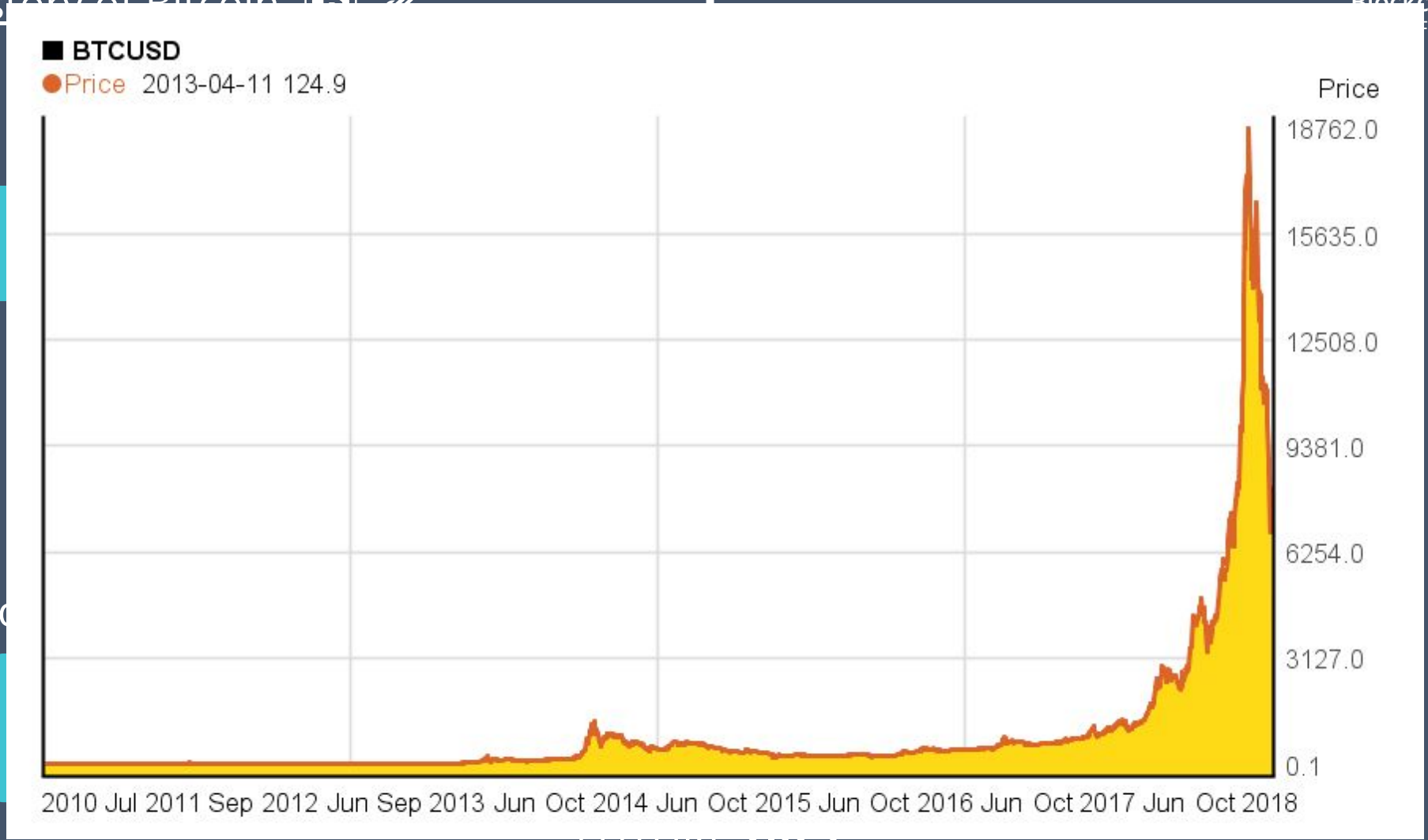
6% of all bitcoin ever created stolen from the largest exchange. $500Mn.

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**

History of Bitcoin



Bitc

FUTURE 2025

What is **Bitcoin**?!

Digital, Decentralized Currency

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

Financial Inclusion: Pseudonymous identities

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

Public ledger with transactions

Full transaction history is public, anyone can audit

Transfer Money Globally **P2P**

Transact money, without trusted 3rd party, intermediary or central authority that validates the transaction.

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: **~500Gb**

5. **Price** May 2nd 2018

$8300 / BTC
$680 / ETH

Approx numbers from May 2018

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)
5. https://coinmarketcap.com/

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 bitcoin.

Private key signs transactions

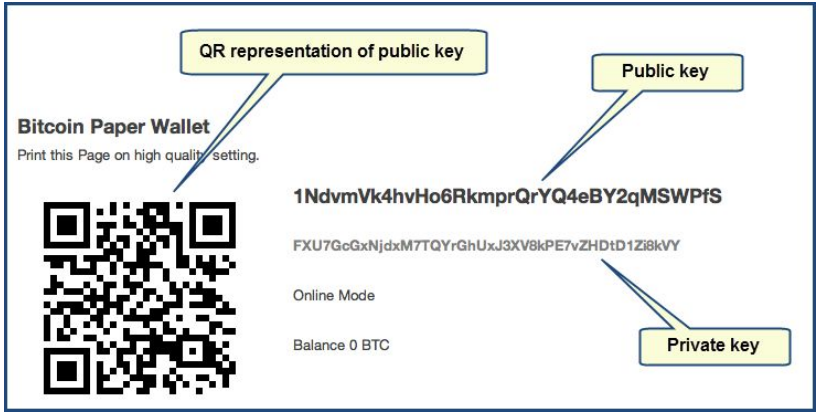
Public key verifies signature

Bitcoin Transaction Example

txid 90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219


```
{
"hash":"90b18aa54288ec610d83ff1abe90f10d8ca87fb6411a72b2e56a169fdc9b0219",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":0,
"size":226,
"in":[
 {
  "prev_out":{
   "hash":"18798f8795ded46c3086f48d5bdabe10e1755524b43912320b81ef547b2f939a",
   "n":0
  },
  "scriptSig":"3045022100c1efcad5cdcc0dcf7c2a79d9e1566523af9c7229c78ef71ee8b6300ab...[snip]
 }
],
"out":[
 {
  "value":"5.93100000",
  "scriptPubKey":"OP_DUP OP_HASH160 4b358739fc7984b8101278988beba0cc00867adc OP_EQUALVERIFY OP_CHECKSIG"
 },
 {
  "value":"1678.06900000",
  "scriptPubKey":"OP_DUP OP_HASH160 55368b388ccfe22a3f837c9eee93d053460db339 OP_EQUALVERIFY OP_CHECKSIG"
 }
]
}
```


- tx format version - currently at version 1
- in-counter - number of input amounts
- out-counter - number of output amounts
- tx lock_time - should be 0 or in the past for the tx to be valid and included in a block
- size - of the transaction in bytes



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. Fixed length string.

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

`5K8BwE76VsatQiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn`

Public Key:

External. Like a username. Generated from Private key. Deterministic. Fixed length string.

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

`1M3RLrXve5wcT2ZcJu8WXoXjdh4WXcWQA9`

Is the Private key **safe**?

Can someone else guess your private key or could randomness generate an exact copy of someone else's private key? (Or collision: 2 inputs giving same outputs?)

The total address space is 160 bits:

2^160 = 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976

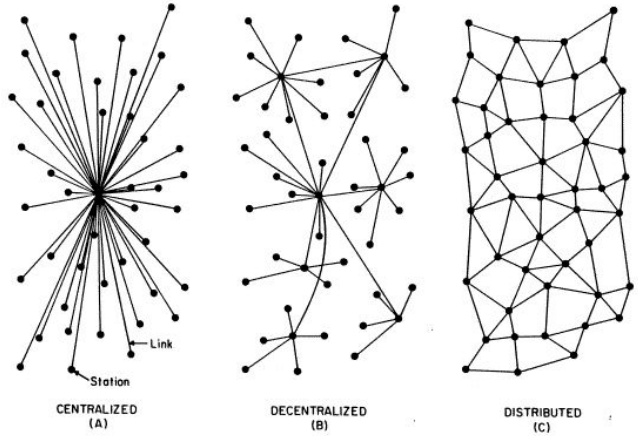
- There are only 2^63 grains of sand on Earth.
- The chance of guessing another private key in use is unfathomably low even if all computers ever created tried for the entire history of the universe

System Perspective: Bitcoin Network

- 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 is called the **Blockchain**.



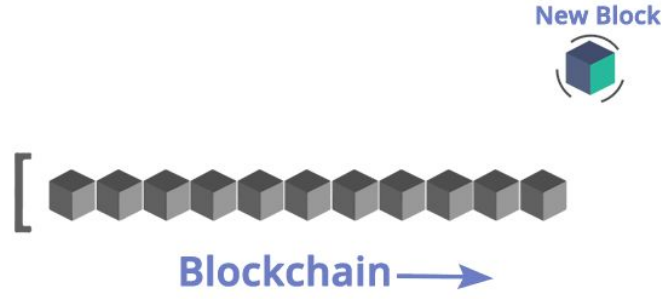
The Bitcoin Blockchain

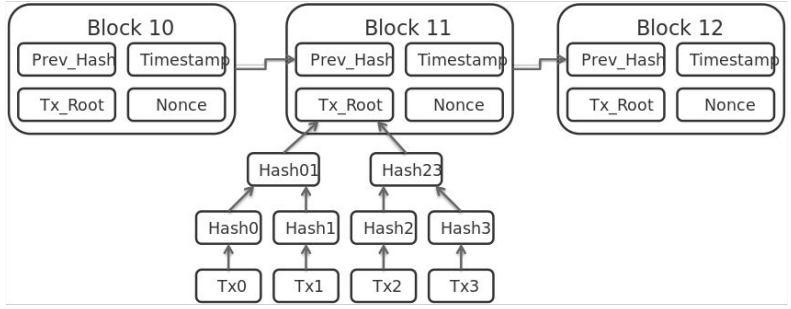
Tracks every transaction since the Genesis block

- **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/

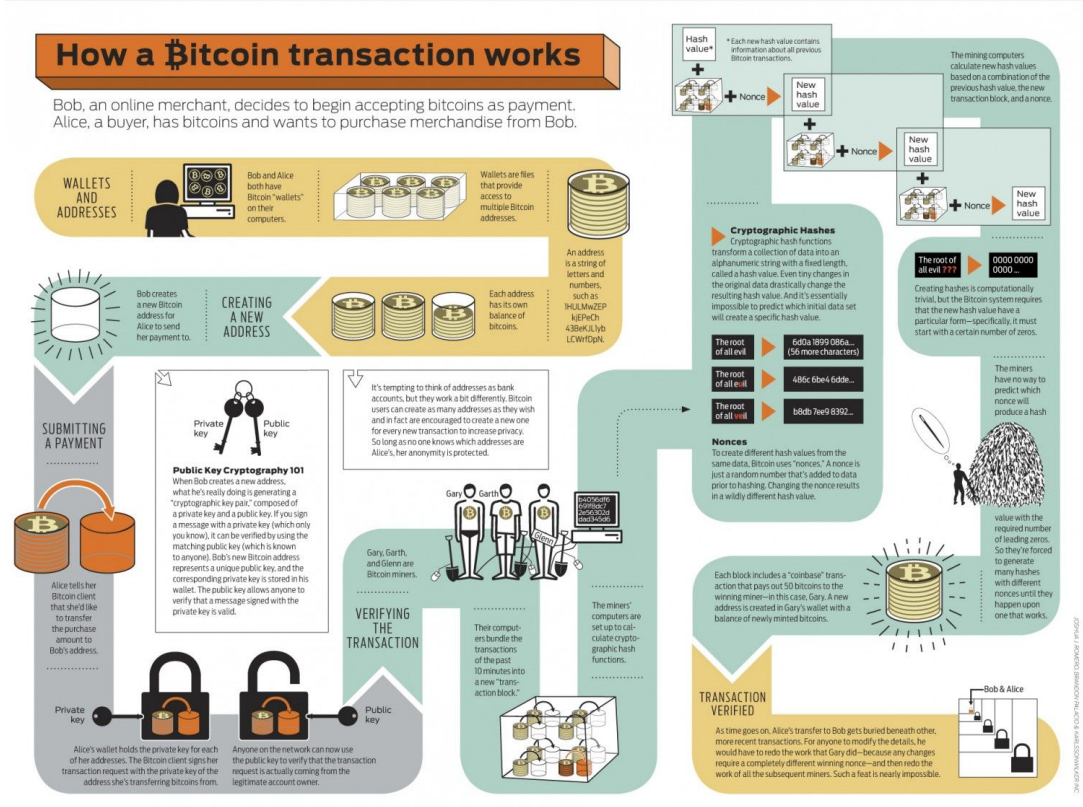
Bitcoin: Incentivizing Participation

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. This is why nodes are called miners. Maintain the ledgers.
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

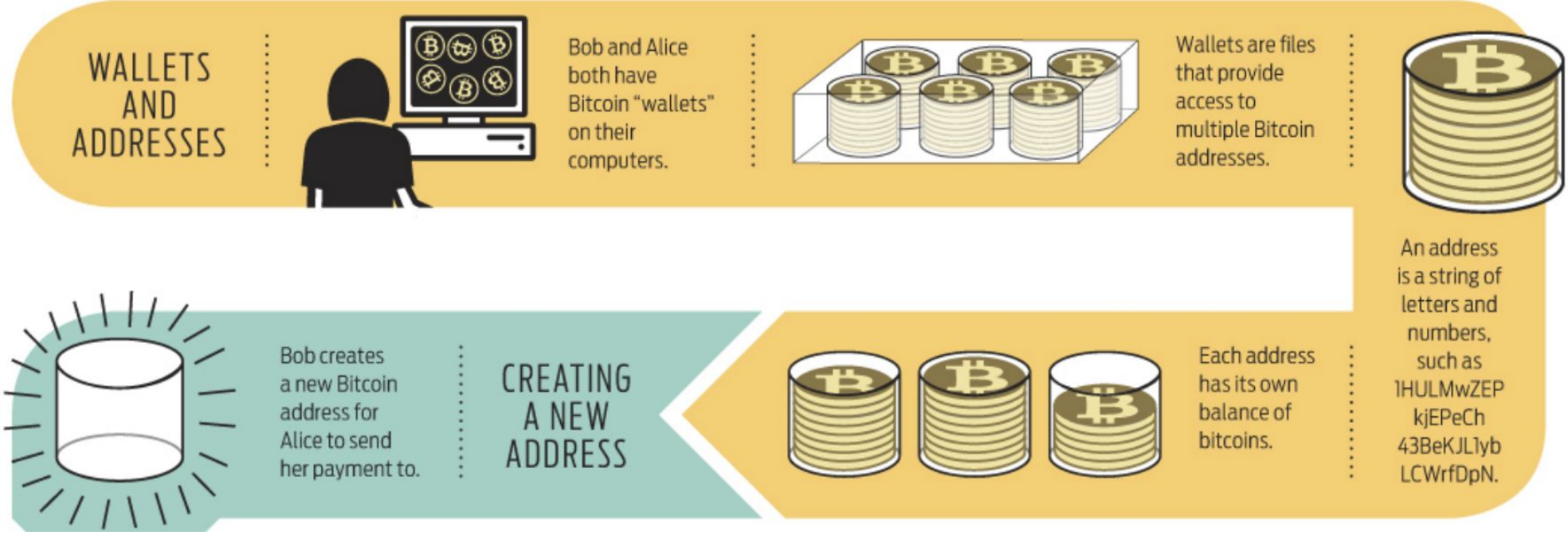
Bitcoin: System Overview



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.



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.

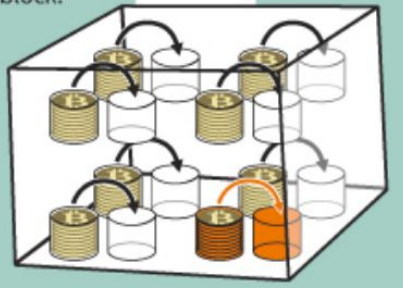
Public key

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)

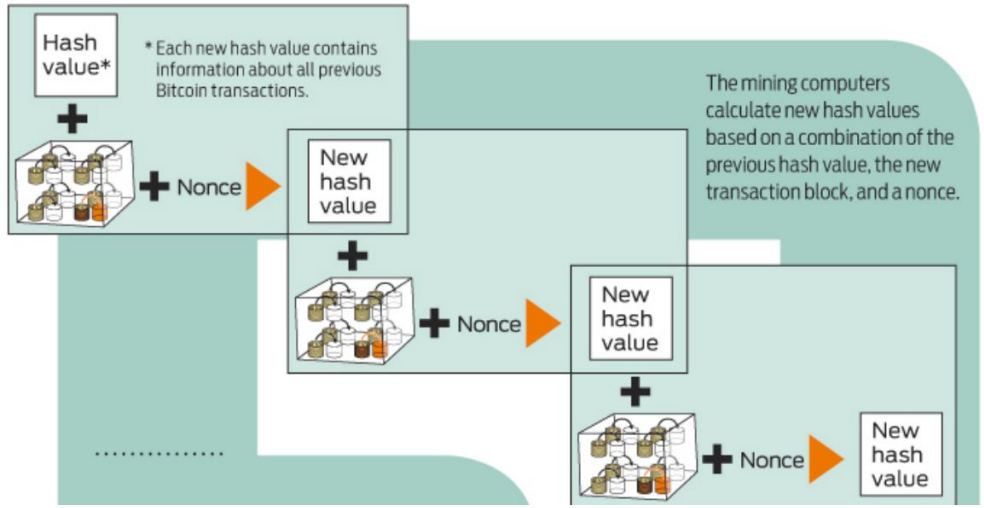
Cryptographic Hashes

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 euil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

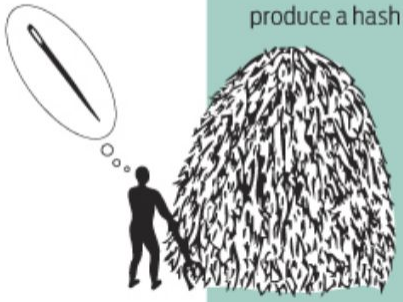
Nonces

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.

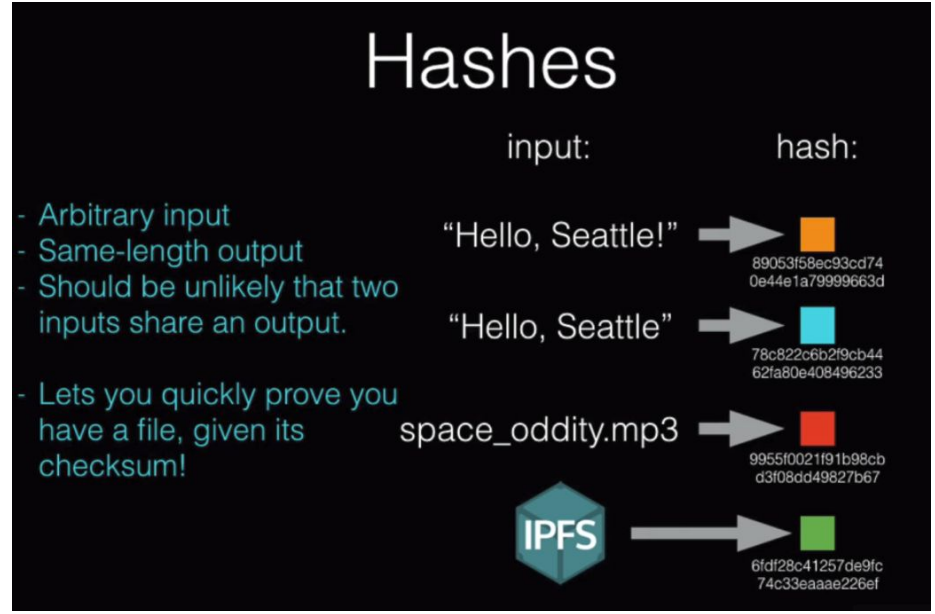


The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Source: IEEE Spectrum

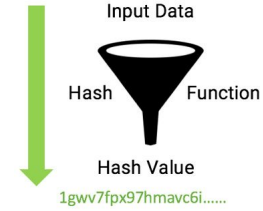
Blockchain: Hashes

Deterministic one way function with arbitrary input and a fixed length output, e.g 1gwv7fpx97hmavc6inruz36j5h2kfi803jnhg.



- **Same input will always create the same output.**
- **Small change in input -> vastly different output**
- **Given output y we cannot recreate input x:**

f_blender(fruits) = smoothie $f(x) = y$



Prove something without revealing the information beforehand.

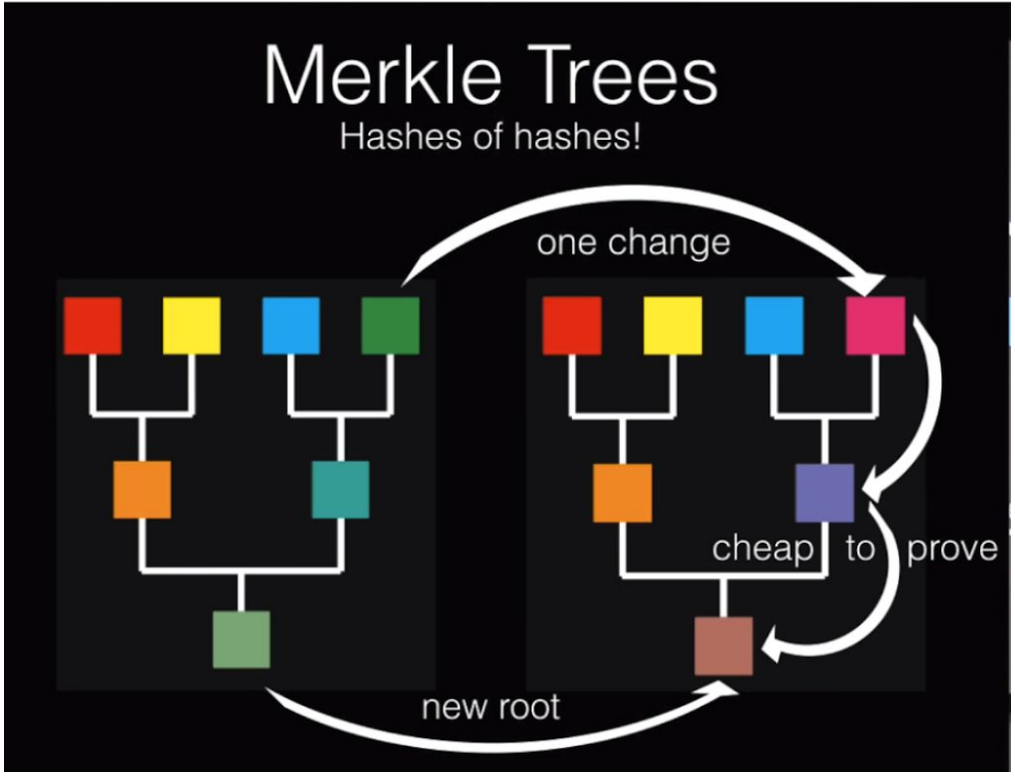
Alice knows the answer to a math problem, wants to prove she knows it but not reveal the answer. Hash the answer. Bob can verify, when / if he finds the answer.

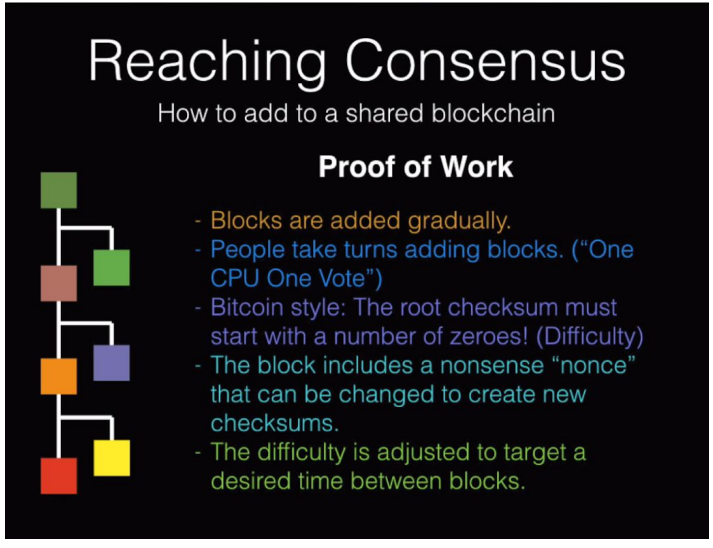
$$md5(\text{"}hello\ world\text{"}) = 5eb63bbbe01eeed093cb22bb8f5acdc3$$

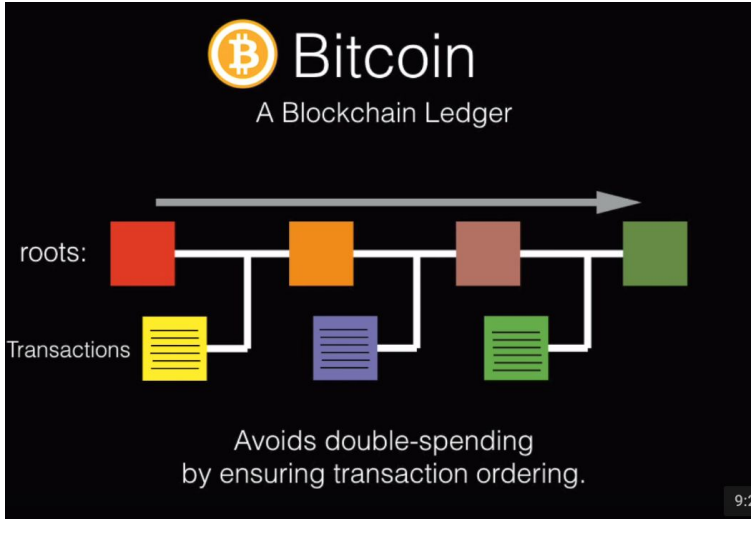
Source: https://www.youtube.com/watch?v=-SMliFtoPn8

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

Blockchain: Merkle Trees

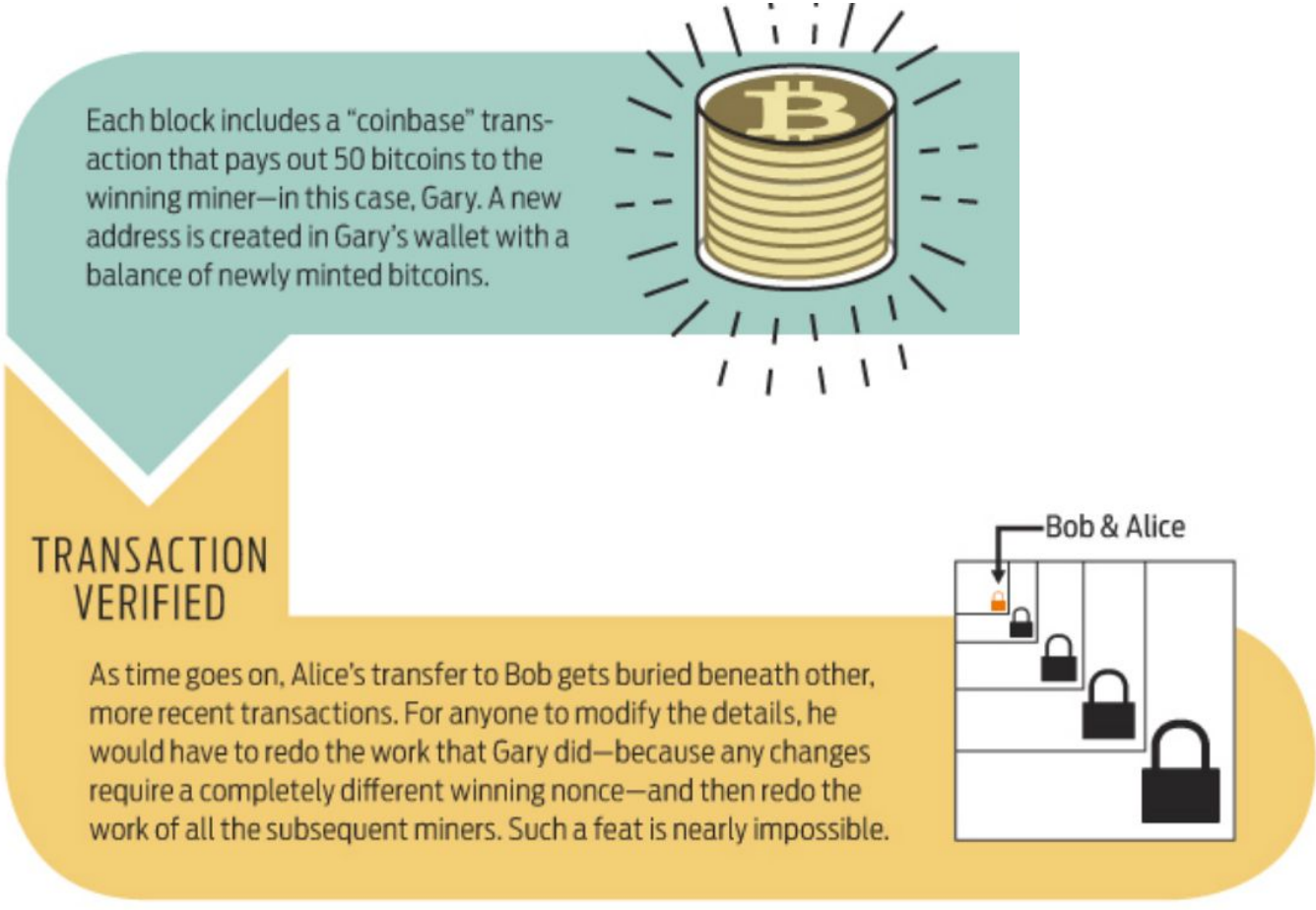






Source: https://www.youtube.com/watch?v=-SMliFtoPn8

Bitcoin: System Overview (4/4)



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

User owned and managed

User owned and managed

Digital, Network Money!

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

Post-Bitcoin

Bitcoin was first to combine:

- **Cryptographic identities:** Public / Private. Reveal nothing about yourself. 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.

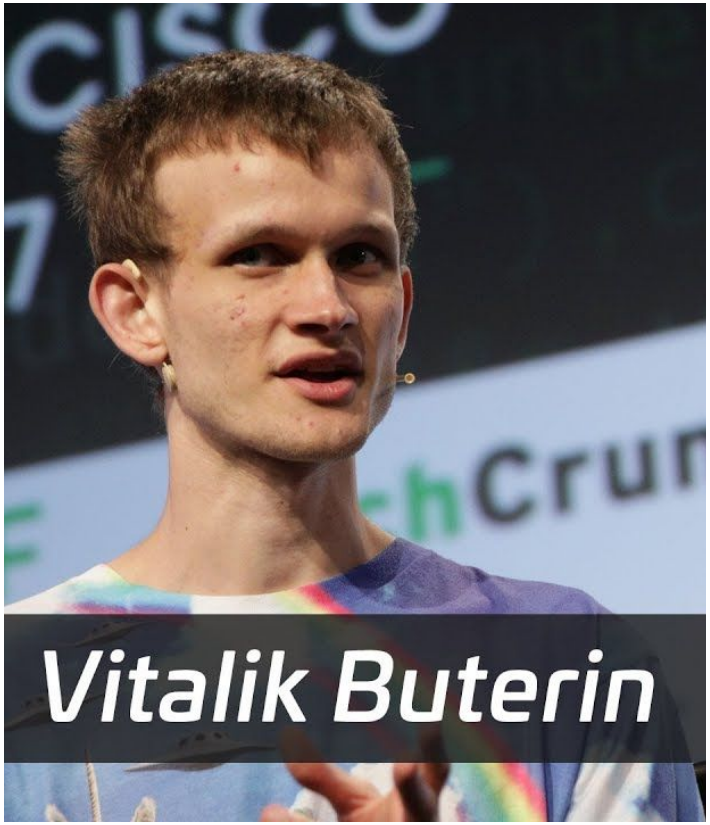
Post-Bitcoin: **Smart Contracts**

- **“Standard” Contract definition:**
  - Agreement with another party.
  - Some entity to enforce the contract and the terms (however, terms can be violated). Escrow agents etc.
- **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

VS.

Vitalik Buterin



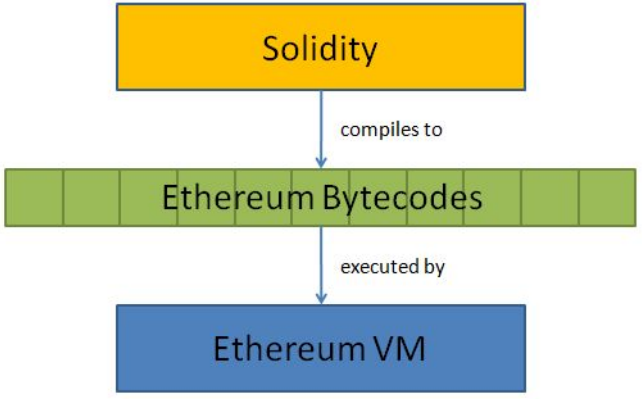

ethereum
HOMESTEAD RELEASE
BLOCKCHAIN APP PLATFORM

Enter Ethereum

- **Blockchain based Smart Contract Platform:**
  - Trust the network to execute the smart contract
  - **The total network has a state**, not just transactions.
  - Transactions and smart contract executions change state.
- **Native Asset: Ether (ETH):**
  - Basis of value in Ethereum ecosystem

ethereum

Ethereum Virtual Machine



A Distributed World Computer for Dapps

- Global distributed computer that runs

  smart contracts and decentralized applications
- Turing Complete (any programmatic code can run on the network)
- Smart Contracts require gas (ether) to be run

Code in Solidity -> Ethereum Bytecodes -> EVM

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

dApp (Decentralized Application)

- Applications that utilizes smart contracts as components.
- Often requires 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.

ICO: Initial Coin Offering

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

Over 3000 cryptocurrencies exist, most of them on the Ethereum Blockchain using the ERC20 standard*.

List of inactive coins: deadcoins.com

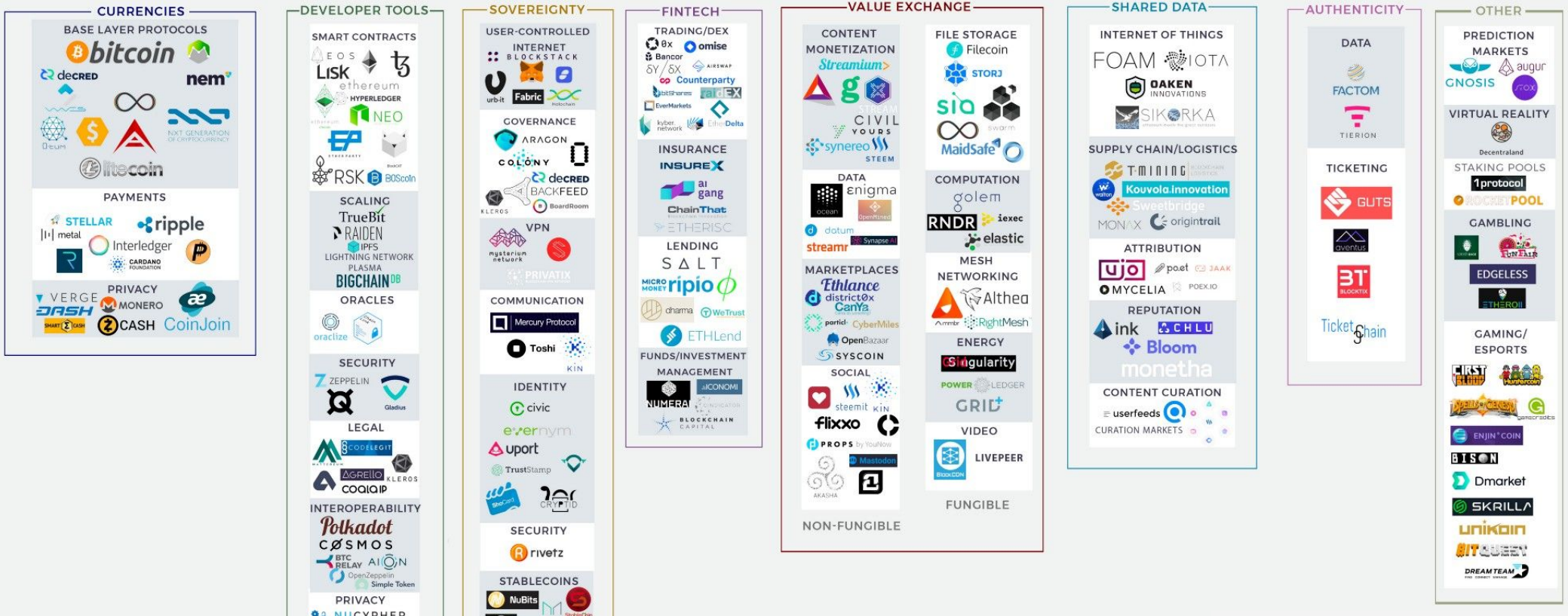
** coinranking.com (April 2018)*

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

Overview: Exciting & Promising Blockchain Projects



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

Blockchain

Examples of Industry Use Cases

FinTech

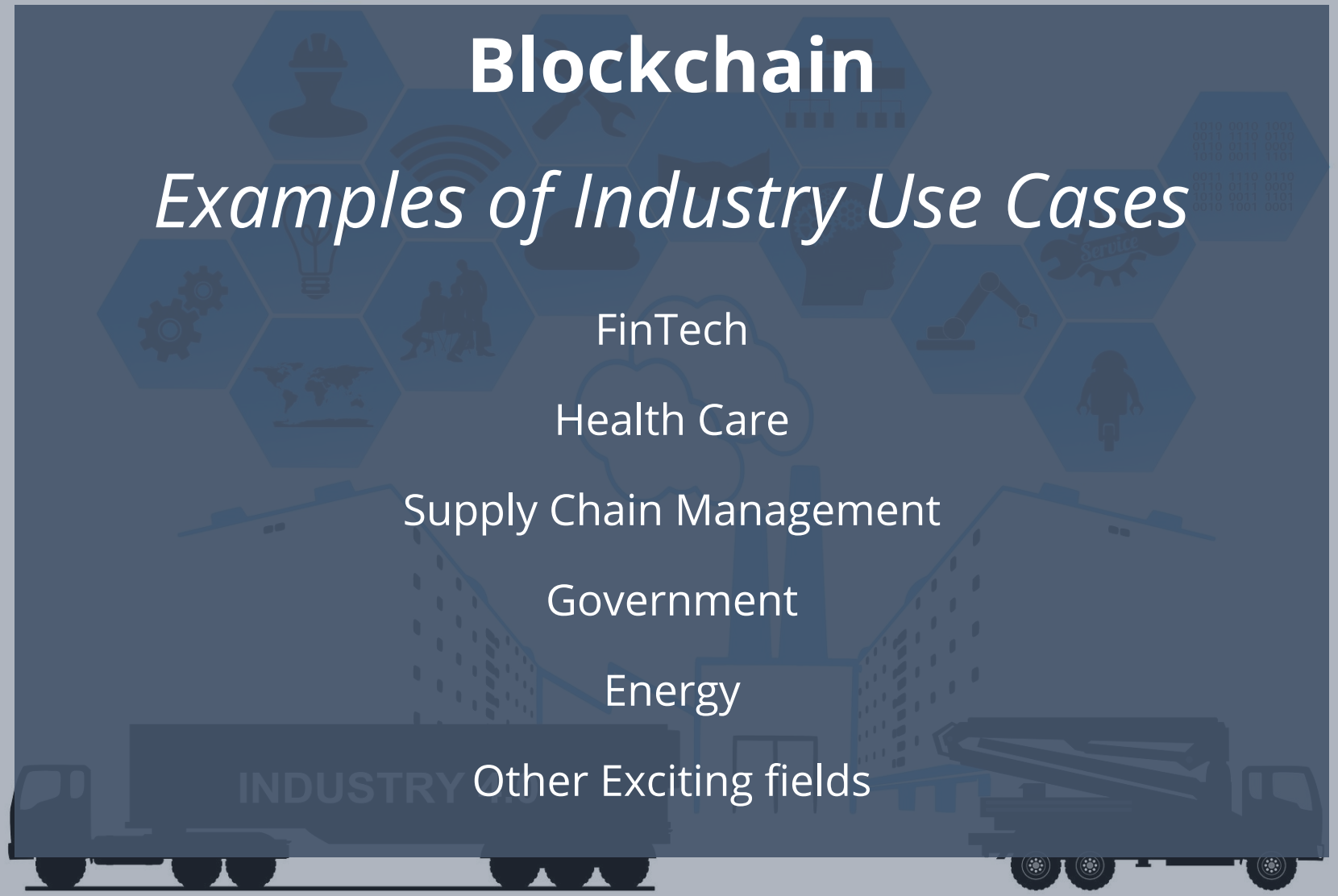
Health Care

Supply Chain Management

Government

Energy

Other Exciting fields



Blockchain Use Cases: **Fintech**

P2P Global Payments, P2P Loans and Financial Inclusion

- **Bank the 2Bn unbanked and 4Bn under-banked**.
- Almost **instant verification and settlement of payments**
- **Improve remittances and prevent corruption for humanitarian aid**
- **Automatic and secure exchange of assets and securities.** 24hr stock exchanges.
- **P2P Loans**

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**

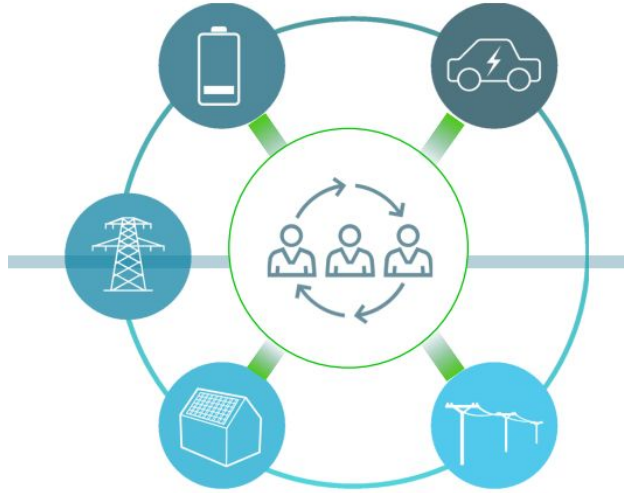
Open Government, Power to the People, Less Corruption

- **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**

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**.

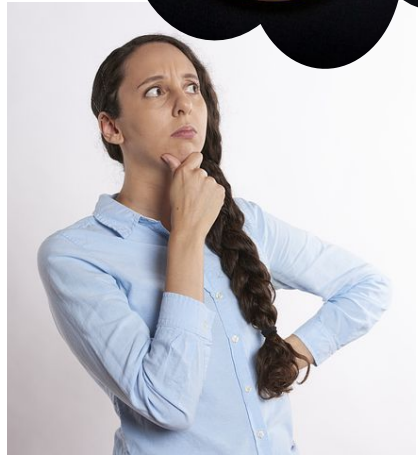


The New Energy Economy

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

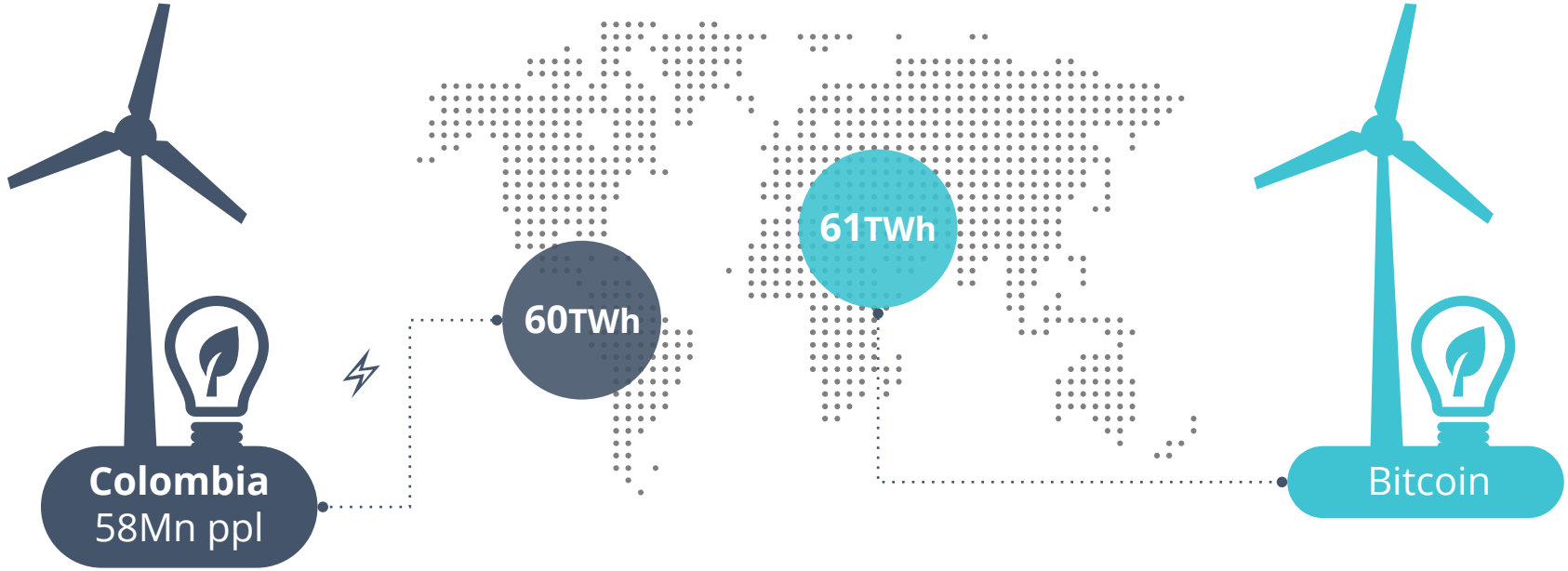
Beyond the Hype: Rational perspective

- **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:** Blockchain tech has the potential for individuals to own their personal data.
- **Financial inclusion:** Today there are 2 billion adults without a bank account.
- **Sharing Economy:** True decentralized services, cut costs of platform owners.
- **Limit Corruption, add transparency**
- **Open-source, free technology, empowering individuals.**

Thanks!

Thanks!

Let's stay connected: 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