Blockchain-X

Blockchain 101

DRAFT VERSION 0.1

Alexander Fred-Ojala
Data-X, SCET, UC Berkeley
afo@berkeley.edu

Berkeley
UNIVERSITY OF CALIFORNIA

Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering

List of Contributors

Alexander Fred-Ojala
Ikhlaq Sidhu

Berkeley
UNIVERSITY OF CALIFORNIA

Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering





OUTLINE

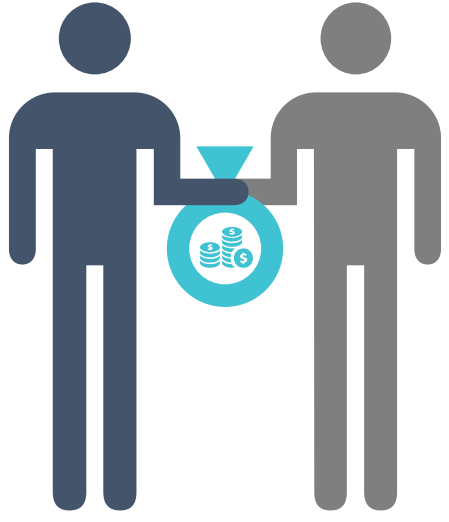
Blockchain 101

1. What is money / banks / bitcoin
2. **Bitcoin: A comprehensive overview**
3. Blockchains, cryptography, hash functions
4. Ethereum / Smart Contracts / Dapps
5. Use cases

First:
QUESTIONS TIME!

What is **Money**?

In order to understand Bitcoin you have to understand money



This is **Money**!

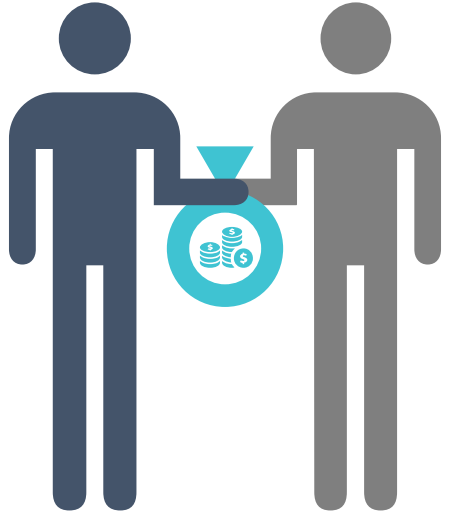
In order to understand Bitcoin you have to understand money

Medium of Exchange

Money exists to facilitate the exchange of *value.*

Requires **Trust**

All parties must trust that the medium of exchange will carry its value.



Scales the Economy

Scales the economy as transactions can be done at greater speeds. You can also split up value into smaller parts (instead of bartering).

Store of **Value**

Money can be accumulated to store value over time. Note this also requires **trust** that the value is sustained.

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**!

In order to understand Bitcoin you have to understand banks

Centralized **Trust Agency**

Regulated by governments. Many people put their trust in them.

Manages **private ledgers**

Banks make sure that your account information is up to date and that it can be audited. Only the banks are able to verify the authenticity of account balances etc.

Identity Management

Links a person to accounts, if the person can show who they are and the bank accepts them as customers.

Offers paid **services**

Banks can offer you loans, investing opportunities, credit cards, mobile apps for transferring and receiving money 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 layer on bartering: Shells, barely, feathers.

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

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

Notes, China, **1200 AD**

Notes and the first fiat-like money system 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 money 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

Network money! Currency as an application!

History of Bitcoin

Blockchain-X
Alexander Fred-Ojala

Bitcoin Whitepaper, **2008**

Satoshi Nakamoto releases Bitcoin in the wake of the financial crisis.

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

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

First Altcoins, **2011**

Namecoin and Litecoin are among the first to fork Bitcoin and create currencies with specific improvements.

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

The bitcoin price falls 87% from one day to another. Largest crash in the currency's history

Mt Gox hack, **2014**

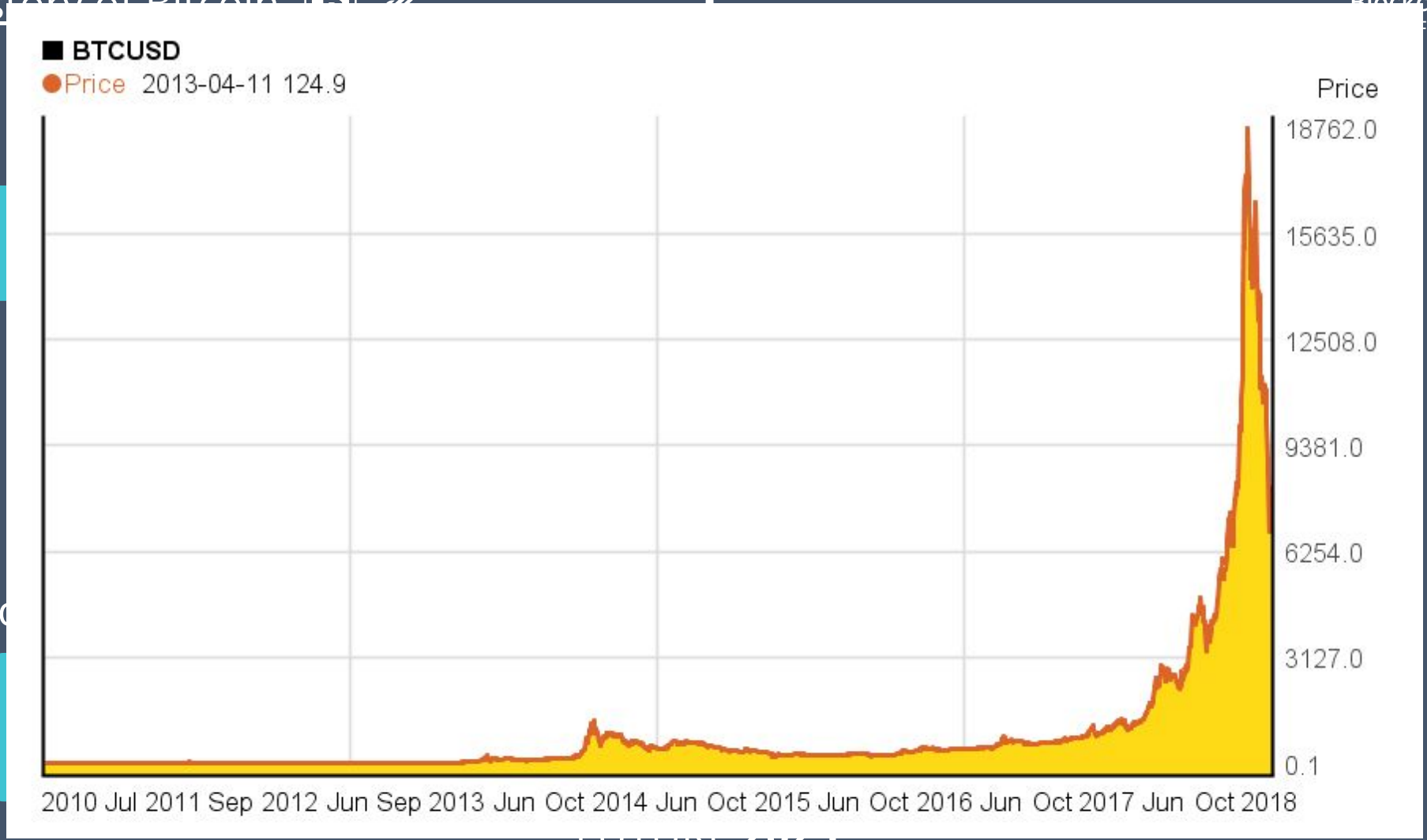
6% of all bitcoin ever created stolen from the largest exchange. $500Mn.

Bitcoin becomes mainstream, **2017**

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**?!

Decentralized **Trust System**

Regulated by a community, where anyone can join and contribute to the system. Trust in the protocols powering the system decided by the community.

Trustless system with **public ledger**

Make sure that your account information is up to date and that it can be audited form any source. Anyone can join this system.

Pseudo-anonymous **Identities**

Anyone can join the network by generating a key that will be used to create and address for a pseudo-anonymous account. The protocol keeps track of owners.

Transfer Money **P2P**

Transactions are carried out between users without any central authority that validates them, person-to-person, without intermedieray. No trusted third party required for transfer of funds.

bitcoin / **Bitcoin**?!

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

  (digital money)

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

  (almost like the infrastructure for a decentralized bank)

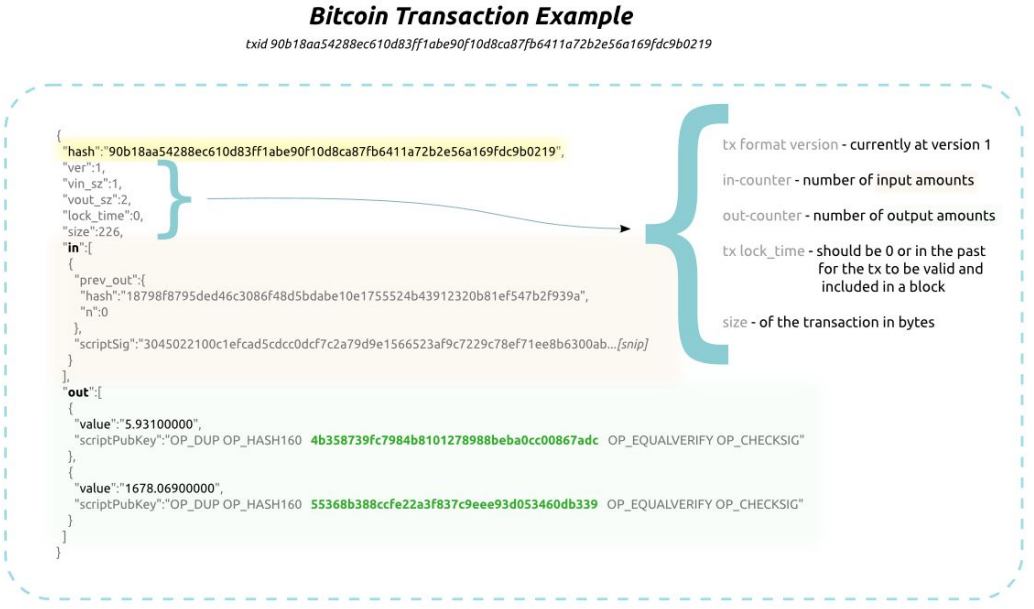
Bitcoin: Digesting the first wiki paragraph!

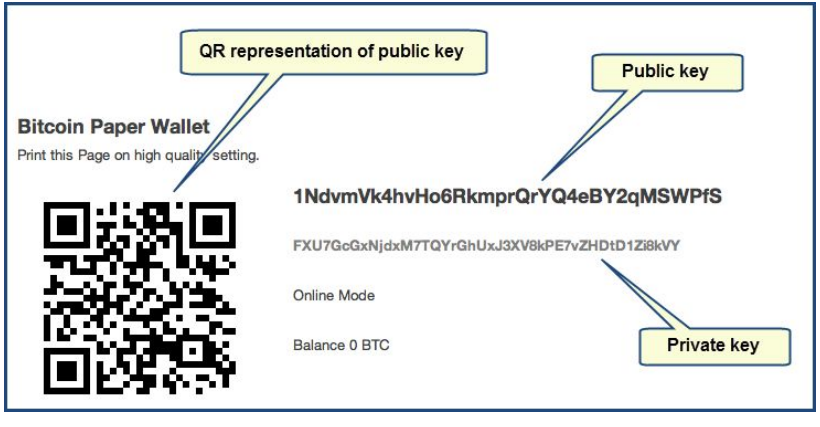
Wiki: *Bitcoin is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and are recorded in a public distributed ledger called a blockchain. Bitcoin was invented by an unknown person or group of people under the pseudonym Satoshi Nakamoto and released as open-source software in 2009. Bitcoins are created as a reward for a process known as mining.*

Bitcoin: Overview

User-perspective:

1. Enables **simple transactions** with a trusted digital currency.
2. Every user creates a **wallet (public / private key chain)** to send and receive transactions. Use private key to sign transactions, use public key to encrypt message. Public key can decrypt, and verify it was you.





Private / Public **Keys**

Bitcoin identity: *Each entity is represented by a unique private - public key pair*

- **Private Key**: Secret. Think of it as a password. You need to keep it safe. If you lose it, it is lost, there is no recovery option. Generated from random processes. Used to sign transactions and prove ownership.
- **Public Key:** External. Think of it as a user name. Generated from the Private key. Elliptic curve cryptography, one way function. Deterministic. Same private key will generate same public key. Your public address for receiving bitcoin.

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 two inputs giving same outputs?)

- **The total address space is 160 bits:**

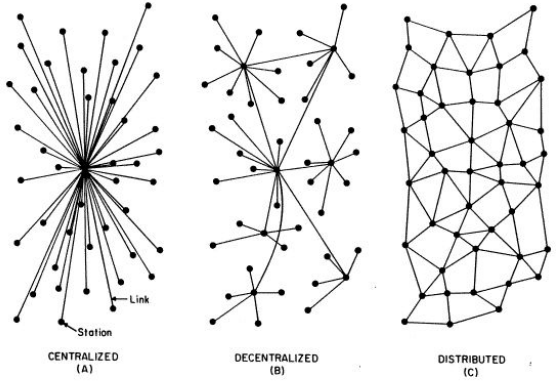
  2^160 = 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976

- There are only 2^63 grains of sand on Earth.
- The total pool of Bitcoin addresses in use is so minuscule compared to the total addresses possible.

Bitcoin: Overview

System perspective:

- Anyone can join and maintain the system / ledger **(trustless)**.
- Every node keeps copy of the ledger and updates it with valid, signed transactions according to **consensus** rules.
- Ledgers exist all over the world **(distributed database)**, users connect to them (decentralized). No single company or government can control it.



Bitcoin: How can we trust the ledger?

Build trust:

1. Traffic delays and fraud attempts -> **Different recent entries.** Every node needs to cast a **vote** on a valid block.
2. To prevent **Sybil attack** (creation of many identities), need to **spend / stake resources to validate ledger entries**. An attacker must outspend the majority.
3. Need to **solve cryptographic puzzle** to confirm a new entry / block in the ledger.
4. Each **puzzle builds on previous answers**, and the winner is not only the most recent solutions, but the blockchain with the most solutions linked together. **The longest chain is the most valid one** (more nodes are working on it).
5. *Repeat*

Bitcoin: Incentivize

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 money.
   Deflationary. After 2140 no new bitcoin.

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

Bitcoin: Intro

Summary:

1. Bitcoin is a **collaborative ledger.**
2. People spend money by sending **signed messages** to nodes describing where and how much money should move. Nodes make sure that they are true by checking signature.
3. **Math based voting process to ensure legitimate transactions.**

Key benefits, bitcoin provides:

4. **Identity:** Share public key to transfer bitcoin and use private key to redeem.
5. **Transactions:** UTXO, balance of all unspent transactions
6. **Record keeping:** Each entity keeps a copy of the blockchain
7. **Consensus:** Peers can cast expensive votes via Proof-of-Work

User owned and managed

Bitcoin: Intro

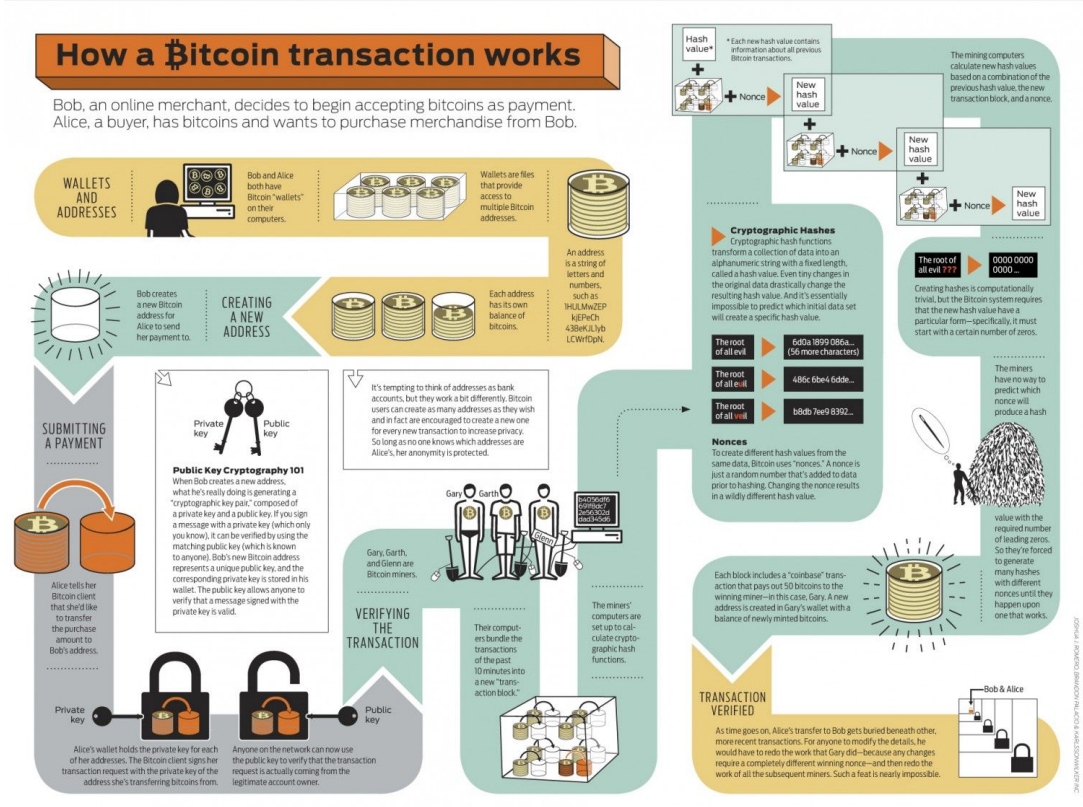
Fulfills characteristics of a currency

1. **Scarcity:** Finite units. Deflationary BTC. 21Mn in total. Mining reward halved every X years.
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:** We can trust the Bitcoin protocol, it has not been hacked for years

User owned and managed

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

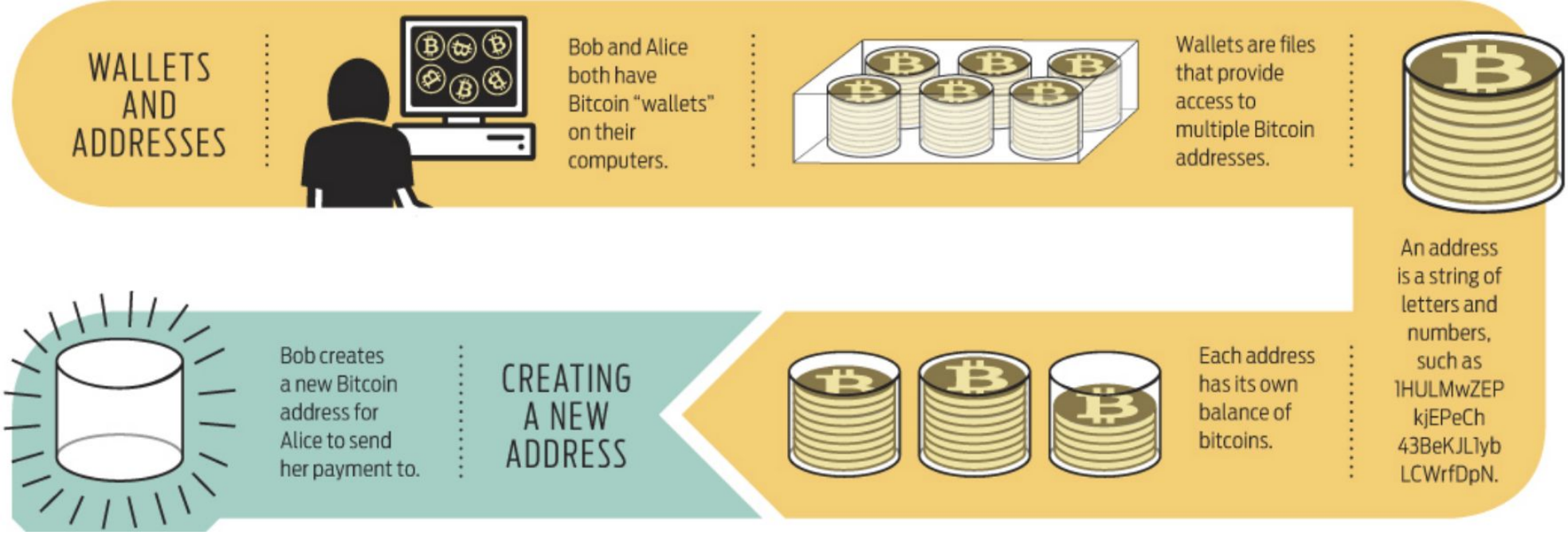
Bitcoin: System Overview



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.

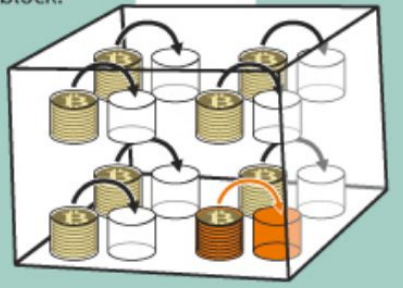
Public key

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."



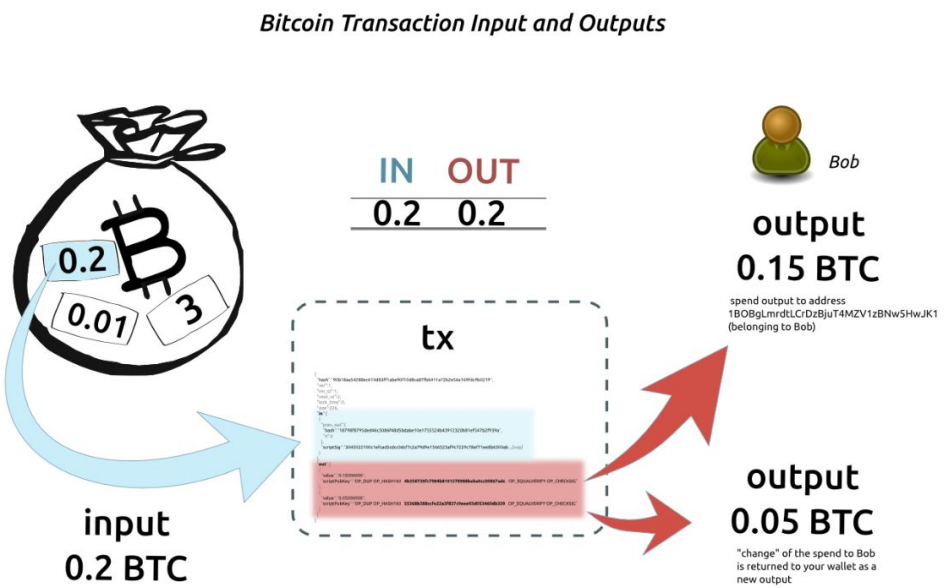
The miners' computers are set up to calculate cryptographic hash functions.

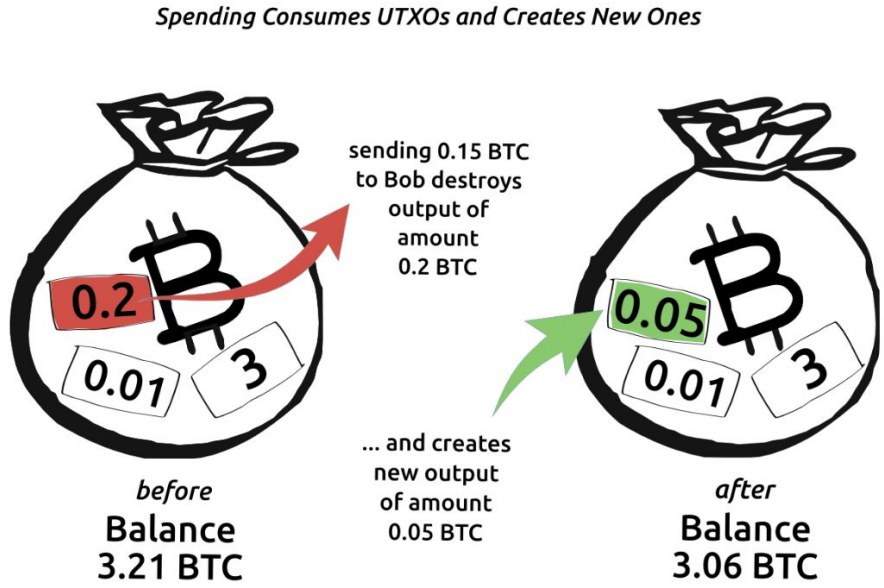
Bitcoin Transactions: The UTXO model

Unspent Transaction Outputs (UTXOs) as a model for available balances and transactions.

Transactions destroy original UTXO(s) and creates two new outputs: receiver and change back to our wallet.

Account balance is achieved by adding up UTXO. Private key redeems UTXO. Wallet tracks UTXOs.





Source: ccn.com/bitcoin-transaction-really-works/

What makes a transaction valid?

- **You have the balance in your account** (available funds)
- Insuring that the **funds have not be used in any other transaction.**
- **Proof of ownership** (signature)

Money:

You have it in the pocket

You cannot clone dollar bill

You are the one with the dollar.

Cryptocurrency:

Your public address have received UTXO

All previous UTXO used have been destroyed

You have the private key to sign transactions

Bitcoin: System Overview (3/4)

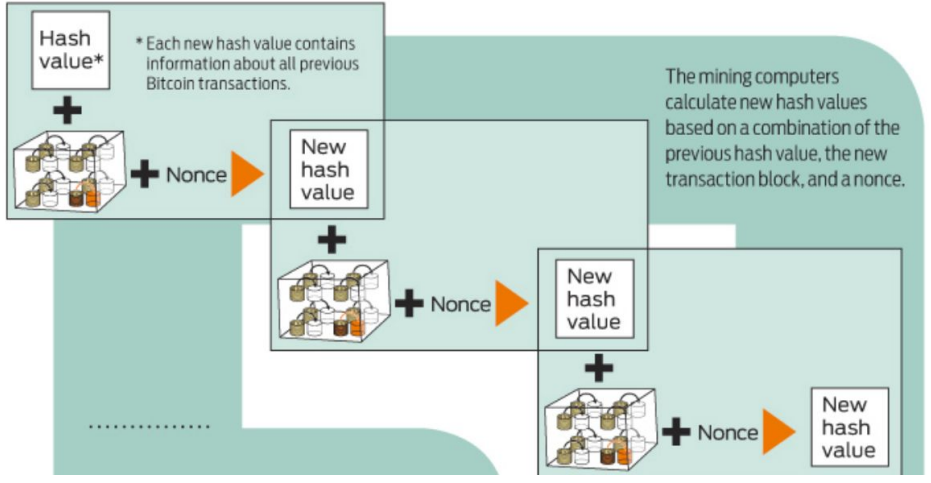
Cryptographic Hashes

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...

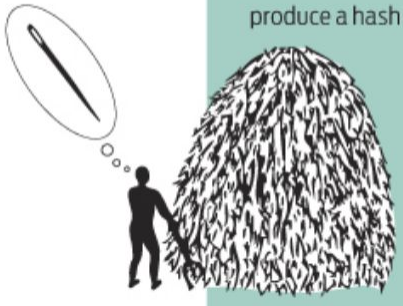
Nonces

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

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

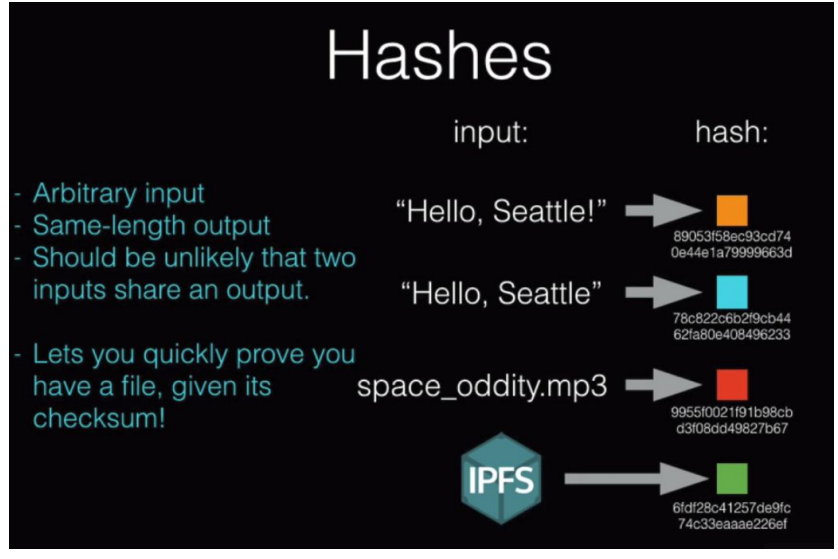
The same input will always create the same output.

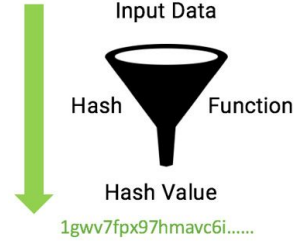
Given output y we cannot recreate input x

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

Used for **proving that something is the same as something else, 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.



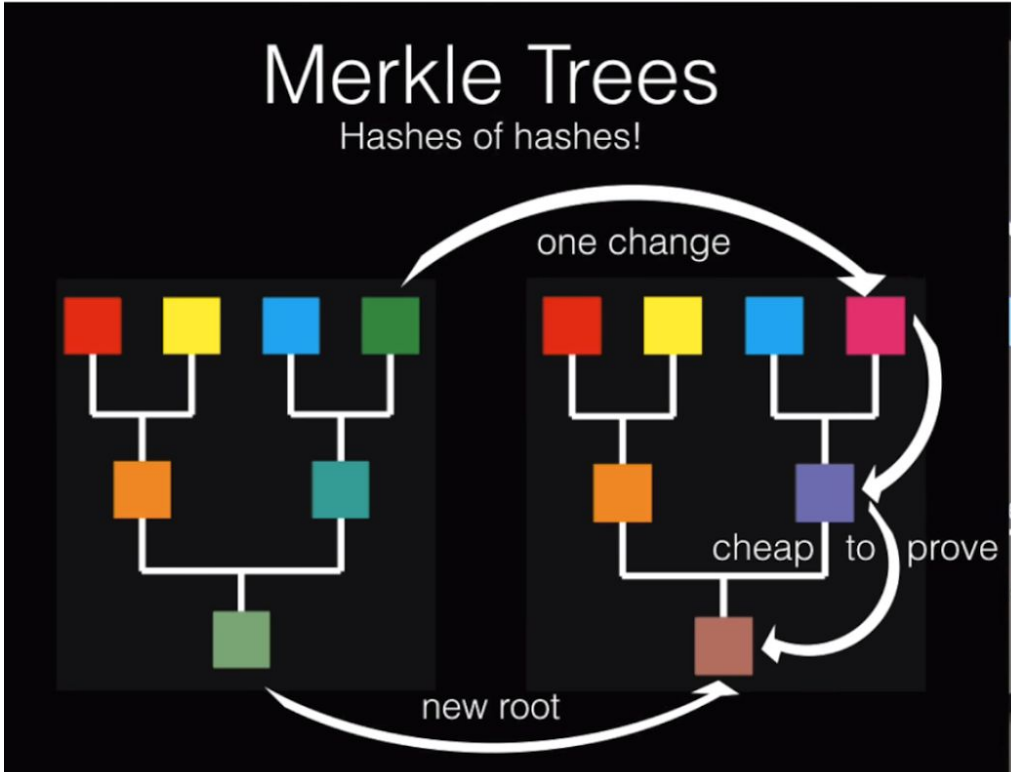


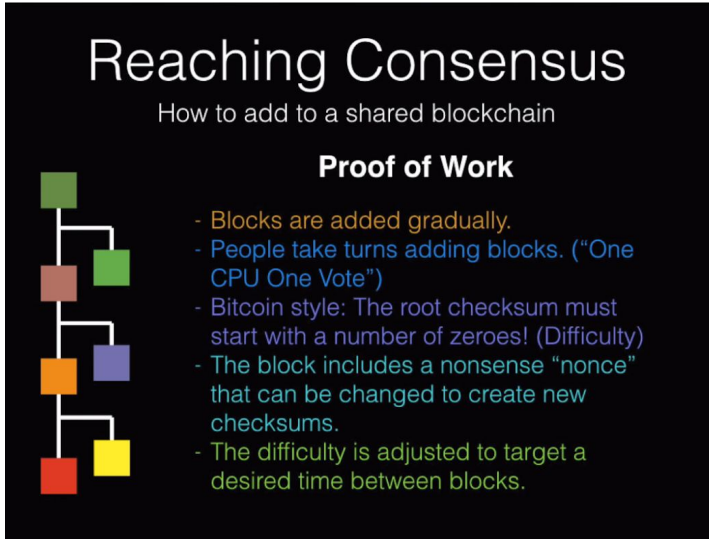
$$md5(\text{"}hello\ world\text{"}) = 5eb63bbbe01eeed093cb22bb8f5acdc3$$

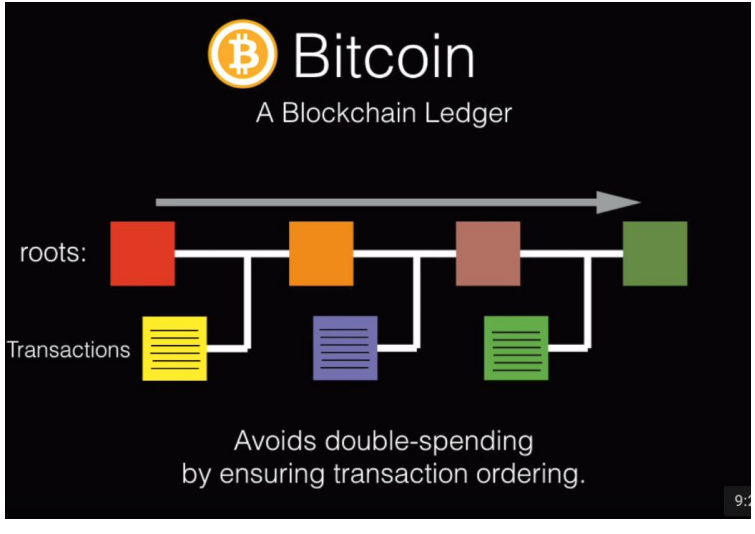
Source: https://www.youtube.com/watch?v=-SMliFtoPn8

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

Blockchain: Merkle Trees

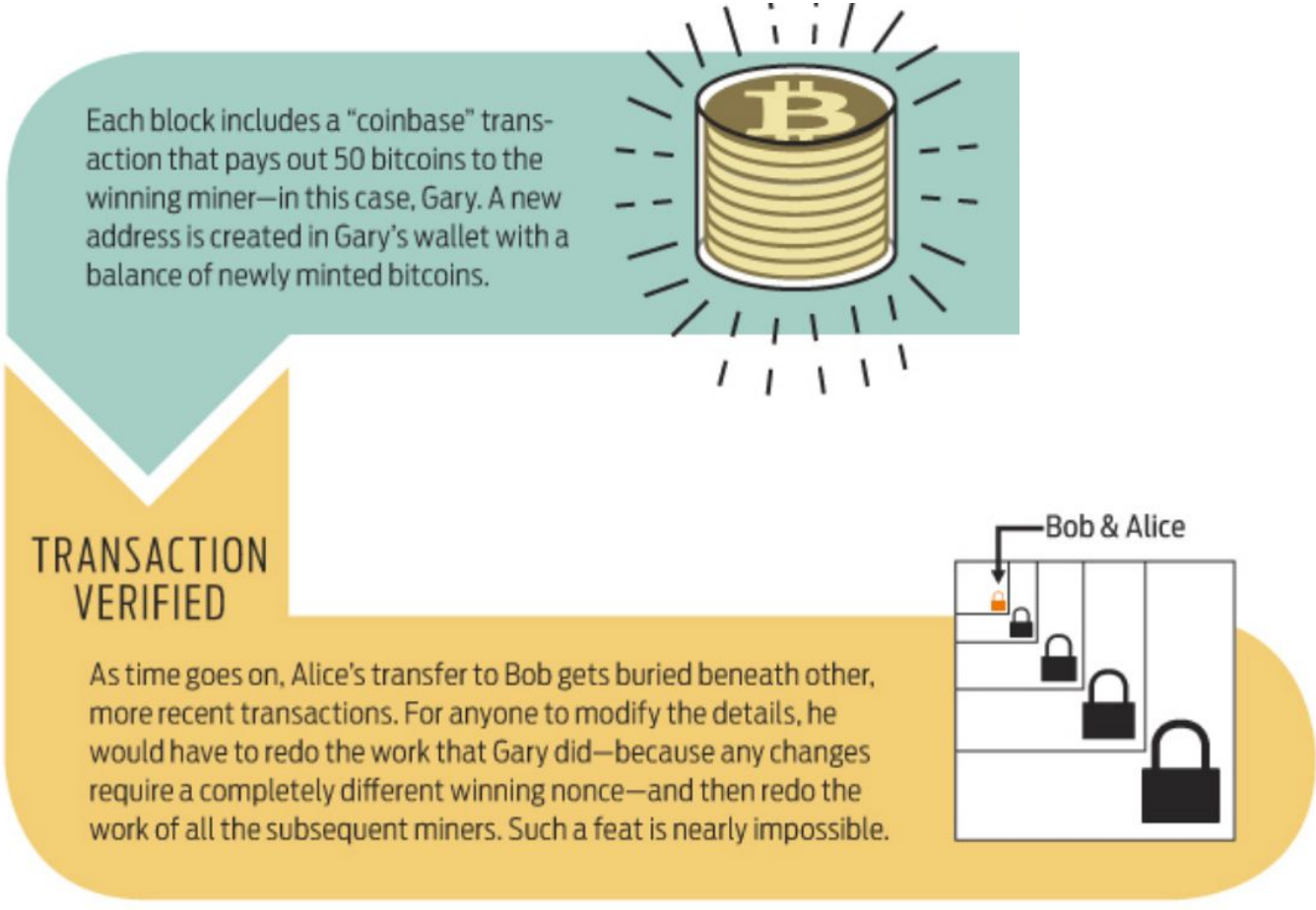






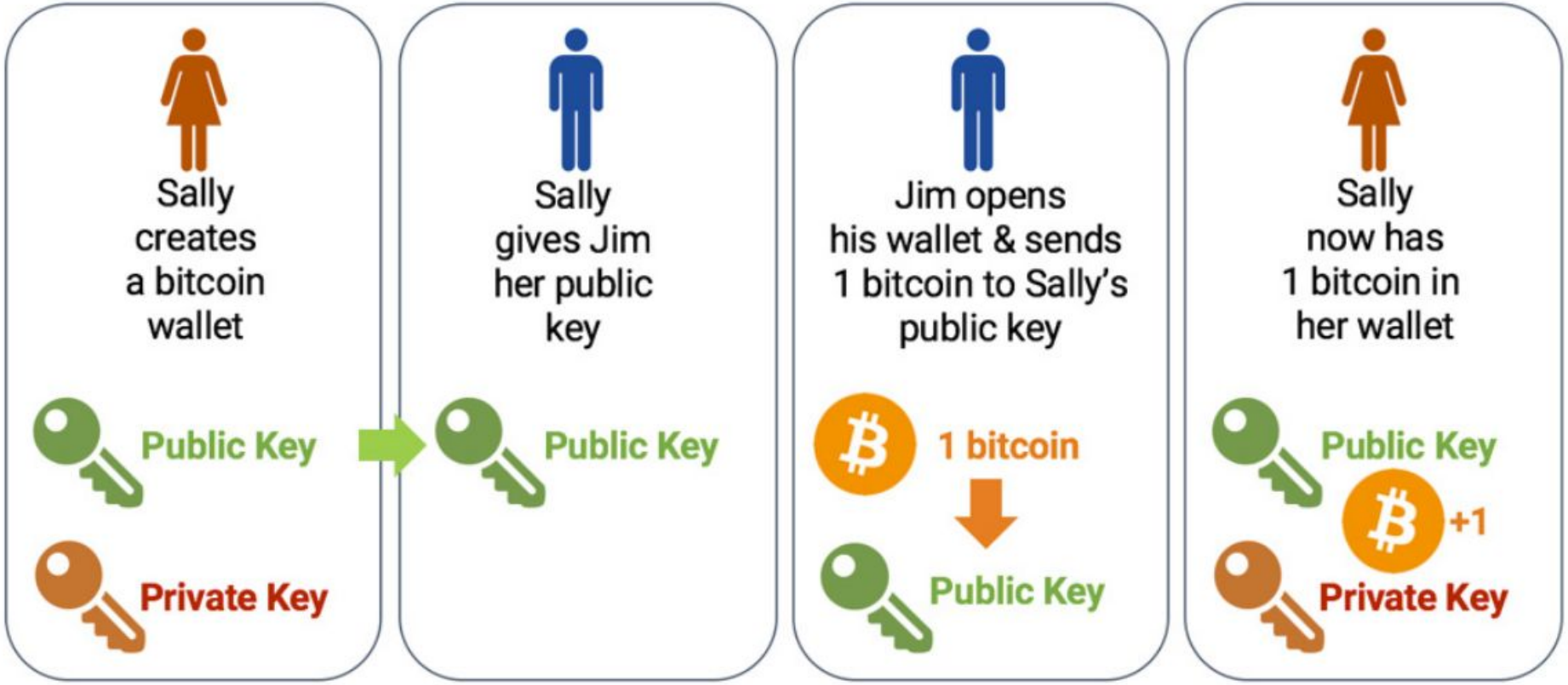
Source: https://www.youtube.com/watch?v=-SMliFtoPn8

Bitcoin: System Overview (4/4)



Source: IEEE Spectrum

Bitcoin: Transaction, summary



Source: stansberrychurchouse.com

Goal of the Bitcoin Blockchain: Trust

Anonymous: Decentralized system, anyone can join without screening.

Decentralized: You have to destroy every node to destroy the network.

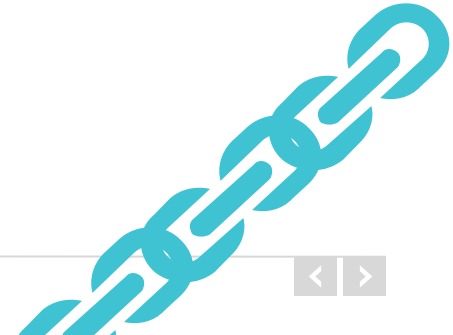
Immutable: Every transaction is recorded and linked together sequentially. Cannot be changed / deleted.

Trustless: You can trust that every obey to the protocol because of incentive structures.

Consensus: Validity of a new block is determined by the network. Enables open network where everyone can join, but we are still able to maintain honesty and integrity of the network!!

Global: Not discriminatory against anyone. As long you have a computer, internet access and resources you can participate in the Bitcoin network. Financial inclusion!

Trust in code.



Consensus Problems **Concentration of Power**

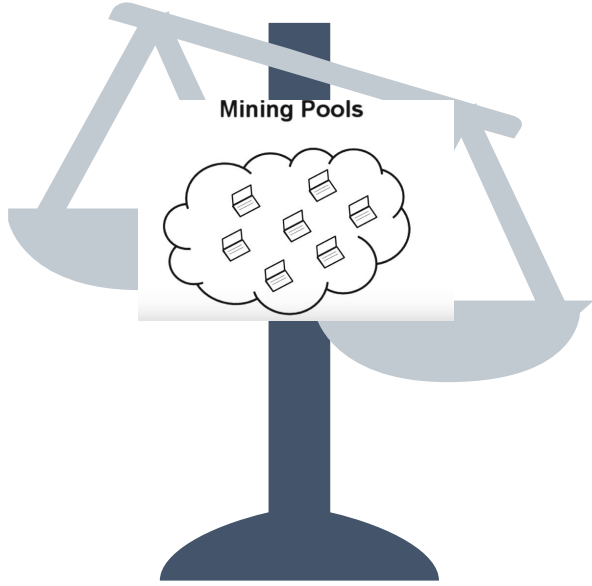
A lot of nuances of the Blockchain ecosystem and technology lead to the concentration of power and that different market actors gain advantages.

ASIC Hardware

Special hardware optimized for Proof of Work leads to

Majority attack

51% of the computing power can result in faulty transactions being posted to the Blockchain



Mining Pools

Consortiums of miners split the reward. Lead to concentration of power.

Owenshership

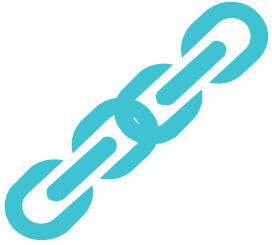
96%: amount of bitcoin owned by just 4% of addresses (containing 2.9 million BTC).

Blockchain: Record Keeping

Keeps track of everything that has happened in Bitcoin since the Genesis block 2008

Normally a centralized system keeps track of everything, and one server will confirm validity.

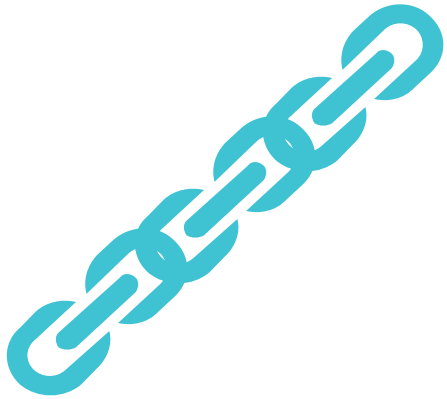
- Every node carries out transaction. **No central point of failure,** gets around the honey pot problem.
- **By including the hash of the previous block the ledger becomes immutable,** because it is cryptographically secured (by adding hash of every block after the other).



Blockchain **Novelties**

Byzantine Fault Tolerant Distributed Computer System

A fundamental problem in distributed computing and multi-agent systems is to achieve overall system reliability in the presence of a number of faulty processes. This often requires processes to agree on some data value that is needed during computation. Handled by Bitcoin.



Solution to the **Double-spend problem**

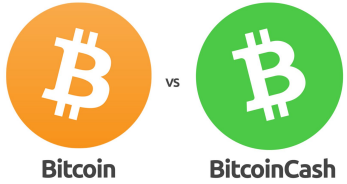
Bitcoin is a was the first digital money system to solve the double spend problem by utilizing the proof-of-work algorithm to verify transactions.

Blockchain **Terminology**

Forking Updating the protocol

A soft fork (backward compatible, previously valid blocks are made invalid) in the protocol is when there is a minor update to the protocol.

A hard fork (not backward compatible, previously valid blocks invalid or vice versa) is when there is a major update to the protocol, and two sides disagree. Can result in a split between the chains.



Forking to the longest chain

When **two votes for a new block are cast at the same time.** Both are valid for a while, but eventually one will have a new block on top, all miners will abandon the shorter chain, and start mining on the longer one.

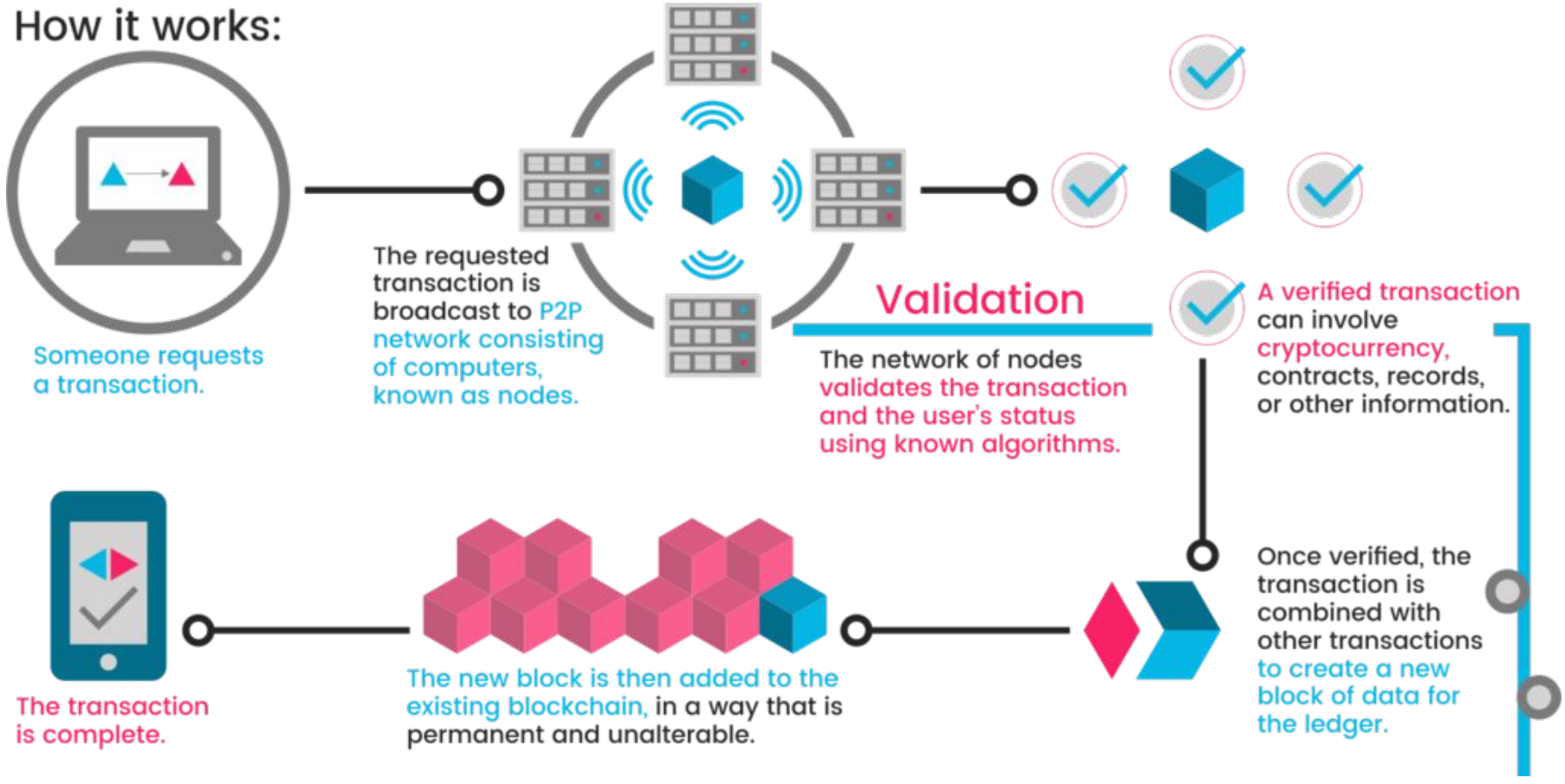
This is a rule built into the protocol. It is as if that block has never happened.

Blockchain **Terminology**

51% attack

- Everything relies on an **honest majority assumption**
- A malicious majority can control the network.
- There was a mining pool that almost had 51% in 2013 of the computing resources. A majority decides the truth. 6 blocks in a row. Wait for more than 6 confirmations.
- Enables opportunity to send transaction to oneself.
- A majority of the computing power, then you can always vote on the longest chain. Can fork from everyone else and say this is chain is the longest and valid.

Blockchain 101: **How it works**



Post-Bitcoin

- **Distributed network:** Bitcoin was one of the first to combine:
  - **Cryptographic identities:** Public / Private. Reveal nothing about yourself. Prove claim ownership of assets. Responsible for actions.
  - **Consensus protocol:** Nakamoto consensus. Tie voting power to a specific external resource (computing power, resources). Democratic decision.
  - **Blockchain:** Immutable source of truth, ledger we can add to but not change later. Append only. Cannot change. No central point of failure.

Smart Contracts

Contract definition:

- Agreement with another party.
- Some entity to enforce the contract and the terms (can be violated)

Smart Contract (Nick Szabo, 1996):

- Define terms of agreement in programmatic code.
- Code that facilitates, verifies, or enforces the negotiation / execution of a digital contract.
  - Need trusted entity to run this code. So that we can verify that the output we get is what we intend it to be.


ethereum
HOMESTEAD RELEASE
BLOCKCHAIN APP PLATFORM

Enter Ethereum

- **Blockchain Smart Contract Platform:** Take away idea of trusted entity needed to run smart contract, replace with trustless distributed network we get from Bitcoin.
- **Distributed Computer / Decentralized platform to run smart contracts**
- **The total network has a state**, not just transactions
- Distributed state machine - transactions change global state (did I send email, vote etc?)
  - transactions == state transaction function
- **Native asset called ether (ETH)**
  - Basis of value in Ethereum ecosystem
  - Needed to align incentives, and reward miners.
- Turing complete Ethereum Virtual machine that can run any code

Smart Contracts on Ethereum

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce a contract. Smart contracts allow the performance of credible transactions without third parties.

- Stored as code on the Blockchain and evaluated by all nodes.

  Like transactions without recipient. Ethereum Virtual Machine
- Transparent, distributed, and decentralized agreement
- Smart Contracts can call other Smart Contracts
- Requires *gas* to run (to prevent DDOS)

ICO: Initial Coin Offering

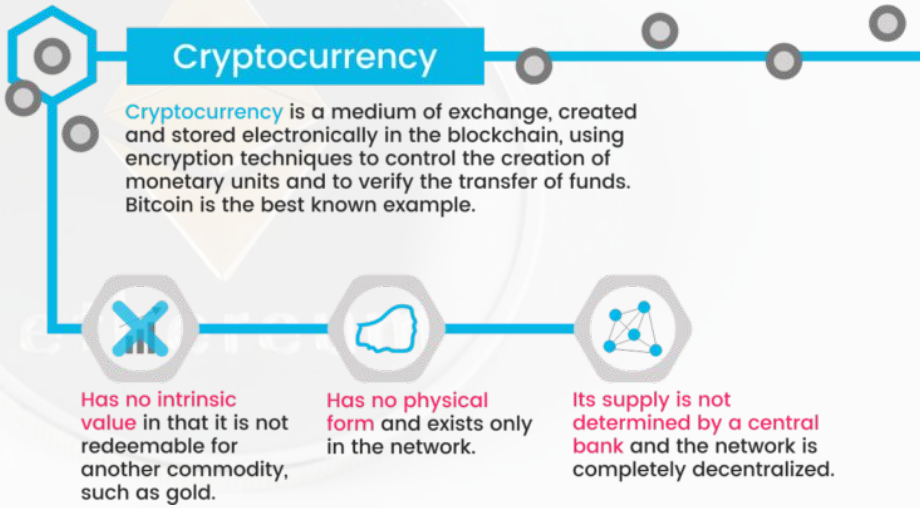
- *The introduction of a new cryptocurrency / token*
- Can either be a security or a utility token
- Incentivizes a community to buy into the idea -> Scale factors and network effects.

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

** coinranking.com (April 2018)*

Altcoins / Cryptocurrency / Tokens

- *Digital currency, medium of exchange* and store of value
- Independent of Central bank
- Utility token or security
- Application-centric or general
- Based on new or existing blockchain



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 for access.
- **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

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 etc.

- **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, to cut costs of middle men. True Airbnb, Uber

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

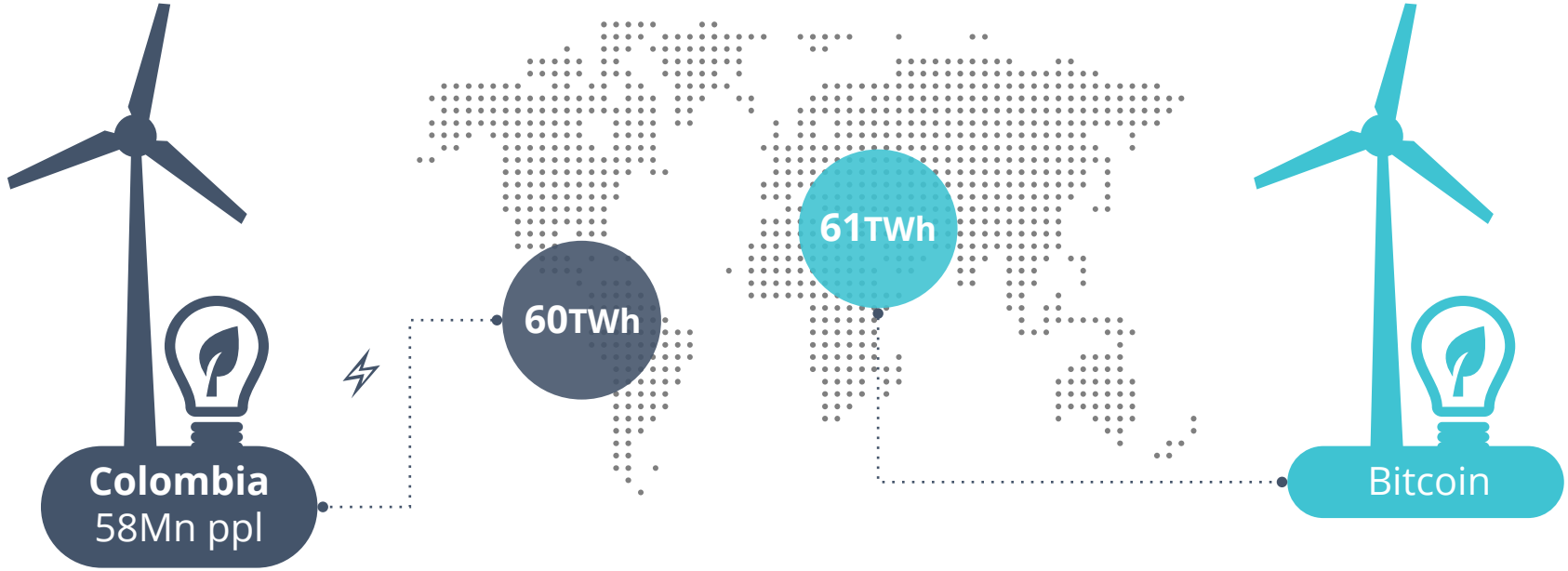
4. Blockchain **Disk Space**

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)

Comparison of Annual **Energy Problem**

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

Ethereum **Development Frameworks**

geth

geth is the the command line interface for running a full Ethereum node implemented in Go. By installing and running geth , you can take part in the Ethereum live network and. mine real ether; transfer funds between addresses; create contracts etc.

etherchain.org

etherchain.org

Etherchain is an Explorer for the Ethereum blockchain. It allows you to view account balances, look up transactions and explore smart contracts.

Ethereum Development Tools: **dApp Browsers**

Mist

Browser that can interact with dApps. Full client that downloads a full node of the Etheruem Blockchain.

Metamask

Browser extension for interacting with the Ethereum blockchain. Only contians keys to sign transactions.

Parity

Modern Ethereum client to interact with the Ethereum blockchain.

Ethereum **Development Frameworks**

Solidity

Programming language designed for developing smart contracts on the Ethereum Blockchain. The language is similar to Javascript and it is compiled down to bytecode to run on the Ethereum Virtual Machine (EVM).

Truffle Framework

Ethereum Swiss Army knife, contains a lot of development tools. Development environment, testing framework and asset pipeline for Ethereum. Smart contract compilation, Automated contract testing with Mocha and Chai etc.

Remix-IDE

Remix is a browser-based compiler and IDE that enables users to build Ethereum contracts with Solidity language and to debug transactions.

Other **Useful Resources**

CoinMarketCap

Top 100 Cryptocurrencies by Market Capitalization. The go to website for Cryptocurrency market cap rankings, averaged exchange rates, charts etc.

bitcoin.org

Wonderfully informative “Official” bitcoin website, with plenty of tutorials etc.

Popular application to buy cryptocurrency for fiat currency. Also has an exchange related to it called GDAX. Bought Earn.com yesterday.

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