Blockchain Technologies for Data Scientists

Bruno Gonçalves

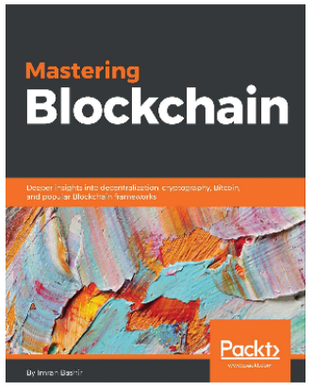
www.data4sci.com

https://github.com/DataForScience/blockchain-data

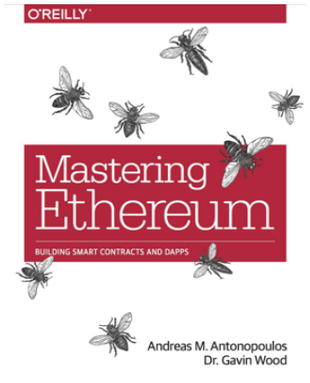
Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of my employers. The examples provided with this tutorial were chosen for their didactic value and are not mean to be representative of my day to day work.

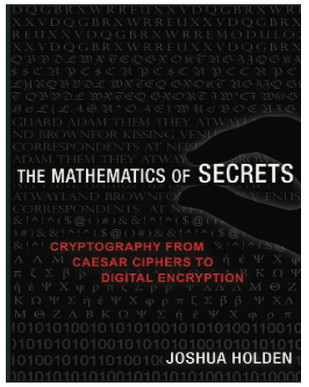
References

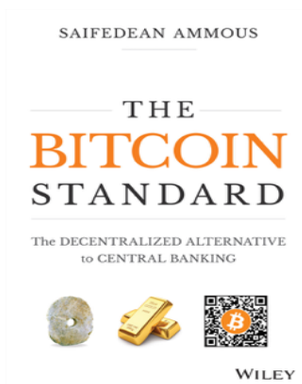

Mastering
Blockchain
Packt

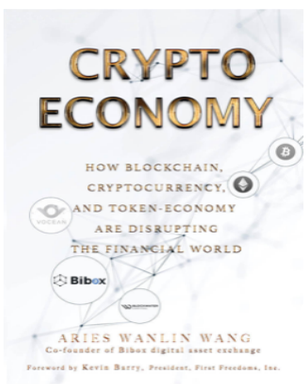

O'REILLY
2nd Edition
Mastering
Bitcoin
PROGRAMMING THE OPEN BLOCKCHAIN
Andreas M. Antonopoulos

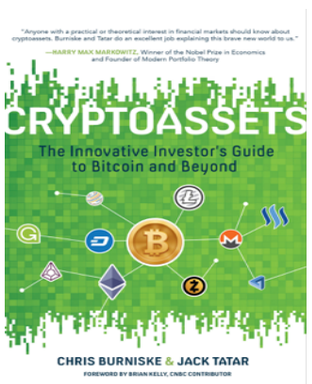

O'REILLY
Mastering
Ethereum
BUILDING SMART CONTRACTS AND DAPPS
Andreas M. Antonopoulos
Dr. Gavin Wood

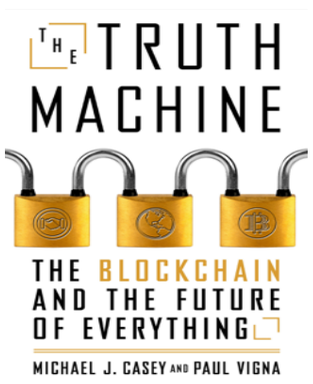

O'REILLY
Blockchain
BLUEPRINT FOR A NEW ECONOMY
Melanie Swan

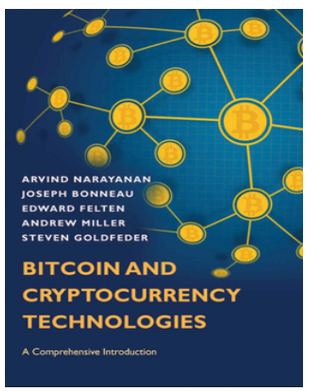

THE MATHEMATICS OF SECRETS
CRYPTOGRAPHY FROM
CAESAR CIPHERS TO
DIGITAL ENCRYPTION
JOSHUA HOLDEN


SAIFEDEAN AMMOUS
THE
BITCOIN
STANDARD
The DECENTRALIZED ALTERNATIVE
to CENTRAL BANKING
WILEY


CRYPTO
ECONOMY
HOW BLOCKCHAIN,
CRYPTOCURRENCY,
AND TOKEN-ECONOMY
ARE DISRUPTING
THE FINANCIAL WORLD
Bibox
ARIES WANLIN WANG


CRYPTOASSETS
The Innovative Investor's Guide
to Bitcoin and Beyond
CHRIS BURNISKE & JACK TATAR


THE TRUTH
MACHINE
THE BLOCKCHAIN
AND THE FUTURE
OF EVERYTHING
MICHAEL J. CASEY AND PAUL VIGNA


ARVIND NARAYANAN
JOSEPH BONNEAU
EDWARD FELTEN
ANDREW MILLER
STEVEN GOLDFEDER
BITCOIN AND
CRYPTOCURRENCY
TECHNOLOGIES
A Comprehensive Introduction

How Money Works

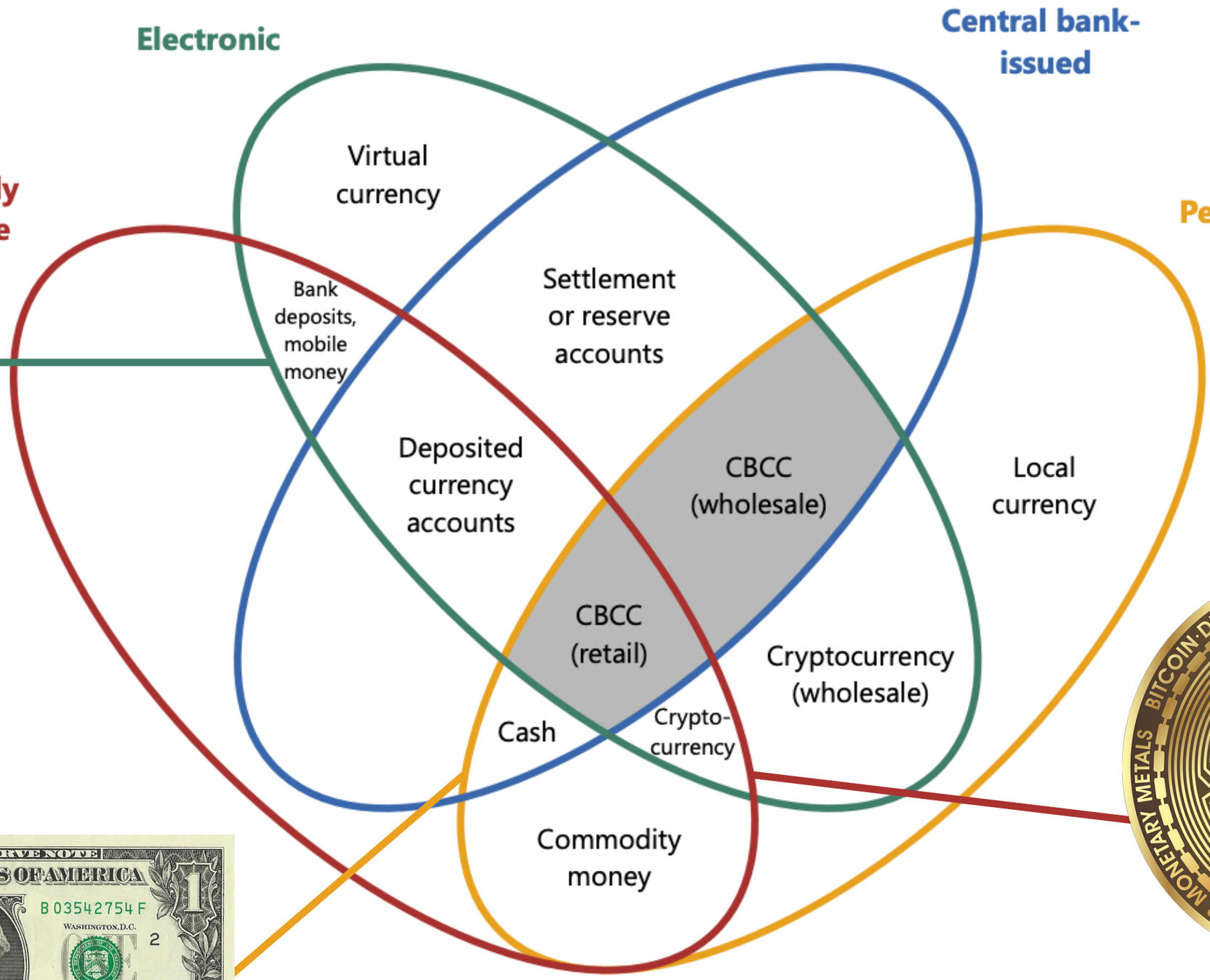
https://www.continentalcurrency.ca/wp-content/uploads/2015/06/continental-currency-exchange.jpg
https://upload.wikimedia.org/wikipedia/commons/2/2b/Olaus_Magnus_-_On_Trade_Without_Using_Money.jpg

- Many different types of currency have been used throughout the years
  - Gold
  - Cattle
  - Salt
  - Rocks
  - Sea Shells
  - etc…

- Fundamental functions (and properties) of money:
  - Medium of Exchange (Fungibility, Portability)
  - Unit of Account (Cognizability)
  - Store of Value (Durability, Stability of Value / Scarcity)

Money Flower

https://www.bis.org/publ/qtrpdf/r_qt1709.pdf
https://upload.wikimedia.org/wikipedia/commons/2/23/US_one_dollar_bill%2C_obverse%2C_series_2009.jpg
https://upload.wikimedia.org/wikipedia/commons/thumb/d/d3/49024-SOS-ATM.JPG/1600px-49024-SOS-ATM.JPG
https://pixabay.com/p-3125488/?no_redirect



www.data4sci.com

The Ingredients of a Crypto-Currency

https://pixabay.com/photos/bank-money-finance-shares-save-2907728/

- Fundamental functions (and properties) of money:
  - Medium of Exchange (Fungibility, Portability)
  - Unit of Account (Cognizability)
  - Store of Value (Durability, Stability of Value / Scarcity)
- Digital currencies have obvious advantages:
  - Fungibility - A bit is a bit
  - Portability - We can easily cary terabytes in our pockets or digitally transfer them across the world
  - Cognizability - It's just a number
  - Durability - Information can easily be stored for decades or even centuries
- And obvious problems:
  - Stability of Value / Scarcity
    - There is no limit to how many you can create
    - They can be easily duplicated (no trust)
    - etc…

The Ingredients of a Crypto-Currency

https://pixabay.com/photos/bank-money-finance-shares-save-2907728/

https://news.bitcoin.com/10-years-ago-bitcoins-genesis-block-changed-the-course-of-history/

- How to avoid the need for a centralized authority?
  - Distributed Ledger
- How to avoid double spending?
  - Consensus algorithm
- How to prevent cheaters?
  - Reward miners for being honest


THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Salman Rushdie I won't marry again

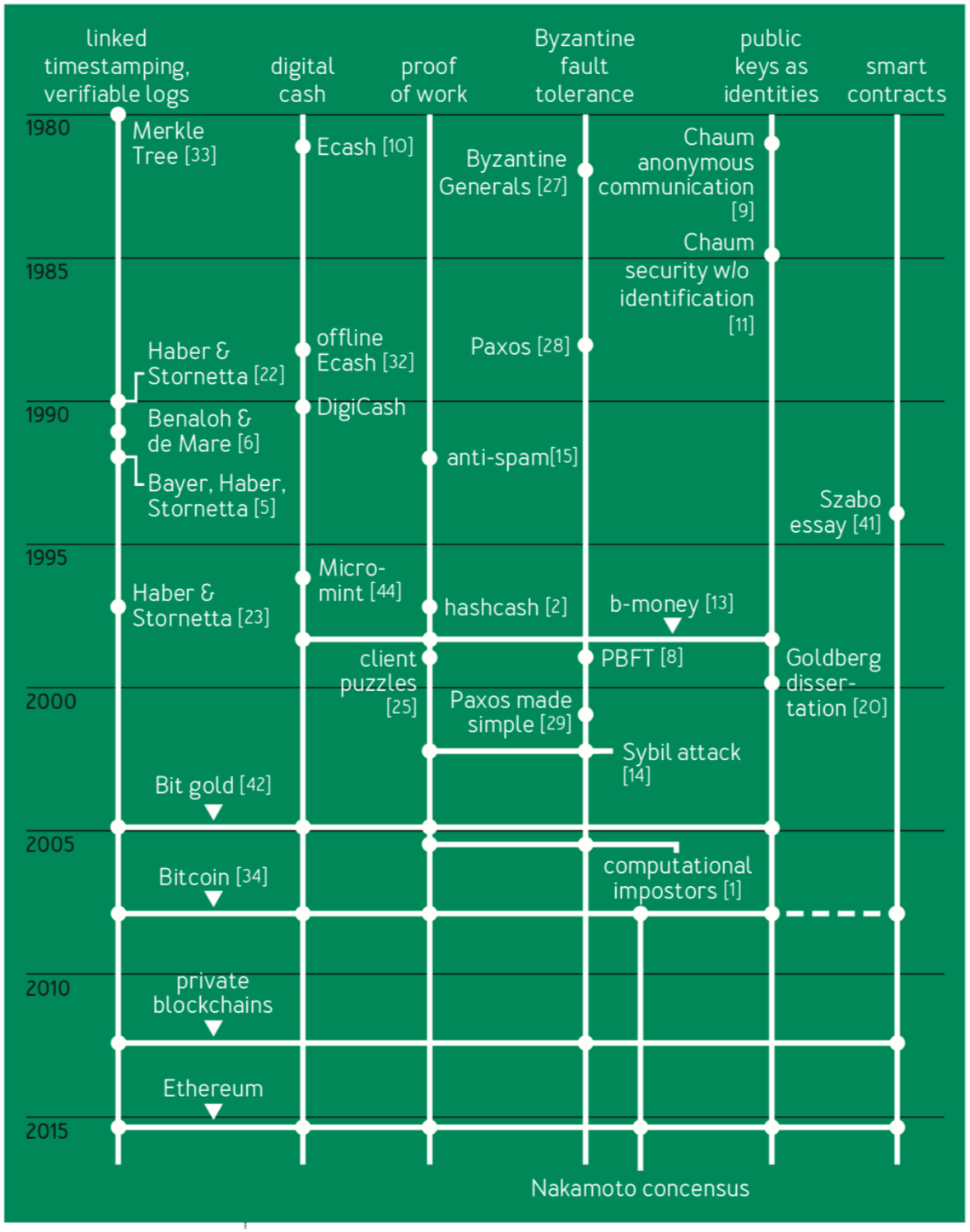
Giant killing? Guide to the FA Cup third round

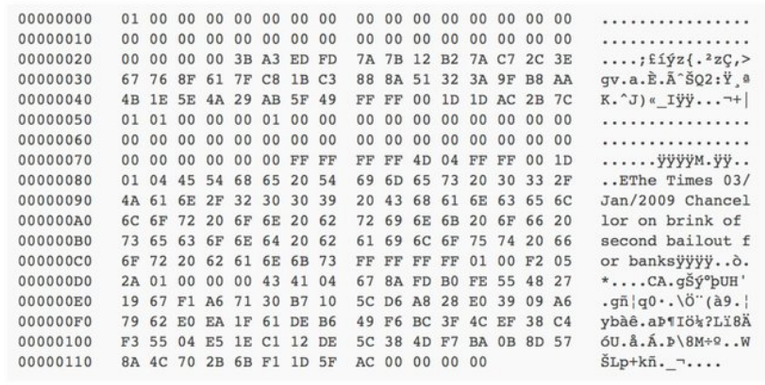
99p

@bgoncalves

The road to Bitcoin

https://queue.acm.org/detail.cfm?id=3136559






THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

@bgoncalves

How does it work?

https://bitcoin.org/bitcoin.pdf

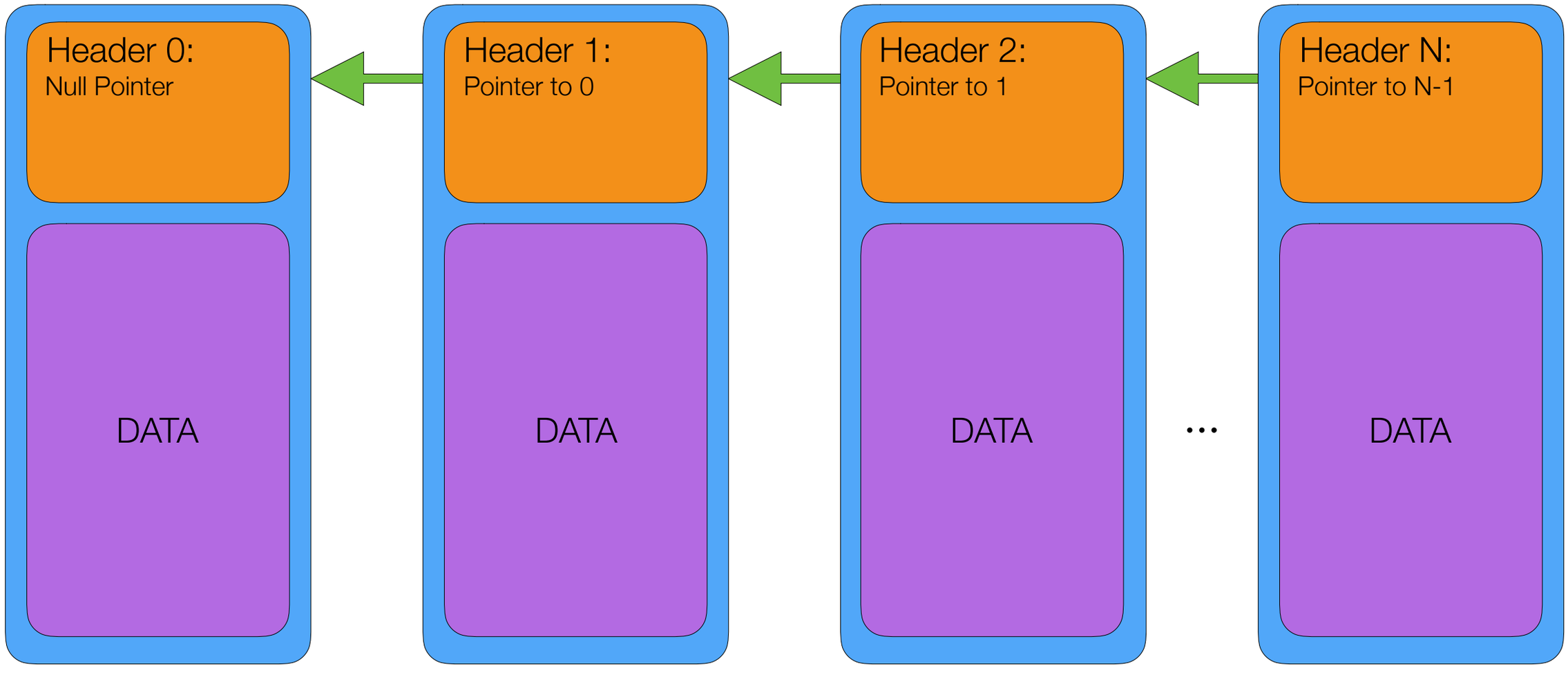
- According to "Satoshi Nakamoto":

The steps to run the network are as follows:

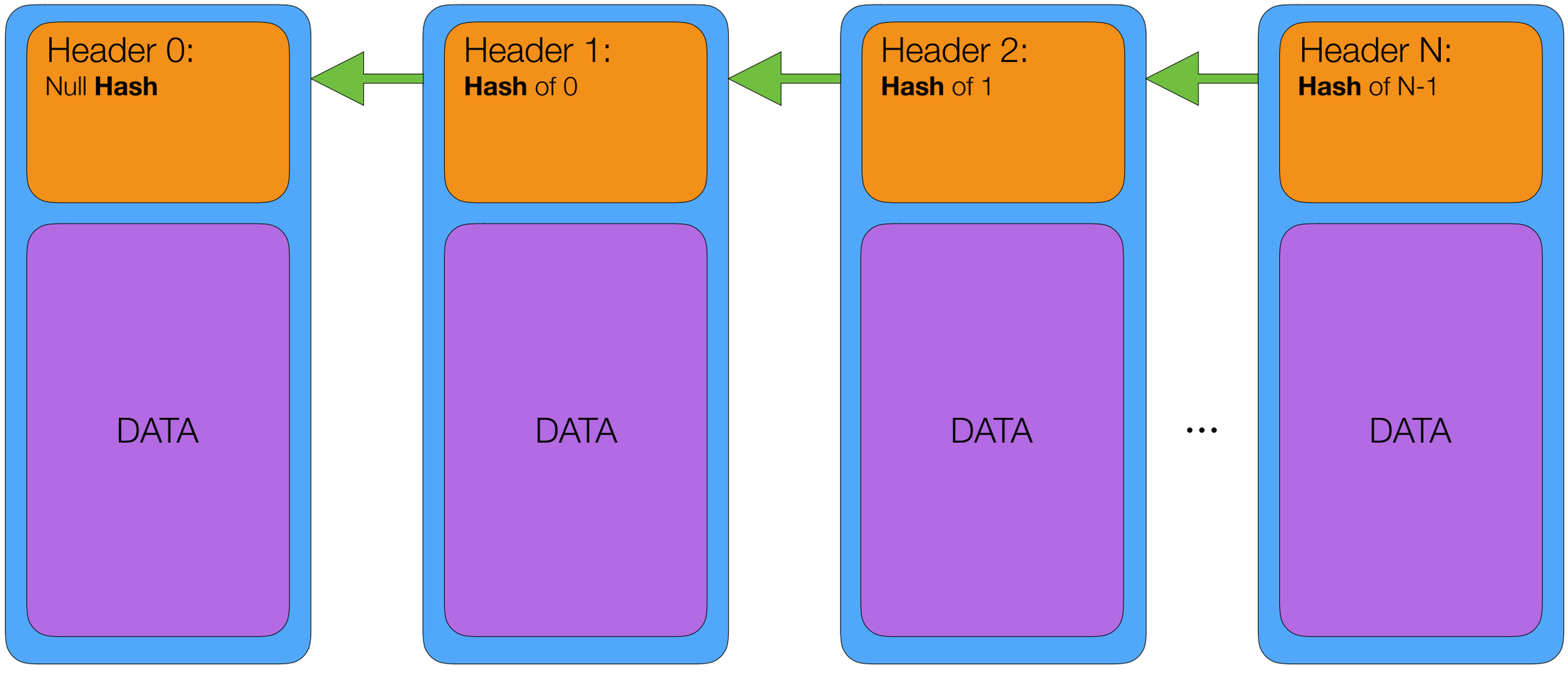
1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

- Essentially:
  - Transactions are processed in blocks
  - Miners verify the transactions in each block [Mining Reward]
  - Blocks are cryptographically signed to prevent tampering [Proof of Work]
  - Each block points to the previous block to form a chain
  - The longest chain is defined as the correct one [Consensus]

Linked List

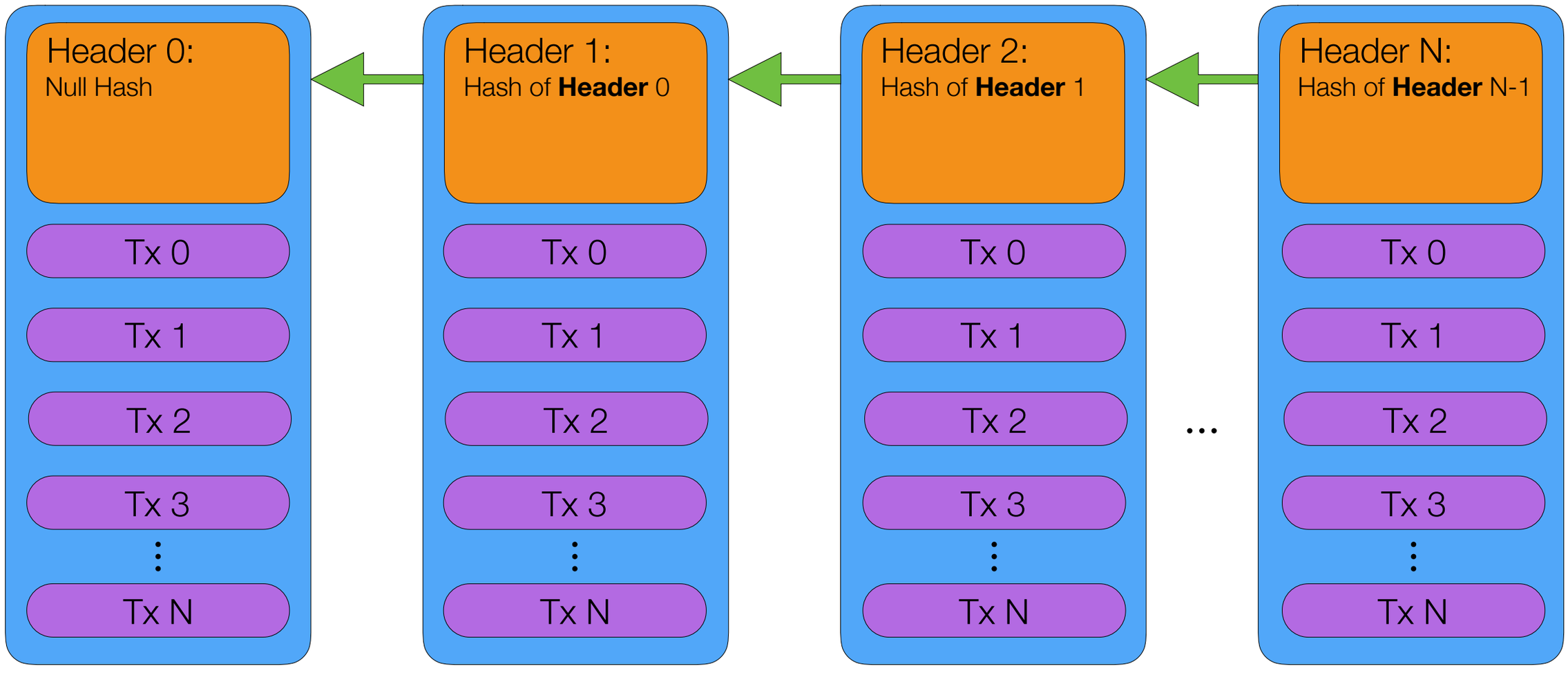

Header 0:
Null Pointer
Header 1:
Pointer to 0
Header 2:
Pointer to 1
Header N:
Pointer to N-1
DATA
DATA
DATA
...
DATA

Blockchain



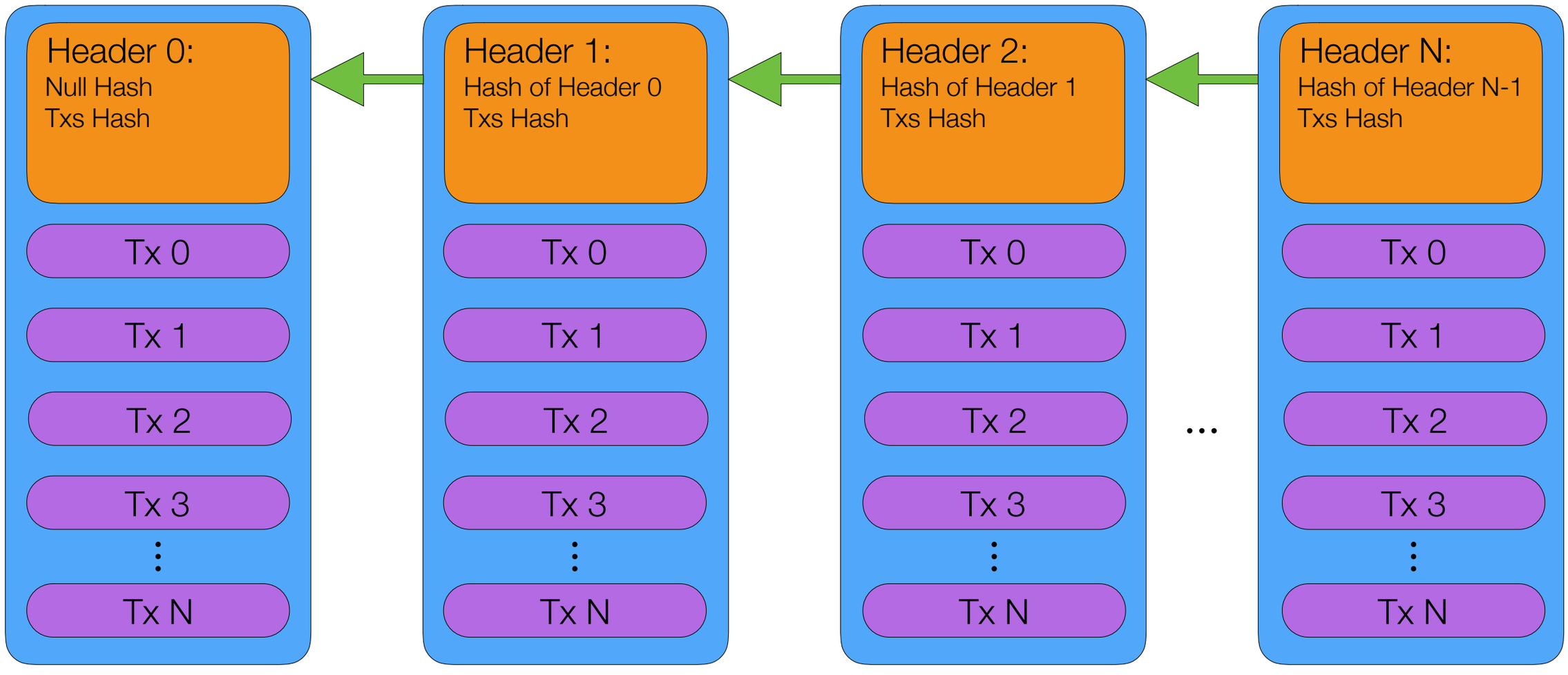
- The hashing function ensures that any changes to a validated previous block invalidates it.

Blockchain



- The hashing function ensures that any changes to a validated previous block invalidates it.
- Keep hash only the previous header for efficiency

Blockchain



- The hashing function ensures that any changes to a validated previous block invalidates it.
- Keep hash only the previous header for efficiency
- Header must include hash of data

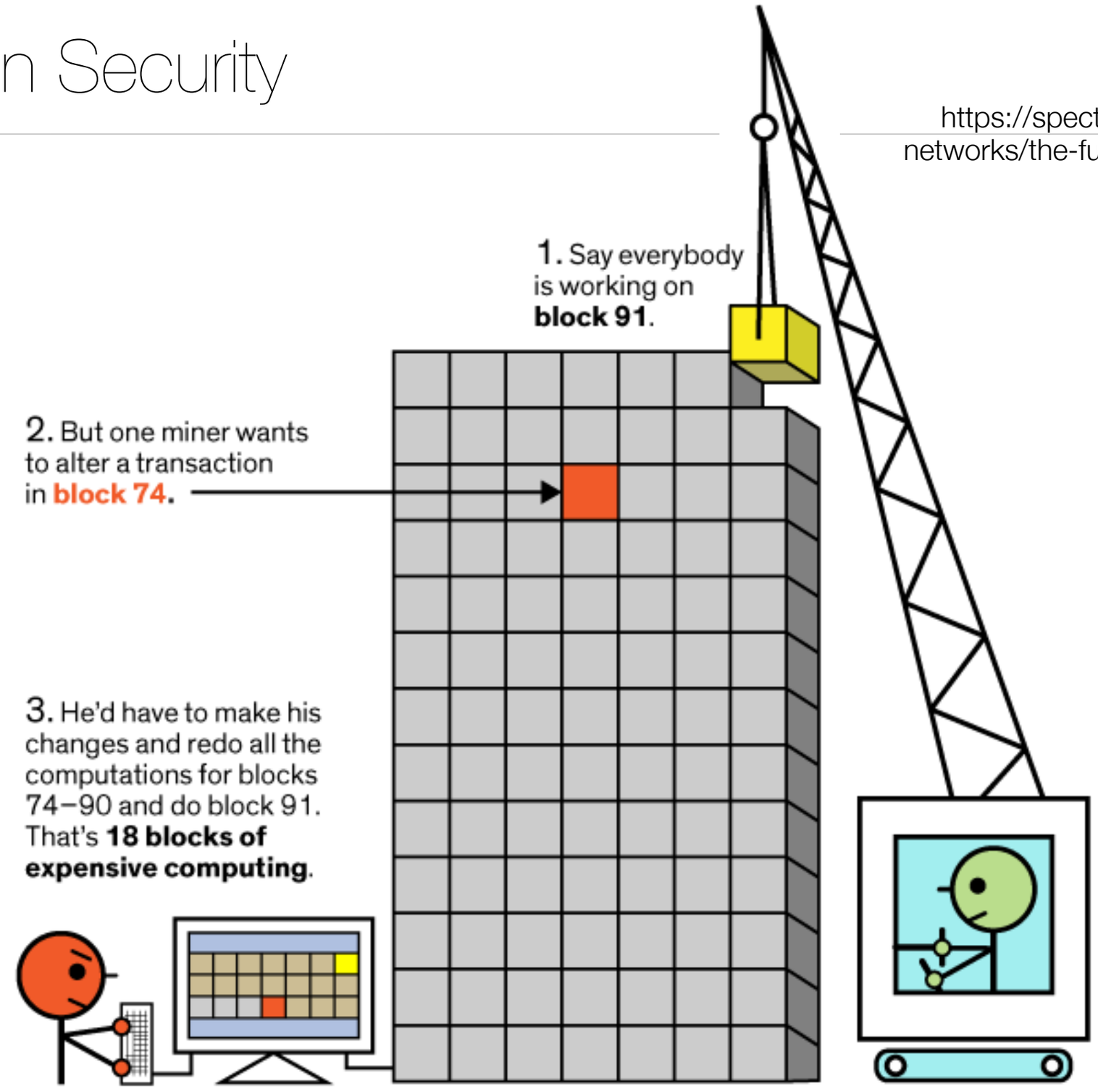
Proof Of Work

- Each block is identified by a hash value
- To control the rate at which blocks can be verified, and avoid malicious attacks the hash value of the block must obey certain conditions
- Miners add values to the data in the header (a nonce) until the hash fulfills these conditions
- The cryptographic properties of the hashing function guarantee that each value of the nonce is a roll of the dice (fairness)
- The "difficulty" level of the chain establishes how hard it is to obtain a valid hash
- Any change to the block data invalidates the hash
- The difficulty is adjusted every two weeks to account for the hashing capability of the network

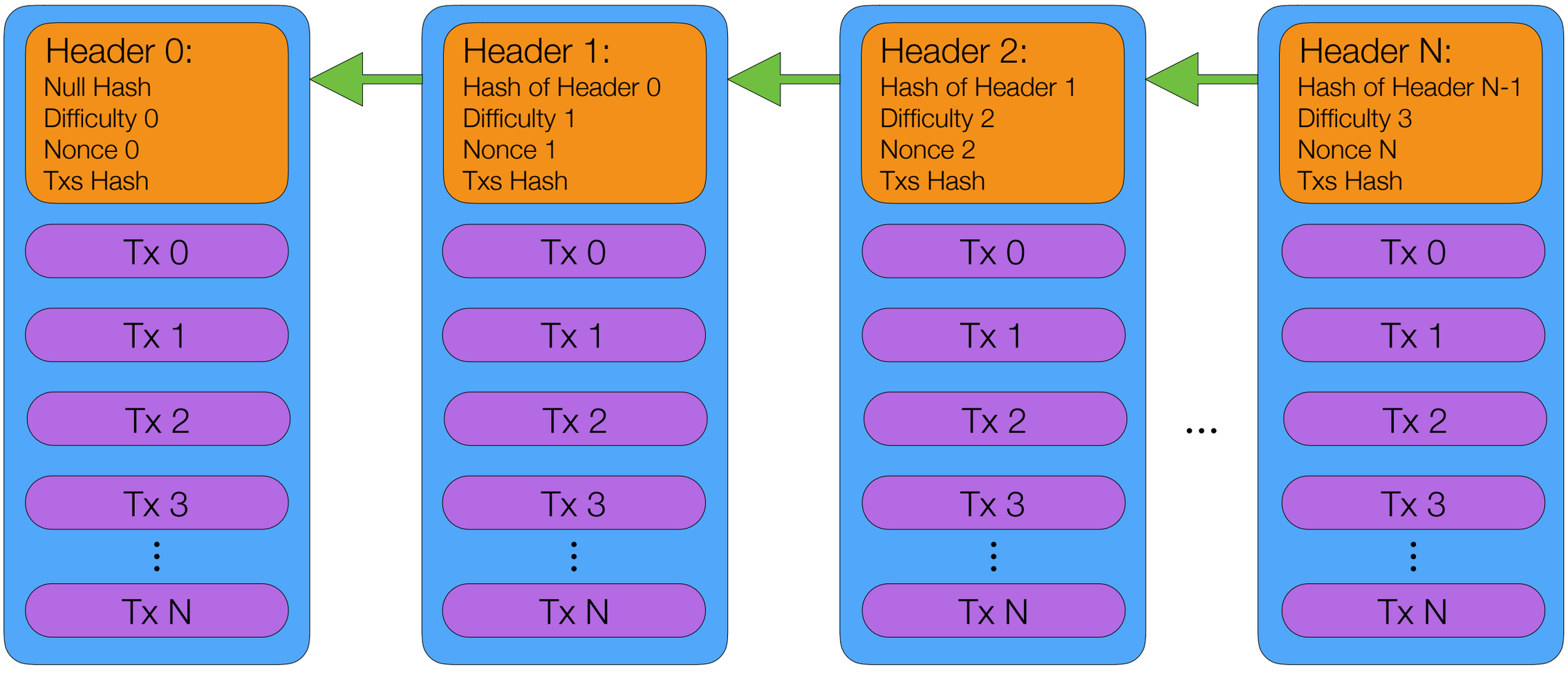
@bgoncalves

Blockchain Security

https://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin

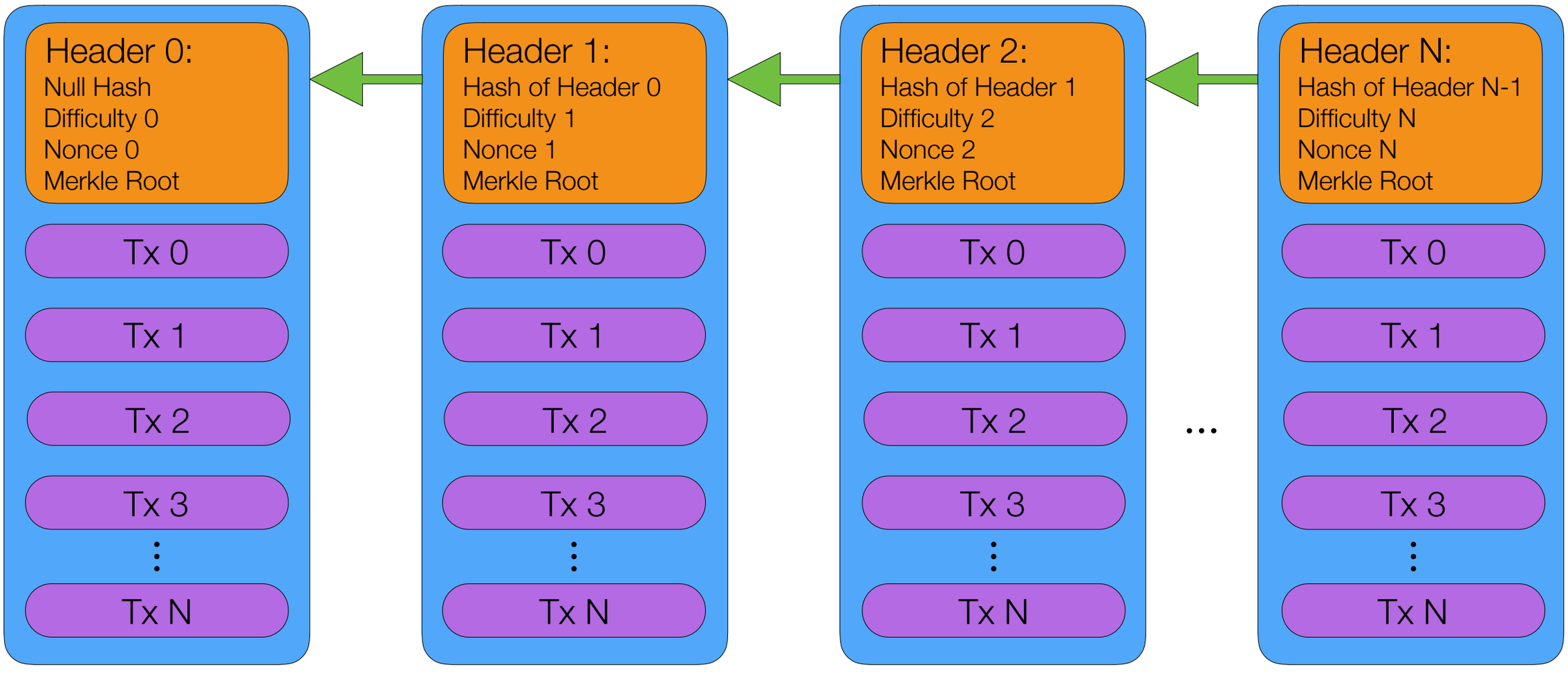


Blockchain



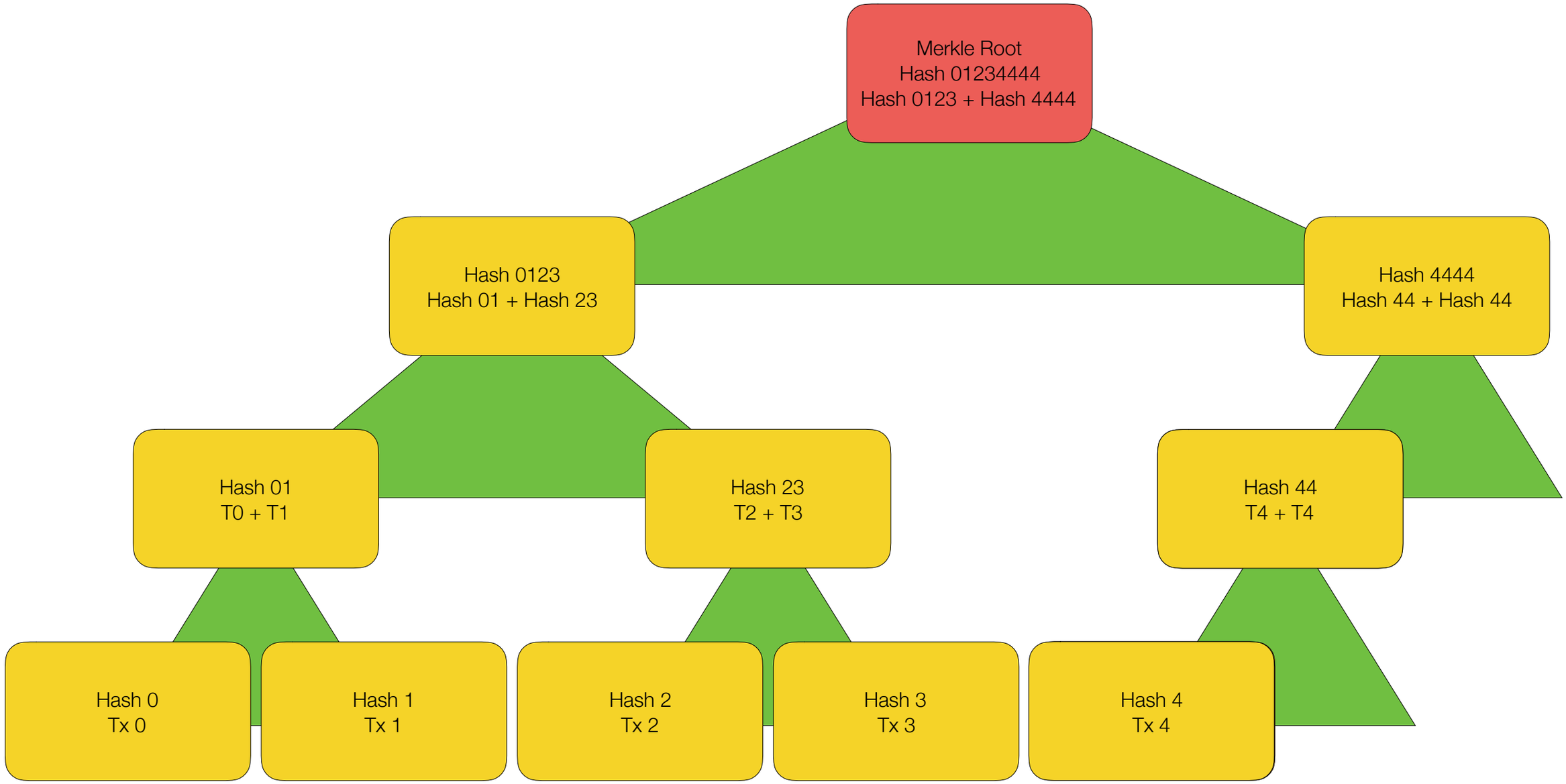
- The hashing function ensures that any changes to a validated previous block invalidates it.
- Keep hash only the previous header for efficiency
- Header must include hash of data

Blockchain



- The hashing function ensures that any changes to a validated previous block invalidates it.
- Keep hash only the previous header for efficiency
- Header must include hash of data

Merkle Tree

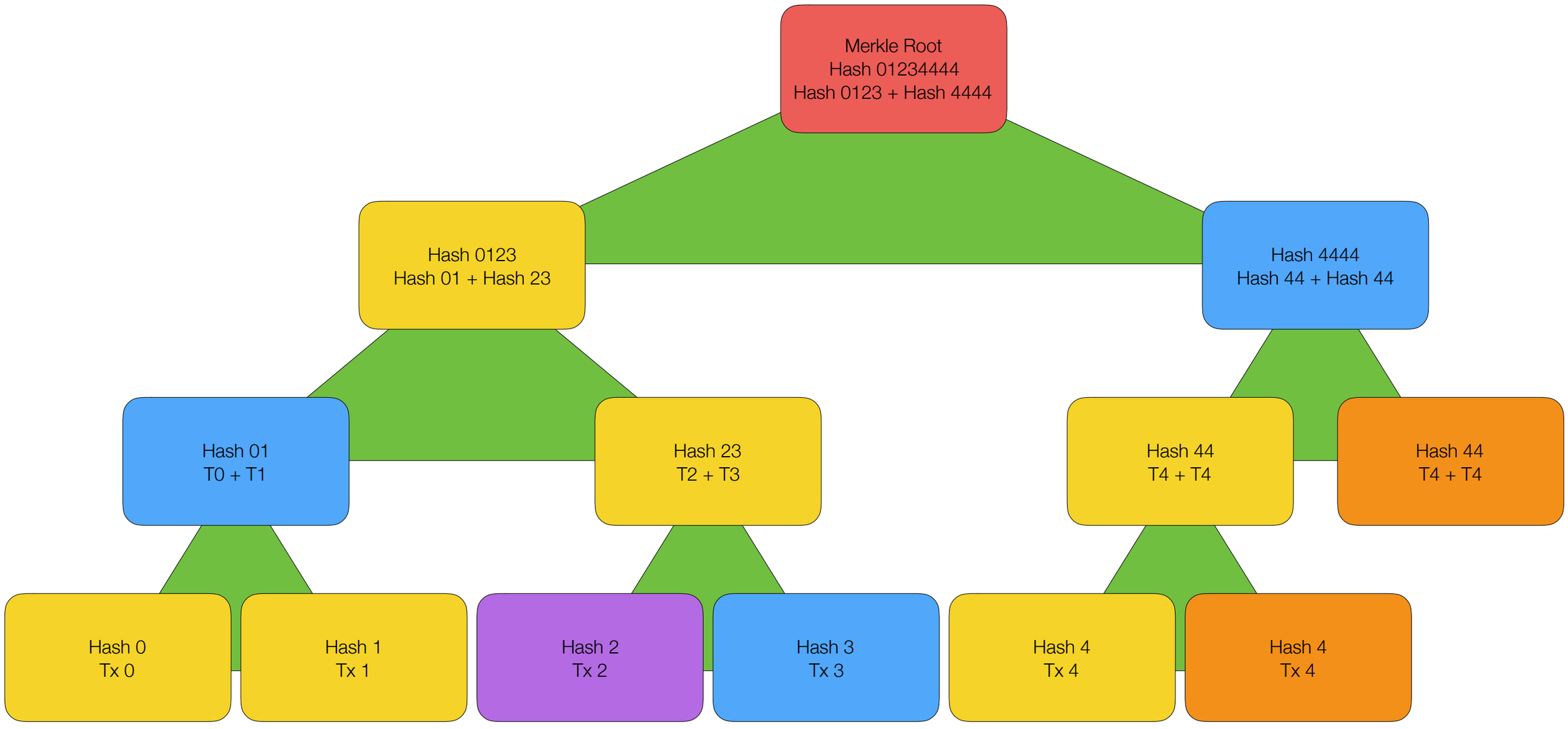

Merkle Root
Hash 01234444
Hash 0123 + Hash 4444
Hash 0123
Hash 01 + Hash 23
Hash 4444
Hash 44 + Hash 44
Hash 01
T0 + T1
Hash 23
T2 + T3
Hash 44
T4 + T4
Hash 0
Tx 0
Hash 1
Tx 1
Hash 2
Tx 2
Hash 3
Tx 3
Hash 4
Tx 4

Merkle Tree

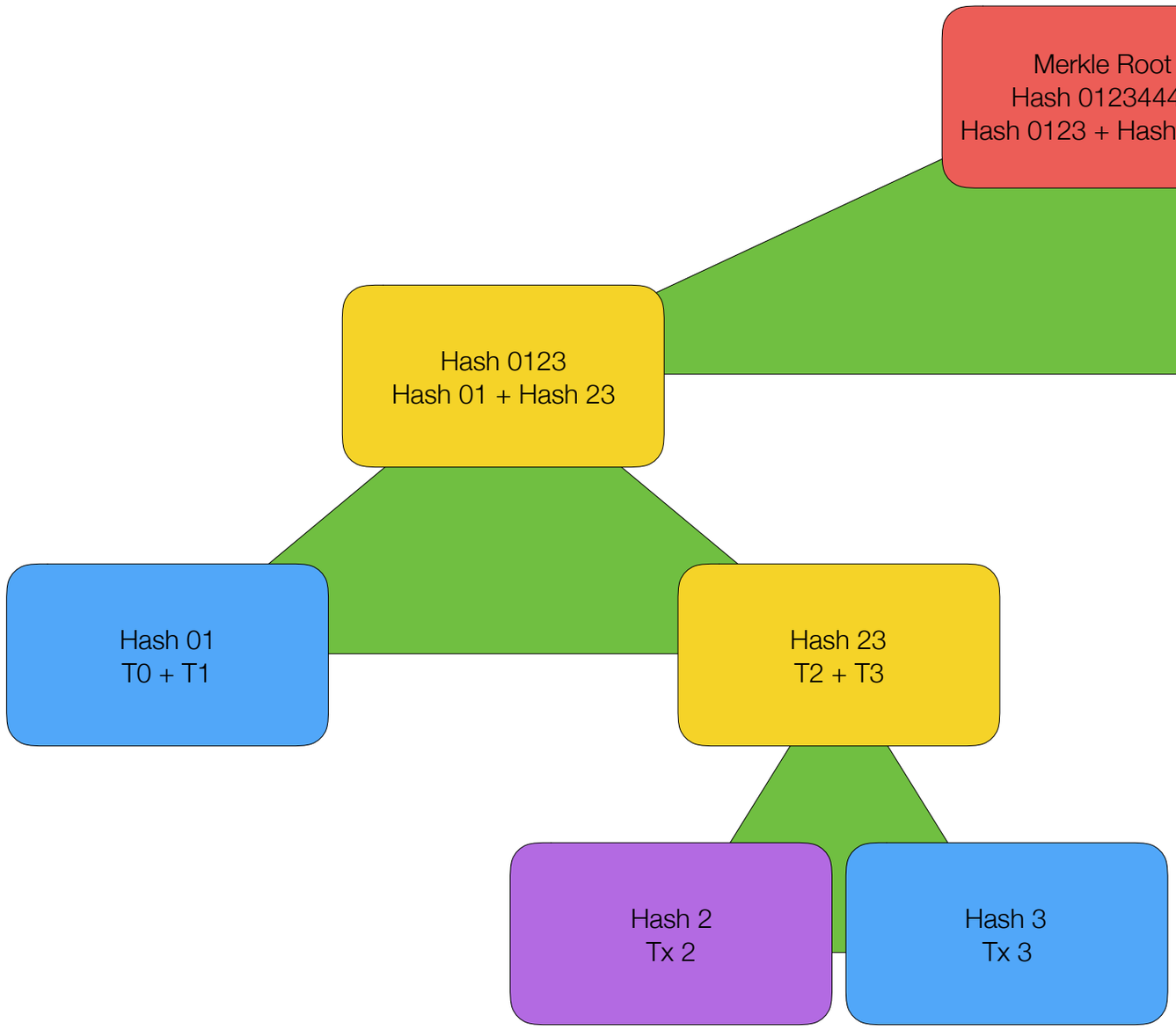
```
def get_root(transactions):
    missing = len(transactions)

    next_transactions = []

    while missing > 1:
        print(missing)
        next_transactions = []

        # If it's odd, repeat the last transaction
        if missing % 2 == 1:
            transactions.append(transactions[-1])
            missing += 1

        for i in range(0, missing, 2):
            input = transactions[i] + transactions[i+1]
            output = doubleSha256_new(input)
            next_transactions.append(output)
            print(i, i+1, next_transactions[-1])


        missing = len(next_transactions)
        transactions = next_transactions[::]

    return invert_byteorder(next_transactions[0])
```

merkle_proof.py

Merkle Proof - Tx 2



Merkle Proof - Tx 2



- In general, with N transactions you need only $\log_2(N)$ hashes to verify if a transaction is part of the tree.

- Building the tree, requires computing..... total hashes

Merkle Proof

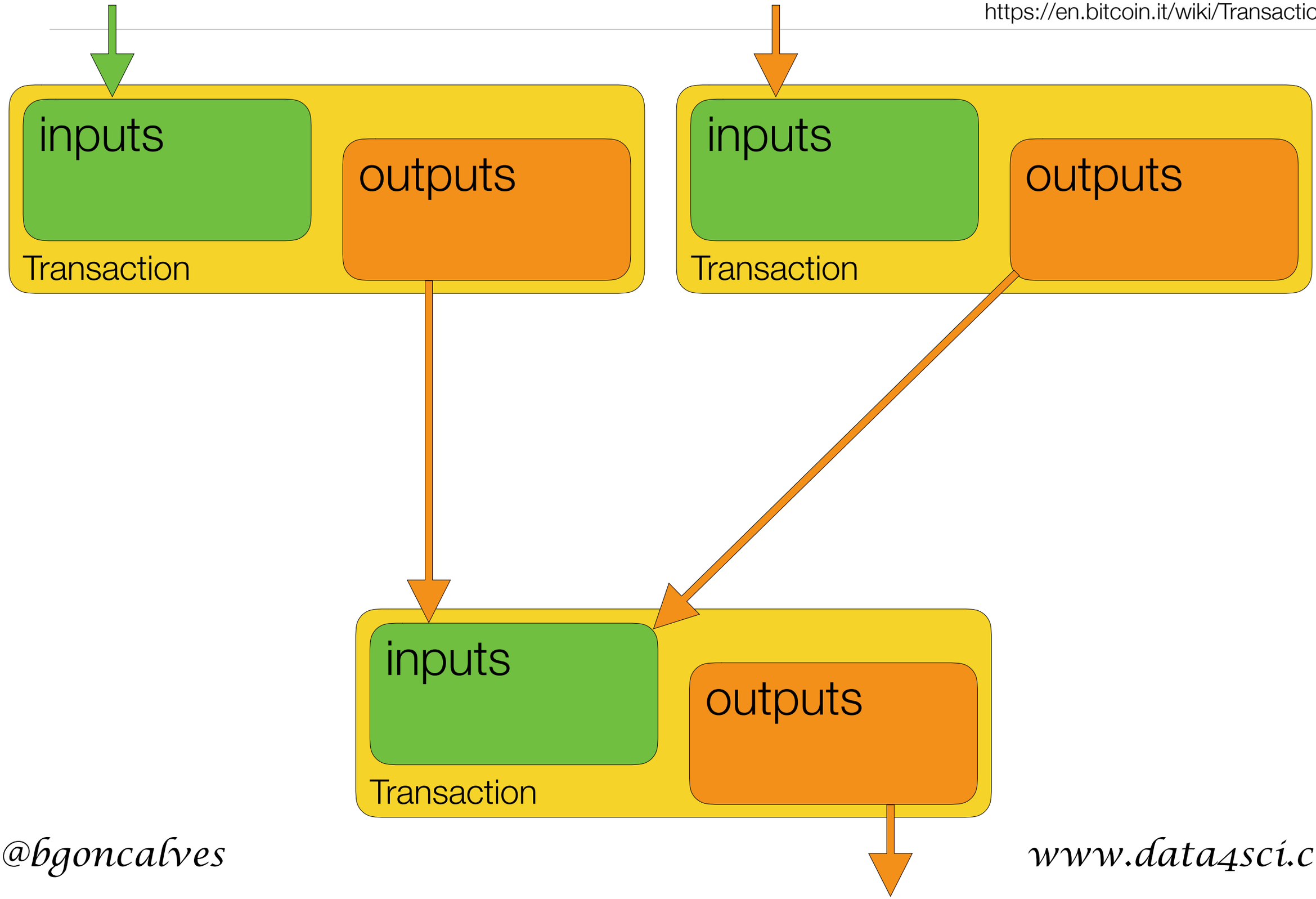
```python
def get_root(transactions):
    missing = len(transactions)

    next_transactions = []

    while missing > 1:
        print(missing)
        next_transactions = []

        # If it's odd, repeat the last transaction
        if missing % 2 == 1:
            transactions.append(transactions[-1])
            missing += 1

        for i in range(0, missing, 2):
            input = transactions[i] + transactions[i+1]
            output = doubleSha256_new(input)
            next_transactions.append(output)
            print(i, i+1, next_transactions[-1])


        missing = len(next_transactions)
        transactions = next_transactions[::]

    return invert_byteorder(next_transactions[0])
```

@bgoncalves

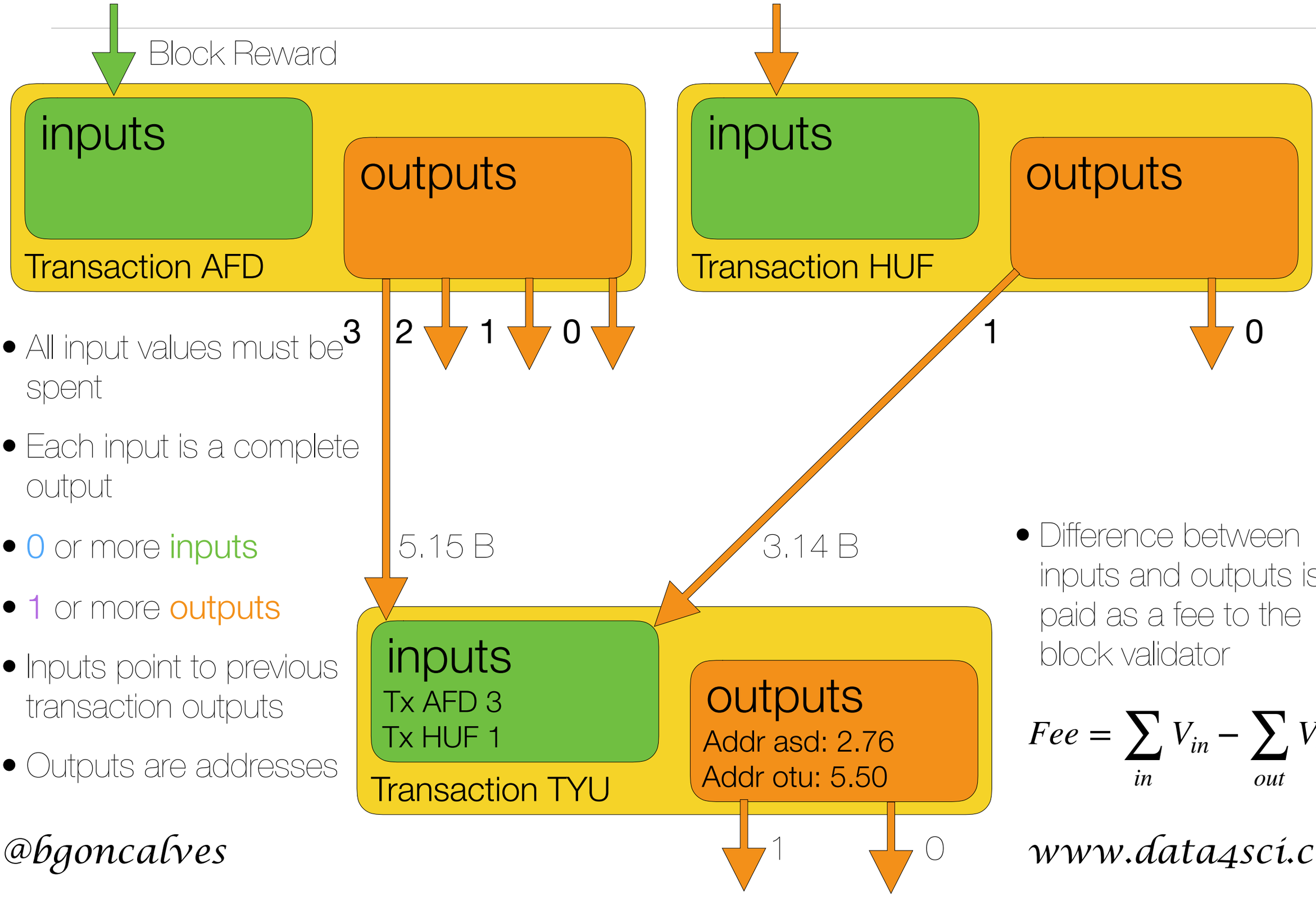
merkle_proof.py

Transactions

https://en.bitcoin.it/wiki/Transaction



Transactions



- All input values must be spent
- Each input is a complete output
- 0 or more inputs
- 1 or more outputs
- Inputs point to previous transaction outputs
- Outputs are addresses

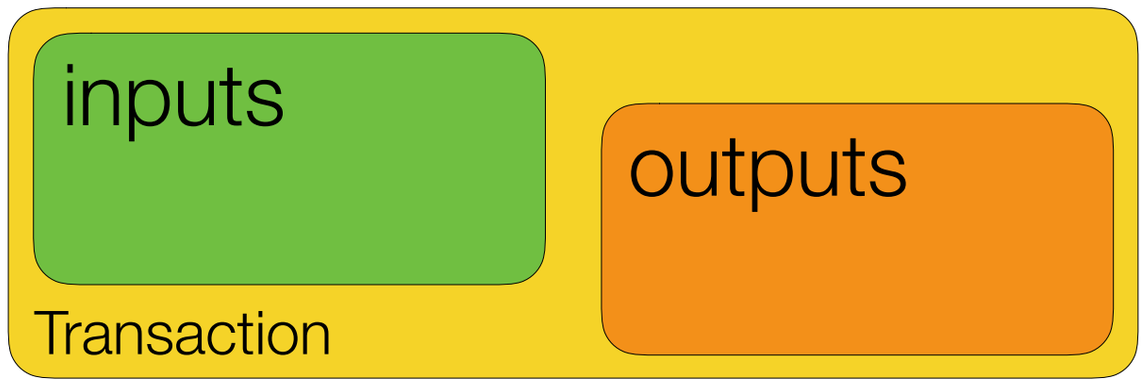
- Difference between inputs and outputs is paid as a fee to the block validator

$$Fee = \sum_{in} V_{in} - \sum_{out} V_{out} \geq 0$$

Transactions

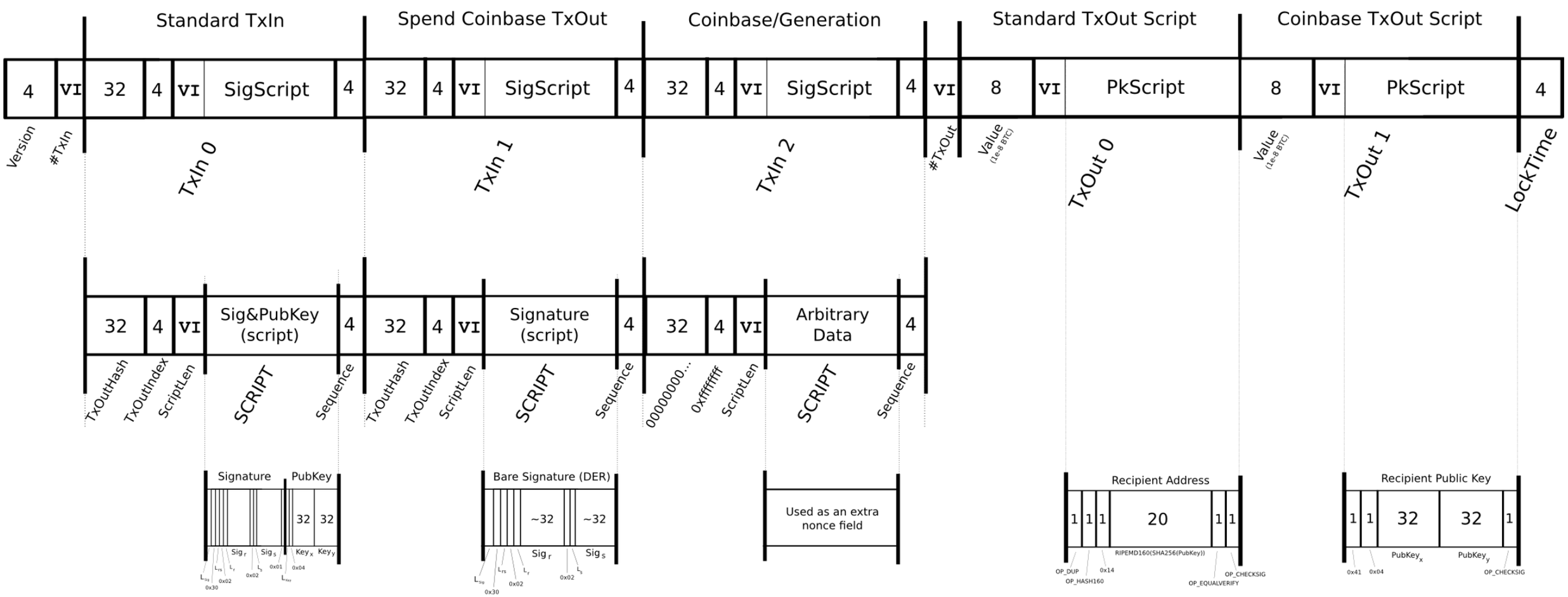
https://en.bitcoin.it/wiki/Transaction

- All input values must be spent
- Each input is a complete output
- 0 or more inputs
- 1 or more outputs
- Inputs point to previous transaction outputs
- Outputs are addresses
- First transaction in a block is the block reward and goes to the miners (coinbase transaction)
- coinbase transactions include all fees for the transactions included in the block
- Base block reward is how new Bitcoins are produced



Transactions

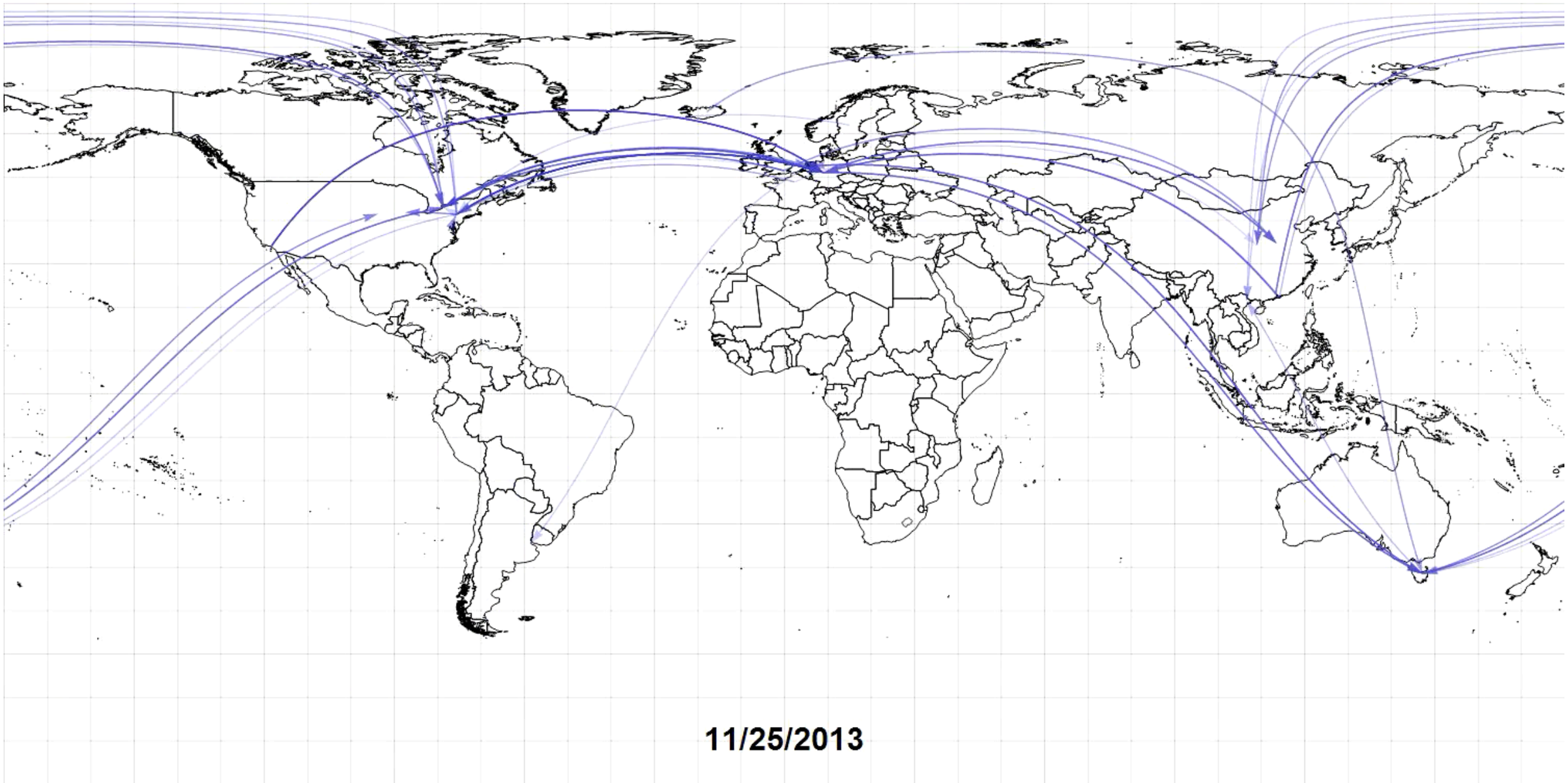
https://en.bitcoin.it/wiki/Transaction



Scripts and DER encoding both use big-endian values, all other serializations use little-endian

Bitcoin transactions around the world

http://www.vo.elte.hu/papers/2017/bitcoin/



Use Cases for Blockchain

Automotive
Track truthful, full history of vehicle from pre-production to sale
Supply chain parts management

Wills and Inheritances
Smart contracts to determine validity of will and allocation of inheritances

Travel
Passenger identification, boarding, passport, payment, and other documentation digitized and verified
Loyalty programs digitization and tracking

Real Estate
Transparency within agreements
Verify Property information, update and decentralize records
Reduce paperwork, digitize transactional processes
Record, track, transfer land titles

Public Transportation/Ride Sharing
Streamline public transportation
Provide more accurate payment for ride, gas, and wear and tear

Music Streaming
Prevent illegal downloading of music
Provide proper compensation for purchased songs to artists

Medical / Healthcare
Drug Supply Chain Integrity
Patient Databases/Indexes on blockchain
Claims Adjudication
Medical Supply Chain Management
Transparency and Automation within the patient-to-hospital or patient-to-doctor transactions
Clinical trial provenance - integrity with an auditable trail of data exchange
Efficiency, privacy, and ownership of patient health data

Media
Control of ownership rights
Anti-piracy / copyright infringement
Use of smart contracts for artist compensation/legal proceedings
Payments processing = cryptographic, secure, and anti-3rd party (this opens up content availability internationally)

Marketing
Bypass intermediaries, providing more cost-effective advertising

Legal
Smart contracts with defined rules, expiration, and accessibility for relevant parties.

Law Enforcement
Integrity of evidence, resistance to falsification of case data
Documentation of time-stamped, chronological chain of facts

IOT
Ability for IoT applications to contribute transactional data to blockchains
Implications across industries (trucking/transportation, supply chain integrity.

Insurance
Improve multi-party contracts
Streamline risk contract efficiency
Streamline claims adjudication
Reduce disputes with transparency of shared data

Human Resources
Background checks: Verification of identity, employment history
Payment and benefits process validation - smart contracts

Banking, Financial, Fintech
Streamline payments processing with high efficiency, fast and secure transactions
Empower global transactions, tearing down national currency borders
Minimize auditing complexity for any financial ledger

Charity
Tracking donation allocation, accountability, integrity
Reduce overhead and complexity of donation payment processing

Cloud Storage
Increased security with a shift from centralized data security to decentralized network
Lower transactional costs within a decentralized network
Crowdsourcing unused cloud storage

Commercial Vehicles and Transportation
Tracking journey stops; paired with IoT to create an immutable ledger of trip data

Credit History
Make credit reports more accurate, transparent, and accessible

Cybersecurity
Fight hacking with immutability of ledger
Guarantee validity with data integrity
No Single Point of Failure (decrease in IP-based DDoS attack success)

Donations
Provide auditable trail for donations to prevent fraud
Ensure crowdfunded campaigns receive donations and contributors are compensated

Education
Digitizing, verifying academic credentials
Federated repository of academic information specific to class, professor, and student

Energy
Bypass public grids to allow for cheaper, peer to peer energy transfer
Smart utility metering

Forecasting
Combined with machine learning algorithms, blockchain can provide a decentralized forecasting tool

Government and Voting
Reduce voter fraud, inefficiencies with verifiable audit trails
Minimize government fraud, digitize most processes
Increase accountability and compliance for government officials
Identity validation; integrity of citizen registry data

Gun Safety
Tracking gun ownership and possession related information
Tracking criminal ID history and attempts to purchase

FlureeDB

START

A. Are you trying to remove intermediaries or brokers?
YES → B
NO → Do not use blockchain

B. Are you working with digital assets (versus physical assets)?
YES → C
NO → Do not use blockchain

C. Can you create a permanent, authoritative record of the digital asset in question?
YES → D
NO → Do not use blockchain

D. Do you require high performance, rapid (~millisecond) transactions?
YES → Blockchain can't do this efficiently yet, but solutions are in development
NO → E

E. Do you intend to store large amounts of non-transactional data as part of your solution?
YES → Blockchain can't do this efficiently yet, but solutions are in development
NO → F

F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)
YES → Blockchain may work – further research is needed
NO → G

G. Are you managing contractual relationships or value exchange?
YES → H
NO → Blockchain may work – further research is needed

H. Do you require shared write access?
YES → I
NO → Are contributors interests unified or well-aligned?

I. Do contributors know and trust each other?
YES → Are contributors interests unified or well-aligned?
NO → J

Are contributors interests unified or well-aligned?
YES → Blockchain may work – further research is needed
NO → J

J. Do you need to be able to control functionality?
YES → K
NO → Strong case for blockchain (private/ permissioned ledger)*

K. Should transactions be public?
YES → Strong case for blockchain (public ledger)*
NO → Strong case for blockchain (private/ permissioned ledger)*

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

Blockchain
Beyond the Hype

See **http://wef.ch/blockchainhype** for accompanying text that further explains the questions.

*See full report at **http://wef.ch/blockchainhype** for more information about public and permissioned ledgers. In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT). DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator. This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant *CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1)* and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

THE CRYPTO UNIVERSE

COMPARING SIX MAJOR CURRENCIES

BITCOIN

Bitcoin is the original cryptocurrency, and was released as open-source software in 2009.

Using a new distributed ledger known as the blockchain, the Bitcoin protocol allows for users to make peer-to-peer transactions using digital currency while avoiding the "double spending" problem.

No central authority or server verifies transactions, and instead the legitimacy of a payment is determined by the decentralized network itself.

KEY FEATURES

- Blockchain - Foundational Technology
- Fast P2P Payments Worldwide
- No Double Spend Problem
- Low Processing Fees
- Decentralized
- Available To Anyone
- Anonymity (Partial)
- Transparent

INTERESTING FACT

In 2010, a programmer bought two pizzas for 10,000 BTC in one of the first real-world bitcoin transactions.

Today, 10,000 BTC is equal to roughly $38.1 million - a big price to pay for satisfying hunger pangs.

1 → 10,000

While regrettable, it is also forgivable. No one knew Bitcoin would be accepted by hundreds of thousands of merchants just years later.

Now cryptocurrency enthusiasts around the world celebrate "Bitcoin Pizza Day" every year on May 22nd, the date the transaction took place.

BOTTOM LINE FOR BITCOIN Bitcoin is the original cryptocurrency with the most liquidity and significant network effects". It also has brand name recognition around the world, with an eight year track record.

LITECOIN

Litecoin was launched in 2011 as an early alternative to Bitcoin.

Around this time, increasingly specialized and expensive hardware was needed to mine bitcoins, making it hard for regular people to get in on the action. Litecoin's algorithm was an attempt to even the playing field so that anyone with a regular computer could take part in the network.

KEY DIFFERENTIATIONS FROM BITCOIN

- A Simpler Cryptographic Algorithm
- 4x Faster Block Generation
- Faster Transaction Processing
- 84 Million Coin Max (Bitcoin: 21 million)

INTERESTING FACT

Litecoin's creator is a former Google employee and MIT grad named Charlie Lee. He wanted to make cryptocurrency more accessible - and for Litecoin to be the "silver" to Bitcoin's "gold".

BOTTOM LINE FOR LITECOIN Other altcoins have taken away some of Litecoin's market share, but it still has an early mover advantage and some strong network effects.

RIPPLE

Ripple is considerably different from Bitcoin. That's because Ripple is essentially a global settlement network for other currencies such as USD, Bitcoin, EUR, GBP, or any other units of value (i.e. frequent flier miles, commodities).

To make any such a settlement, however, a tiny fee must be paid in XRP (Ripple's native tokens) - and these are what trade on cryptocurrency markets.

KEY DIFFERENTIATIONS FROM BITCOIN

- Global Settlement Network
- Works With Any Store of Value
- Backed By Many Banking Institutions
- No Mining Involved

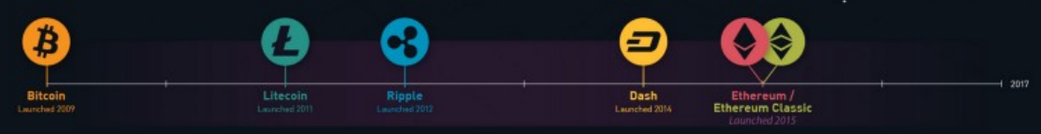
INTERESTING FACT

Because Ripple is intended as a new global settlement system for the exchange of currencies and other assets, many banks are experimenting with the technology.

Banks counted as early supporters include: Royal Bank of Canada, Santander, UBS, and UniCredit.

There is no "mining" on the Ripple network – instead, there is an existing supply of 100 billion ripples, with many still being held by the company. In mid-2017, the company announced they'd lock up billions of dollars worth of ripples in escrow smart contracts, to decrease any fears of the market being "flooded".

BOTTOM LINE FOR RIPPLE Ripple runs on many of the same principles of Bitcoin, but for a different purpose: to serve as the middle man for all global FX transactions. If it can successfully capture that market, the potential is high.



% OF THE CRYPTO UNIVERSE VALUE

source: coinmarketcap.com as of Sept. 12, 2017

METRICS BY COIN

sources: bitinfocharts.com as of Sept. 7, 2017
*2017: XRPCharts

ALL-TIME PEAK PRICE USD

source: coinmarketcap.com as of Sept. 12, 2017

DASH

Dash is an attempt to improve on Bitcoin in two main areas: speed of transactions, and anonymity.

To do this, it has a two-tier architecture with miners and also "masternodes" that help the network perform advanced functions such as near-instant transactions and coin-mixing to provide additional privacy.

KEY DIFFERENTIATIONS FROM BITCOIN

- Two-Tier Architecture
- Advanced Transactions
- Decentralized Autonomous Organization (DAO)
- Improved Anonymity

INTERESTING FACT

For each block mined, a 10% reward goes to the treasury to help fund improvements and projects around Dash.

Dash is the first ever Decentralized Autonomous Organization (DAO), a type of organization run through rules encoded in computer programs and smart contracts.

BOTTOM LINE FOR DASH The innovations behind Dash are interesting, and could help to make the coin more consumer-friendly than other alternatives.

ETHEREUM

Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

KEY DIFFERENTIATIONS FROM BITCOIN

- Platform For Making Blockchain Applications
- Multiple Industry Uses
- Uses Smart Contracts
- Ether Powers The Network

INTERESTING FACT

Ethereum has quickly skyrocketed in value since its introduction in 2015, and it is now the 2nd most valuable cryptocurrency by market cap.

It's increased in value by 2,226% in just the last year - a huge boon for early investors.

BOTTOM LINE FOR ETHERUM Ethereum serves a different purpose than other cryptocurrencies, but it has quickly grown to displace all but Bitcoin in value. Some experts are so bullish on Ethereum that they even see it becoming the world's top cryptocurrency in just a short span of time - but only time will tell.

ETHEREUM CLASSIC

In 2016, the Ethereum community faced a difficult decision: The DAO, a venture capital firm built on top of the Ethereum platform, had $50 million in ether stolen from it through a security vulnerability.

The majority of the Ethereum community decided to help The DAO by "hard forking" the currency, and then changing the blockchain to return the stolen proceeds back to The DAO.

The minority thought this idea violated the key foundation of immutability that the blockchain was designed around, and kept the original Ethereum blockchain the way it was. Hence, the "Classic" label.

KEY DIFFERENTIATIONS FROM BITCOIN

- Platform For Making Blockchain Applications
- Multiple Industry Uses
- Uses Smart Contracts
- Ether Powers The Network

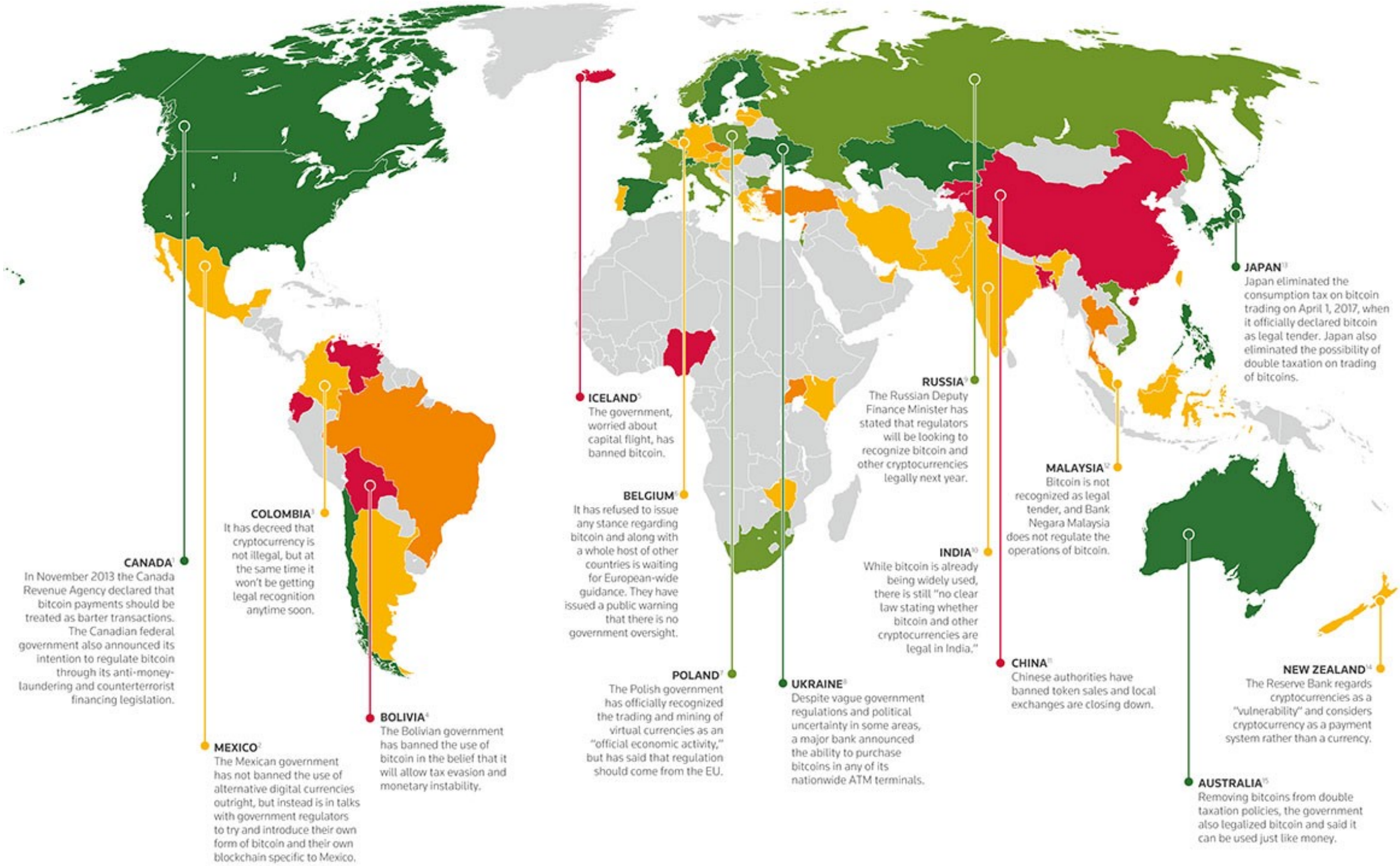
INTERESTING FACT

Because Ethereum and Ethereum Classic stem from the same code, they run in parallel, doing virtually the same thing.

The DAO hacker still holds over 3 million of Ethereum Classic, which could be "dumped" somewhere along the line – a baked in risk that could drag on price.

BOTTOM LINE FOR ETHERUM CLASSIC As time goes on, Ethereum Classic has been carving out a separate identity from its bigger sibling. With similar capabilities and a different set of principles, Ethereum Classic could still have upside.

A WORLD OF CRYPTOCURRENCIES



CANADA[1]
In November 2013 the Canada Revenue Agency declared that bitcoin payments should be treated as barter transactions. The Canadian federal government also announced its intention to regulate bitcoin through its anti-money-laundering and counterterrorist financing legislation.

MEXICO[2]
The Mexican government has not banned the use of alternative digital currencies outright, but instead is in talks with government regulators to try and introduce their own form of bitcoin and their own blockchain specific to Mexico.

COLOMBIA[3]
It has decreed that cryptocurrency is not illegal, but at the same time it won't be getting legal recognition anytime soon.

BOLIVIA[4]
The Bolivian government has banned the use of bitcoin in the belief that it will allow tax evasion and monetary instability.

ICELAND[5]
The government, worried about capital flight, has banned bitcoin.

BELGIUM[6]
It has refused to issue any stance regarding bitcoin and along with a whole host of other countries is waiting for European-wide guidance. They have issued a public warning that there is no government oversight.

POLAND[7]
The Polish government has officially recognized the trading and mining of virtual currencies as an "official economic activity," but has said that regulation should come from the EU.

UKRAINE[8]
Despite vague government regulations and political uncertainty in some areas, a major bank announced the ability to purchase bitcoins in any of its nationwide ATM terminals.

RUSSIA[9]
The Russian Deputy Finance Minister has stated that regulators will be looking to recognize bitcoin and other cryptocurrencies legally next year.

INDIA[10]
While bitcoin is already being widely used, there is still "no clear law stating whether bitcoin and other cryptocurrencies are legal in India."

CHINA[11]
Chinese authorities have banned token sales and local exchanges are closing down.

MALAYSIA[12]
Bitcoin is not recognized as legal tender, and Bank Negara Malaysia does not regulate the operations of bitcoin.

JAPAN[13]
Japan eliminated the consumption tax on bitcoin trading on April 1, 2017, when it officially declared bitcoin as legal tender. Japan also eliminated the possibility of double taxation on trading of bitcoins.

NEW ZEALAND[14]
The Reserve Bank regards cryptocurrencies as a "vulnerability" and considers cryptocurrency as a payment system rather than a currency.

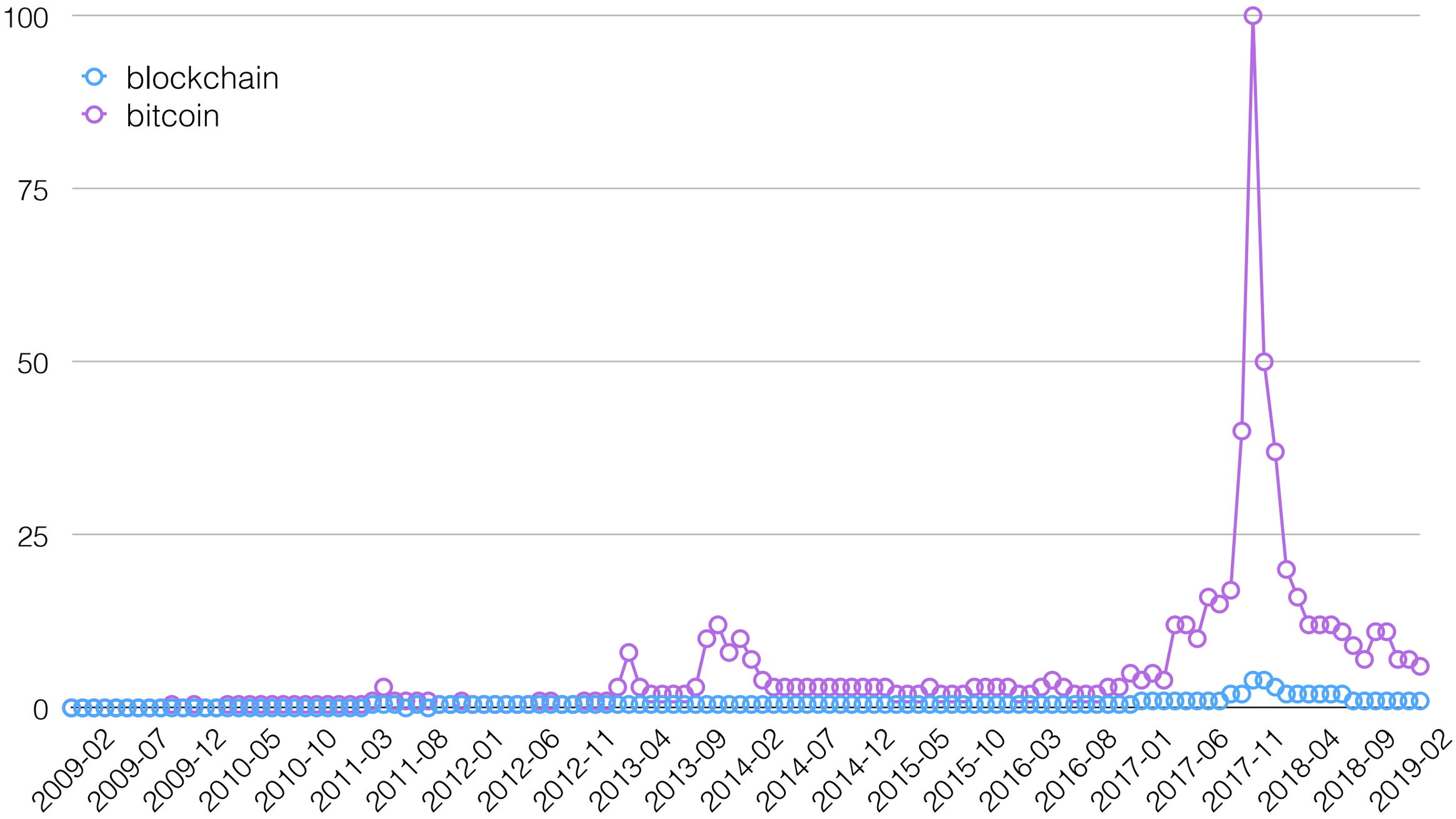
AUSTRALIA[15]
Removing bitcoins from double taxation policies, the government also legalized bitcoin and said it can be used just like money.

1 https://www.fxempire.com/education/article/what-does-the-future-of-bitcoin-look-like-404636
2 https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies
3 http://insidebitcoins.com/news/colombia-clarifies-stance-bitcoin-is-not-illegal/60667
4 https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies
5 https://themerkle.com/bitcoins-legal-status-worldwide
6 https://www.cryptocompare.com/coins/guides/how-legal-is-bitcoin-and-crypto-currencies
7 https://cointelegraph.com/news/poland-officially-recognizes-trading-in-bitcoin-and-other-cryptocurrencies
8 https://www.forbes.com/sites/realspin/2017/03/20/ukraine-is-silently-leading-a-digital-currency-revolution/#7e902d53465c
9 https://www.fxempire.com/education/article/what-does-the-future-of-bitcoin-look-like-404636
10 https://news.bitcoin.com/india-supreme-court-bitcoin-legalization-taxation
11 https://qz.com/1079900/huobi-and-okcoin-chinas-two-biggest-bitcoin-exchanges-will-halt-all-trading-services-for-local-customers/
12 https://www.nst.com.my/opinion/columnists/2017/06/249010/are-we-ready-bitcoin
13 https://news.bitcoin.com/india-supreme-court-bitcoin-legalization-taxation
14 http://www.stuff.co.nz/business/93087302/cybercurrency-exchange-offers-more-than-bitcoin-for-new-zealand-dollars
15 https://news.bitcoin.com/india-supreme-court-bitcoin-legalization-taxation

Read about all of the countries at
thomsonreuters.com/know360app

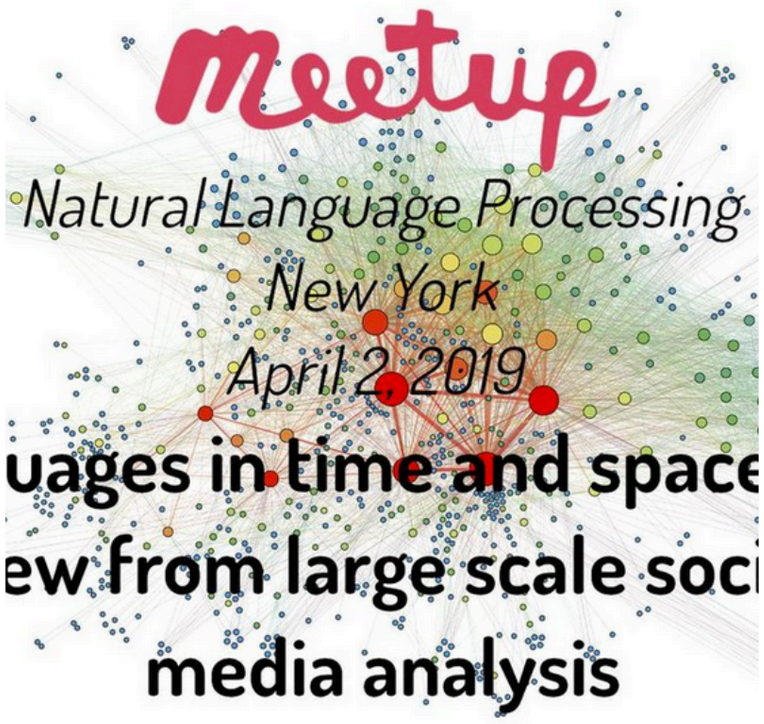
How much is it worth?

Bitcoin interest over time



Bitcoin price

Questions?

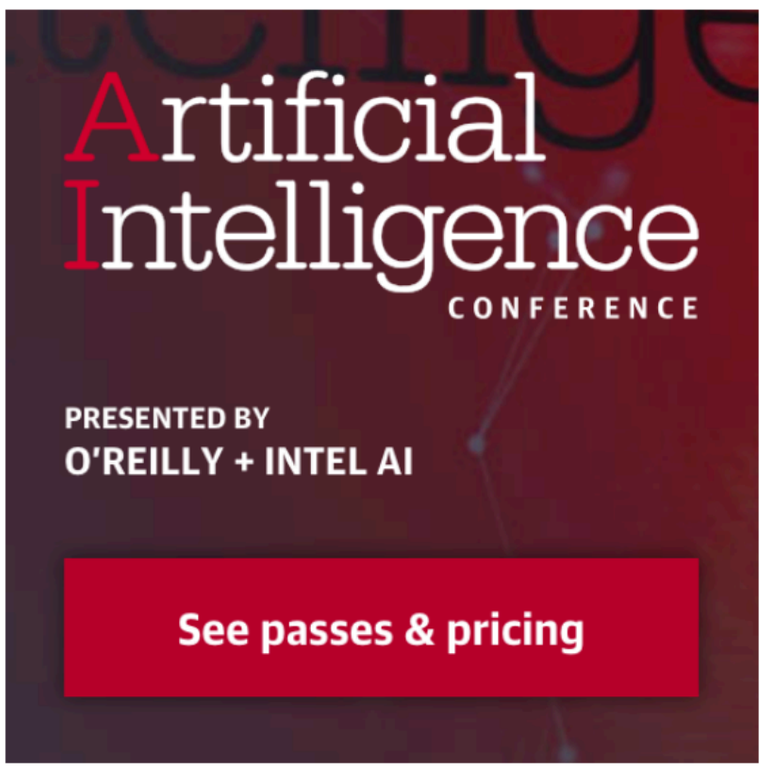


Languages in time and space: the view from large scale social media analysis
Apr 2, 2019

The advent of online social services coupled with GPS-enabled smartphones resulted in the accumulation of massive amounts of data documenting our individual and social behavior. Using sources such as Twitter, Wikipedia, Google Books and others, this talk will present how languages are used across both time and space. In particular, we will analyze how language dialects can be defined based on how they are used in the real world. We will also analyze how English usage changes from place to place and over time and how languages can be used to identify communities within the urban environment.

REGISTER

LEARN MORE



Recurrent neural networks for time series analysis
Apr 16, 2019

Time series are everywhere around us. Understanding them requires taking into account the sequence of values seen in previous steps and even long-term temporal correlations. Join Bruno Gonçalves to learn how to use recurrent neural networks to model and forecast time series and discover the advantages and disadvantages of recurrent neural networks with respect to more traditional approaches.

REGISTER

LEARN MORE

HOW A BITCOIN IS MINTED

The birth of a new Bitcoin begins when a number of existing Bitcoins are used in transactions.

1 Alice sends Bob a unique Bitcoin from her secure digital wallet.

2
Software bundles this transaction, along with others, into a block, and transmits this block to a network of computers for verification.

3
Computers on this network race to verify the block of transactions.

4
Once it is proven valid, the block is added to the entire shared ledger of all Bitcoin transactions. This shared ledger is called the blockchain.

5 The updated blockchain is then distributed to the entire network and used for future verification.

6
The "miners" whose computers are first to verify transactions and maintain the blockchain win a chunk of brand new Bitcoins as their reward.

@bgoncalves

www.data4sci.com

THE FINTECH ECOSYSTEM

Payments & Transfers

DWOLLA
stripe
PayPal
Square
Klarna
venmo
Braintree
iZettle
SHOPKEEP
SMARTER BUSINESS
adyen
Paydiant
VISA Checkout
AMEX EXPRESS CHECKOUT
Pay
pay
SAMSUNG pay
CURRENTC
xoom
REMITLY
azimo
worldremit
TransferWise
BitPesa
currency cloud
flywire

Lending & Financing

LendingClub
PROSPER
OnDeck
Funding Circle
prêt d'union
Zopa
AVANT CREDIT
BOND STREET
SoFi
auxmoney
Patch of Land
Orchard
Rate%Setter
credible
FUNDRISE
AssetAvenue
陆金所 Lufax.com
lendio
信而富 China Rapid Finance
CREDIBLY
CAN CAPITAL
Affirm
toborrow
Even
Biz2Credit
zest finance
Bondora
able
Upstart
EVEN FINANCIAL
earnest
CommonBond

Retail Banking

SIMPLE
Moven
ally
GObank
WeBank 微众银行
Atom
TANDEM
Together we can build a better bank
CapitalOne 360

Financial Management

LendingRobot
Credit Karma
Betterment
motif INVESTING
wealthfront
nutmeg
robinhood
BILL GUARD
mint.com

Insurance

metromile
oscar
friendsurance
MyDrive
bizinsure
business insurance just got smarter

Markets & Exchanges

WeSwap
SOCIAL CURRENCY
ripple
coinbase
BITSTAMP
kraken
LendingRobot
BTC e
coinsetter

BI INTELLIGENCE

IN BLOCKCHAIN WE TRUST

Proof of Stake

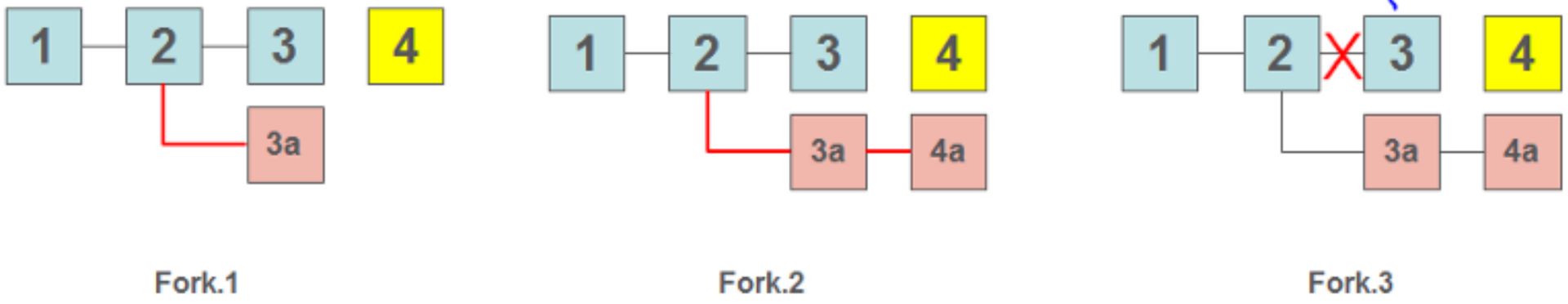
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

❖ **Sign = func(order message, Private key)** ⟶

Transaction Messages

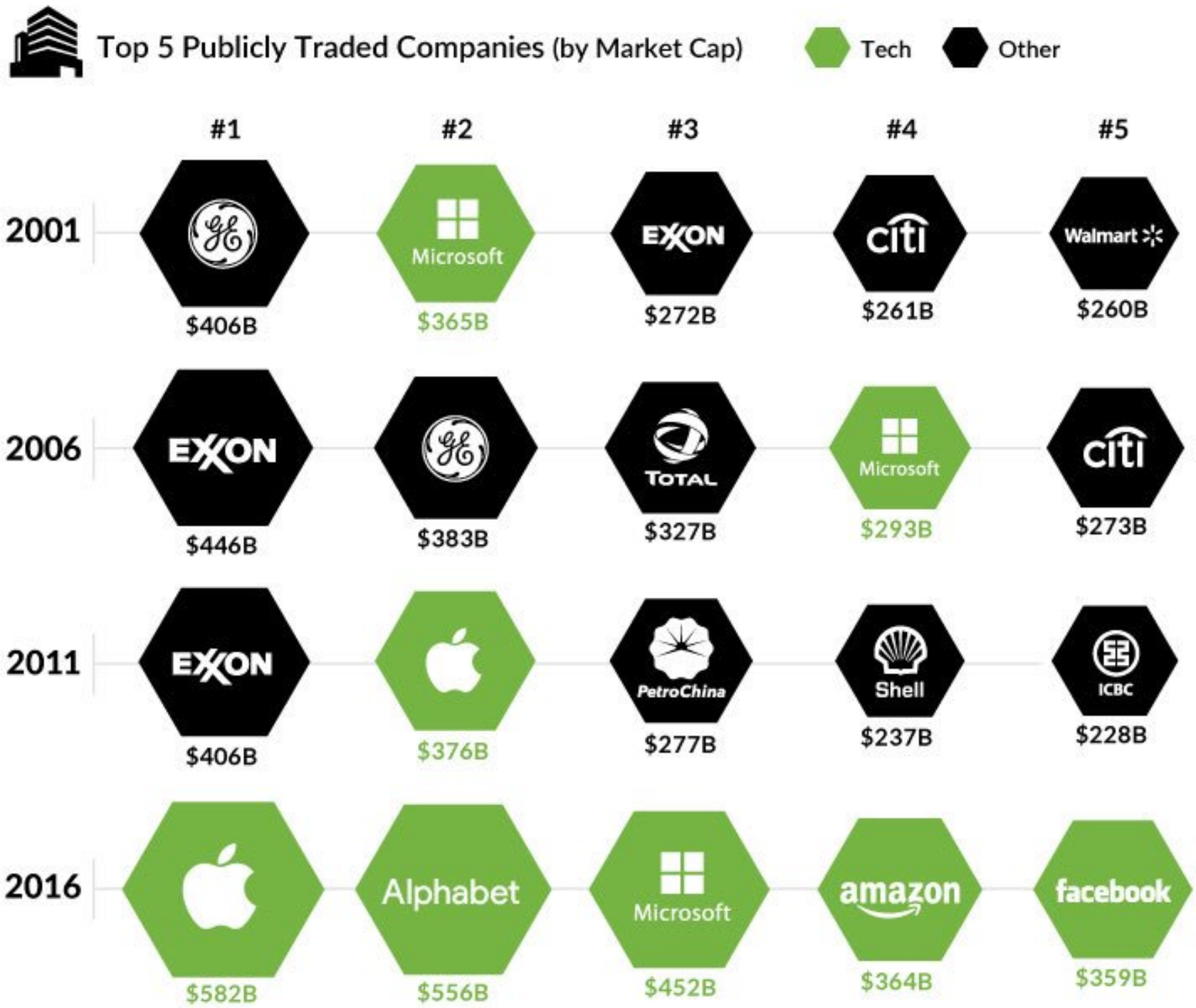
		Digital Signature
Alice → Bob	5.0 BTC	04323784...
Alice → Dave	12 BTC	88432738...
Alice → Juan	2000 BTC	00328434...
Alice → Bob	14 BTC	19382637...

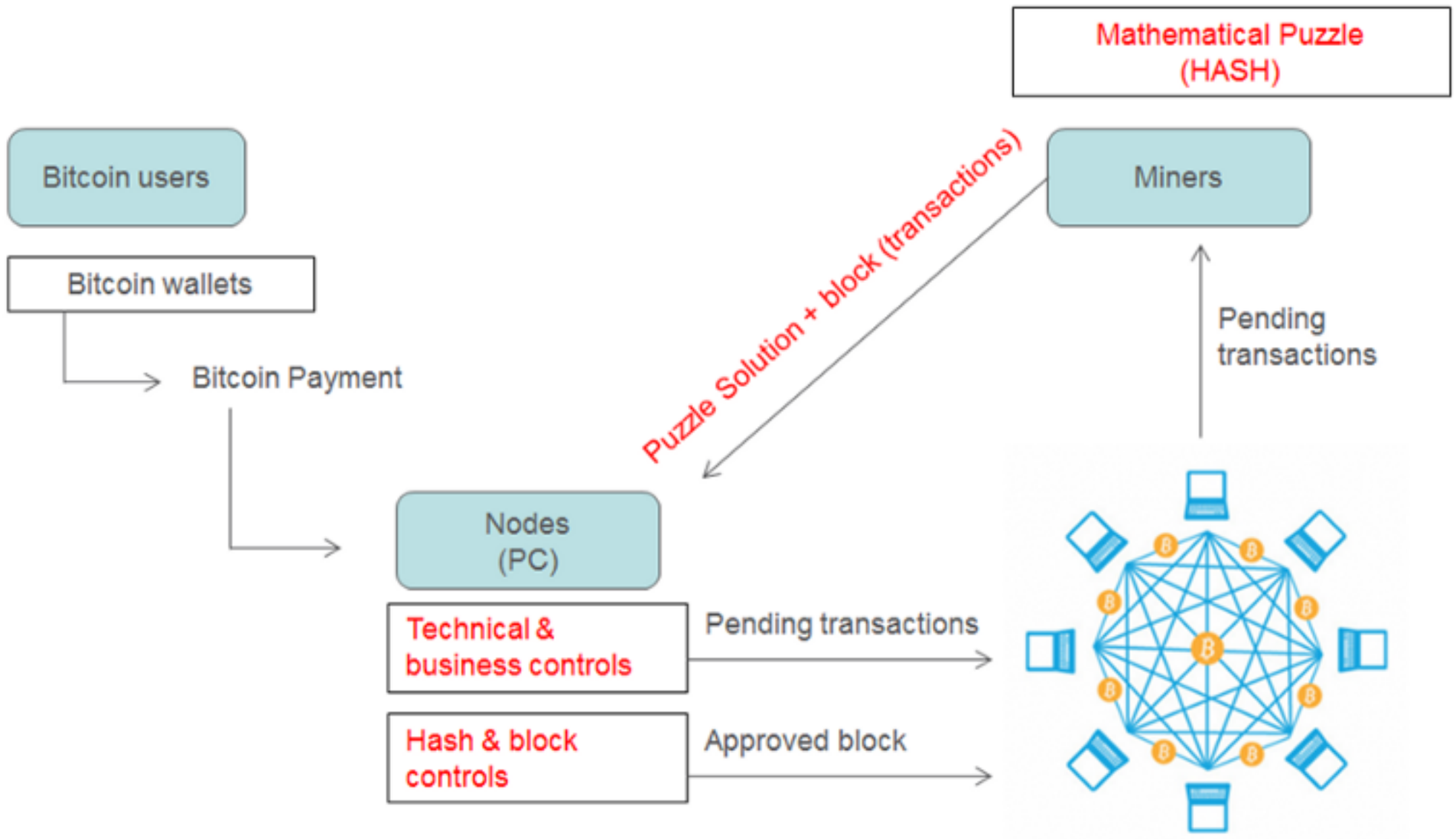
^ different every time

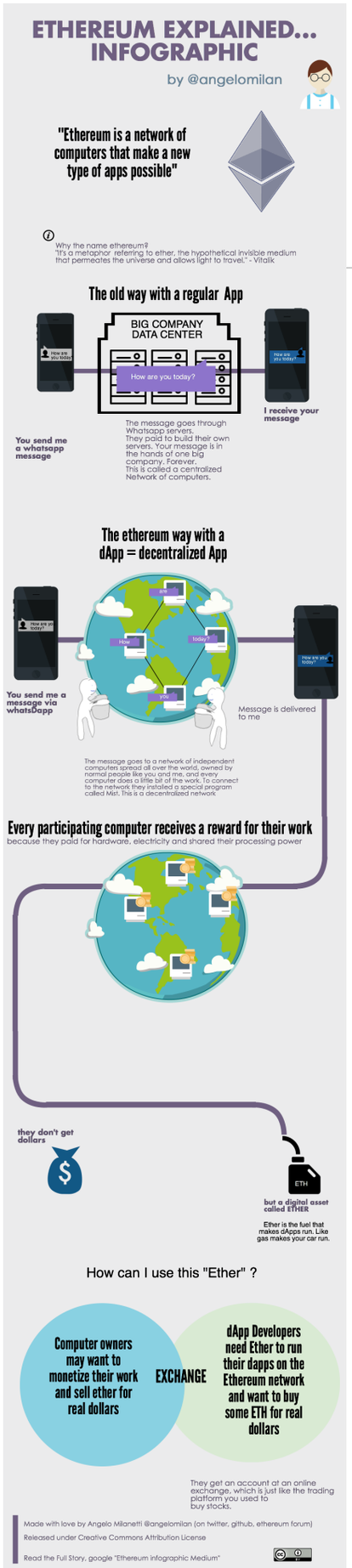


THE LARGEST COMPANIES BY MARKET CAP

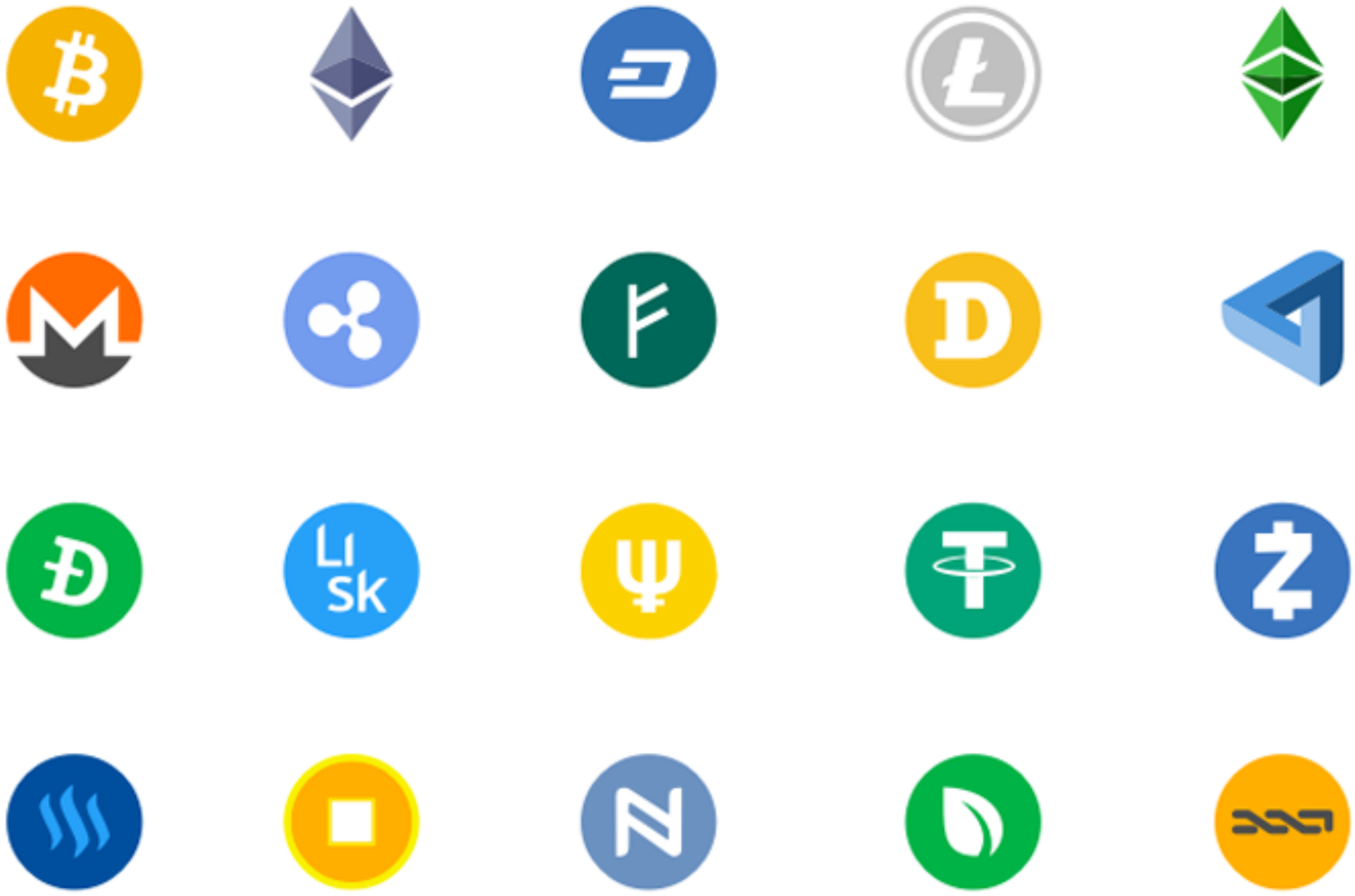
The oil barons have been replaced by the whiz kids of Silicon Valley




Mathematical Puzzle
(HASH)
Bitcoin users
Bitcoin wallets
Bitcoin Payment
Miners
Puzzle Solution + block (transactions)
Pending
transactions
Nodes
(PC)
Technical &
business controls
Pending transactions
Hash & block
controls
Approved block



	Hyperledger Fabric	Ethereum	Ripple	Bitcoin
Description of Platform	General Purpose Blockchain	General Purpose Blockchain	Payments Blockchain	Payments Blockchain
Governance	Linux Foundation	Ethereum Developers	Ripple Labs	Bitcoin Developers
Currency	None	Ether	XRP	BTC
Mining Reward	N/A	Yes	No	Yes
State	Key-value database	Account Data	None	Transaction data
Consensus Network	Pluggable: PBFT	Miniig: Proof of Work	Ripple Protocol	Mining: Proof of Work
Network	Private or Permissioned	Public or Private	Public	Public
Privacy	Open to Private	Open	Open	Open
Smart Contracts	Multiple Programming languages like Java,GO.	Solidity Programming Language	None	Possible, but not obvious



Public

Private

Platform

ethereum

ripple

Blockstream

Blockchains

Software

HYPERLEDGER PROJECT

Digital Asset Holdings

eris

Perceptron

- Popularized by F. Rosenblatt who wrote “Principles of Neurodynamics"
- Still used today
- Simple but limited training procedure
- Single Layer

2009
Satoshi
Nakamoto