Blockchain Technologies: A Tutorial for Engineering Faculty and Researchers

Nitin Kalé and Bhaskar Krishnamachari

Monday, December 4, 2017
10:00am-12:00pm

USC Viterbi
School of Engineering
Center for Cyber-Physical Systems and the Internet of Things
CCI

About Us

Nitin Kalé

Associate Professor of Engineering Practice
Information Technology Program and
Epstein Department of Industrial and Systems Engineering

Viterbi School of Engineering
University of Southern California
Los Angeles

Bhaskar Krishnamachari

Professor
Ming Hsieh Department of Electrical Engineering
Computer Engineering Group
Director of Center for Cyber-Physical Systems and the Internet of Things

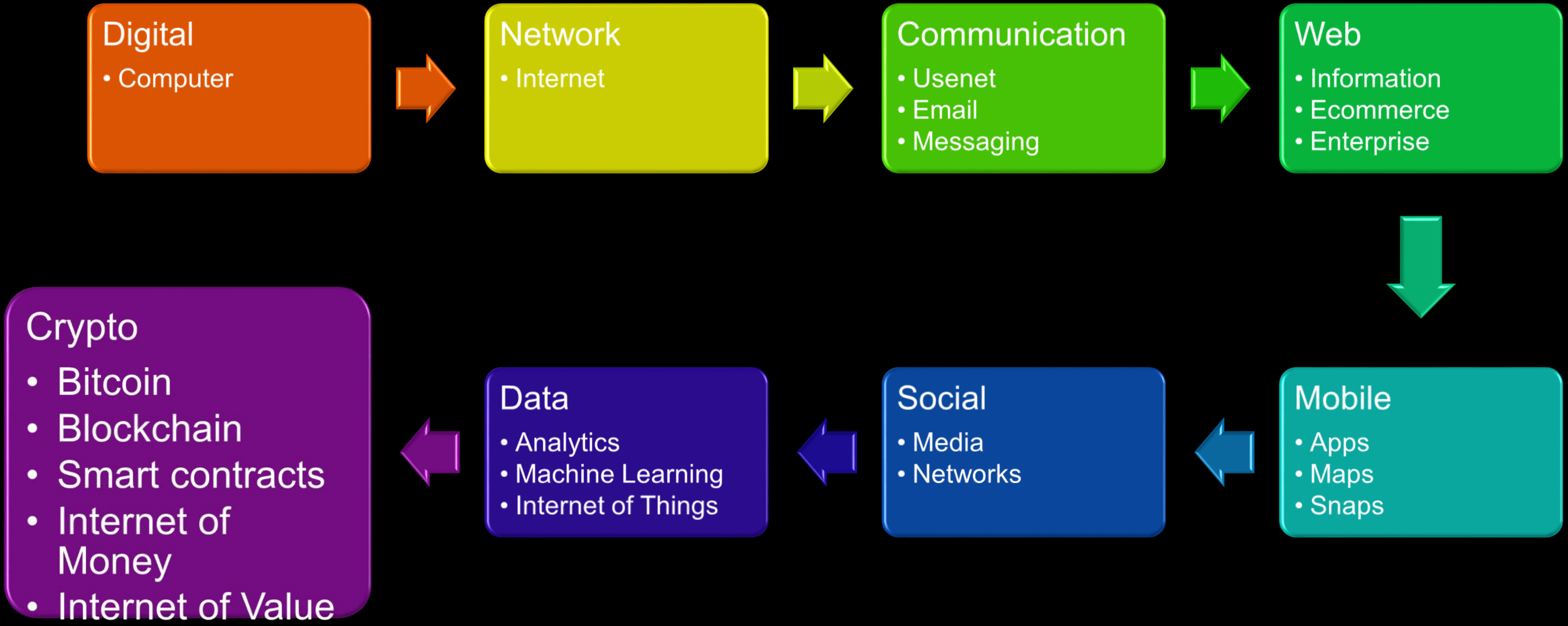
Viterbi School of Engineering
University of Southern California
Los Angeles

Part I

Introduction to Blockchain, Bitcoin and Ethereum

Nitin Kalé

Landmark technological advances



Digital
- Computer

Network
- Internet

Communication
- Usenet
- Email
- Messaging

Web
- Information
- Ecommerce
- Enterprise

Mobile
- Apps
- Maps
- Snaps

Social
- Media
- Networks

Data
- Analytics
- Machine Learning
- Internet of Things

Crypto
- Bitcoin
- Blockchain
- Smart contracts
- Internet of Money
- Internet of Value

Disclaimer (and warning)!

This is a particularly complex workshop (if you are not familiar with blockchain technology)

The more you dig, the more you learn, the more you discover, the more complicated it gets, the more *there is* to learn

Skepticism is natural for something as revolutionary as blockchain

Keep an open mind

There is a lot of tech jargon but those are good to know

You will be thinking about this for days and months to come…It will consume you. I promise. ☺

Do not dabble in bitcoin unless you know what you are doing!

<u>There is no financial advice in this tutorial.</u>

Preliminaries

Reading Assignment

Read this paper first, before you explore blockchain technology https://bitcoin.org/bitcoin.pdf

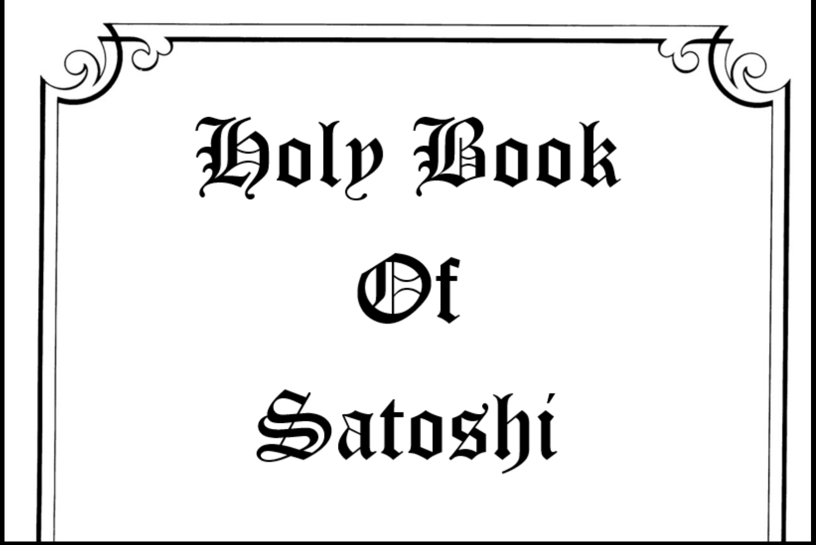
9 pages only (one page is for references)

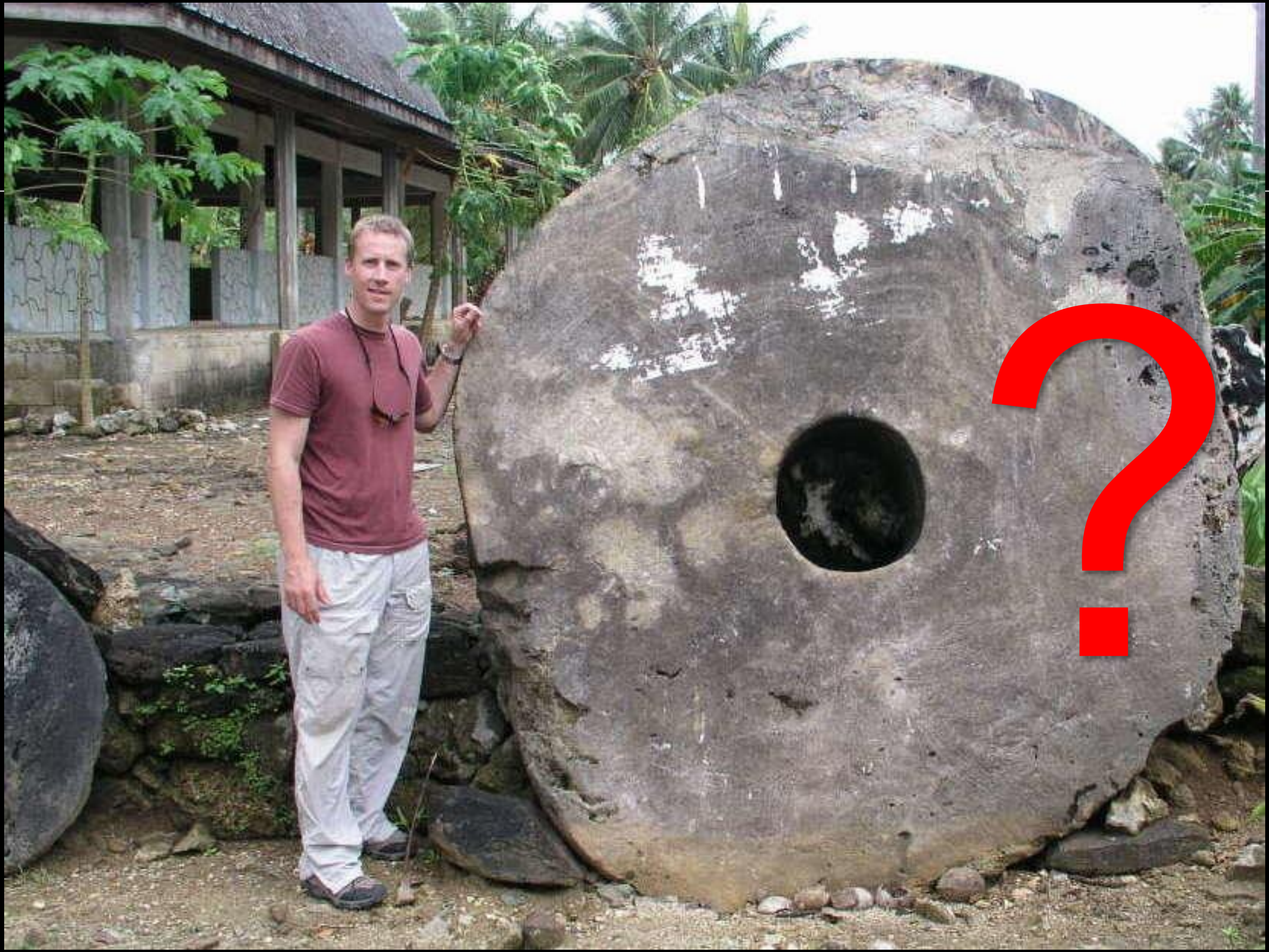
A seminal paper, also referred to as the *Holy Book of Satoshi*

Quite technical but this workshop will cover several of the topics in the paper

Has the potential to change the world (internet → email → web → e-commerce → mobile → social → financial? → blockchain?)

Then read the paper again, and again, and again.





http://www.npr.org/sections/money/2011/02/15/131934618/the-island-of-stone-money

How to “mint” Rai stones

Commission (hire) workers to sail to another island

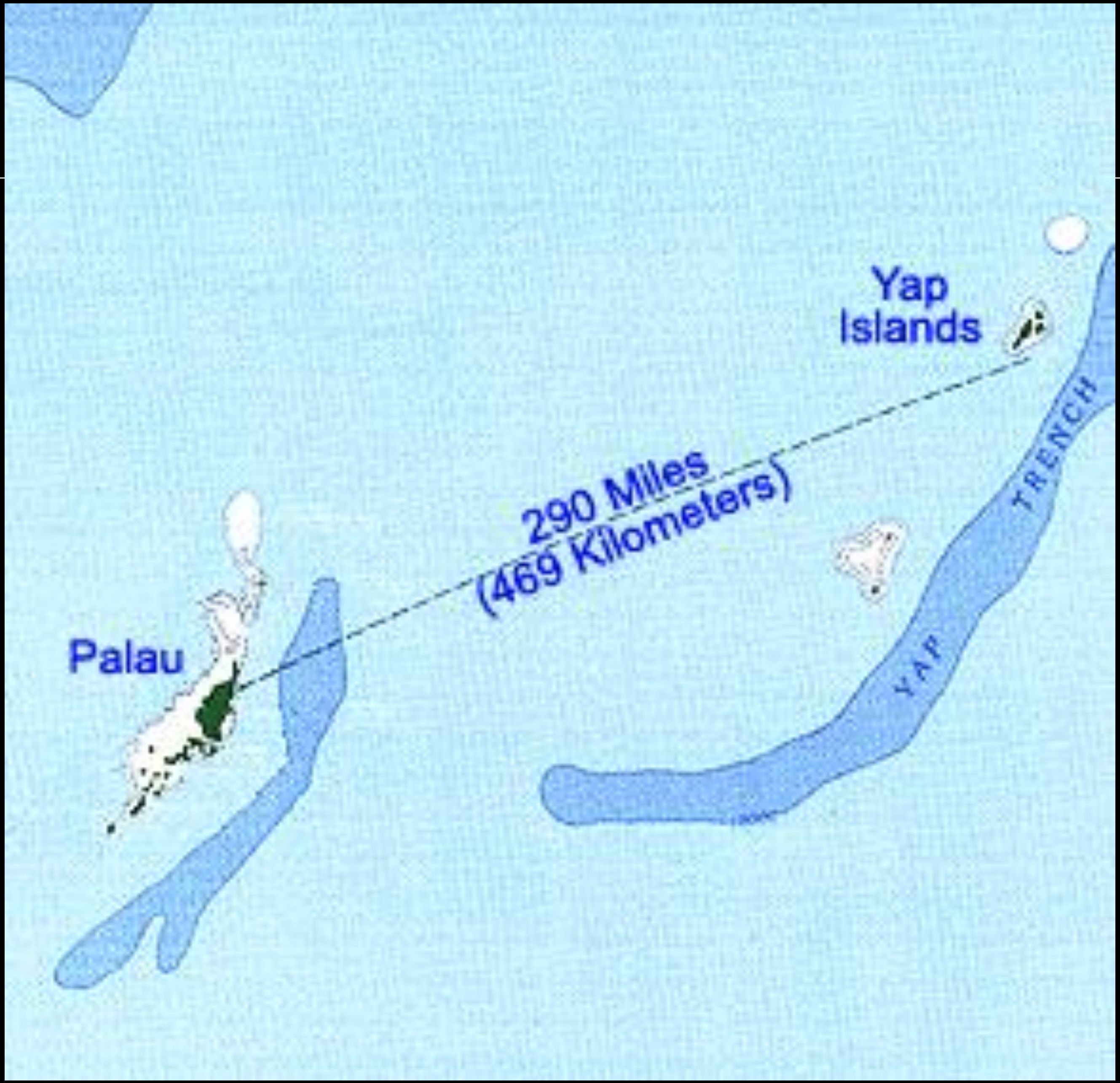
Cooperate with other island’s residents to quarry their limestone

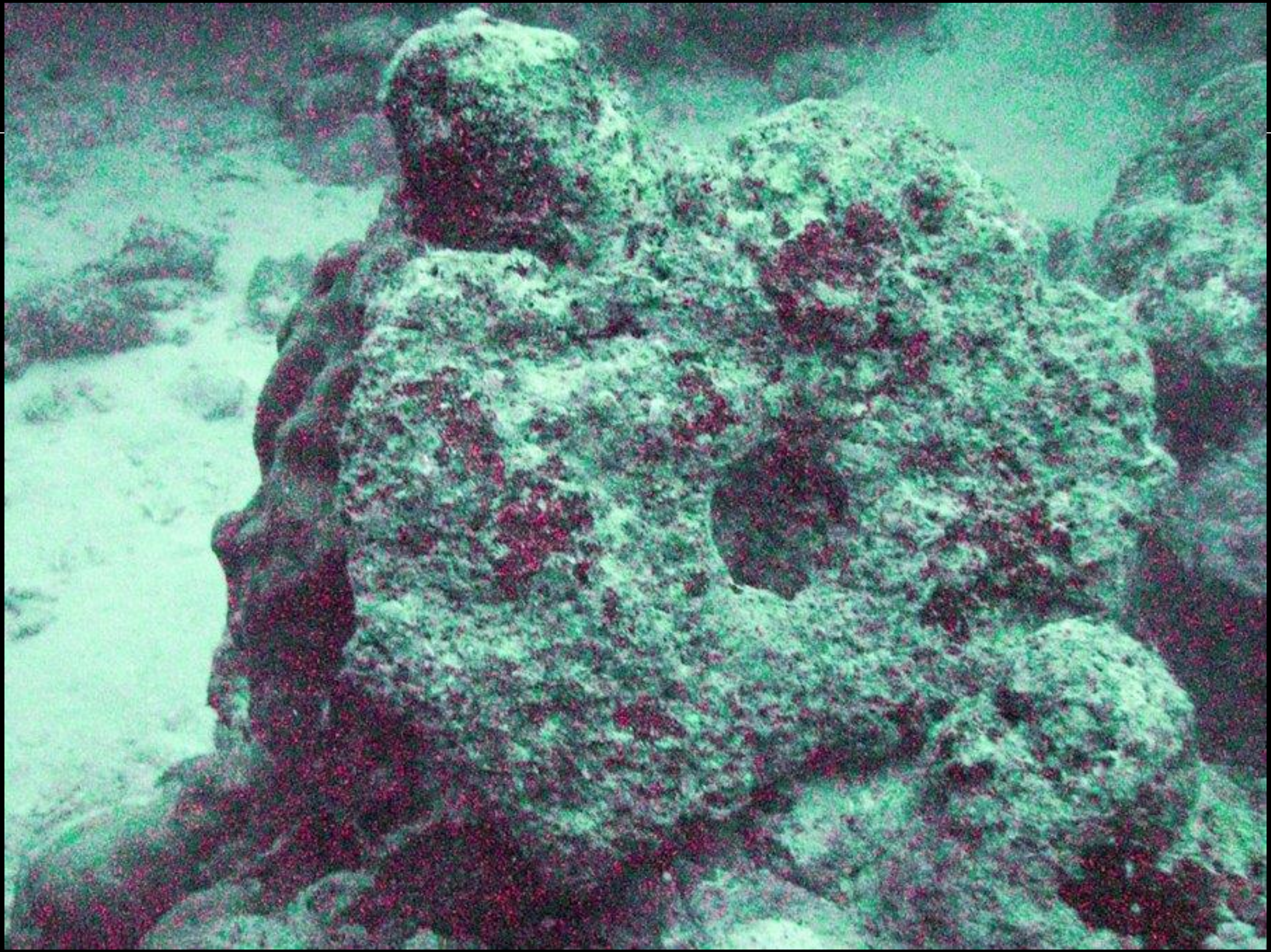
Carve out the stone from limestone

Carry (sail) the stone back to Yap island

Commit the ownership of the stone to the commissioner/owner

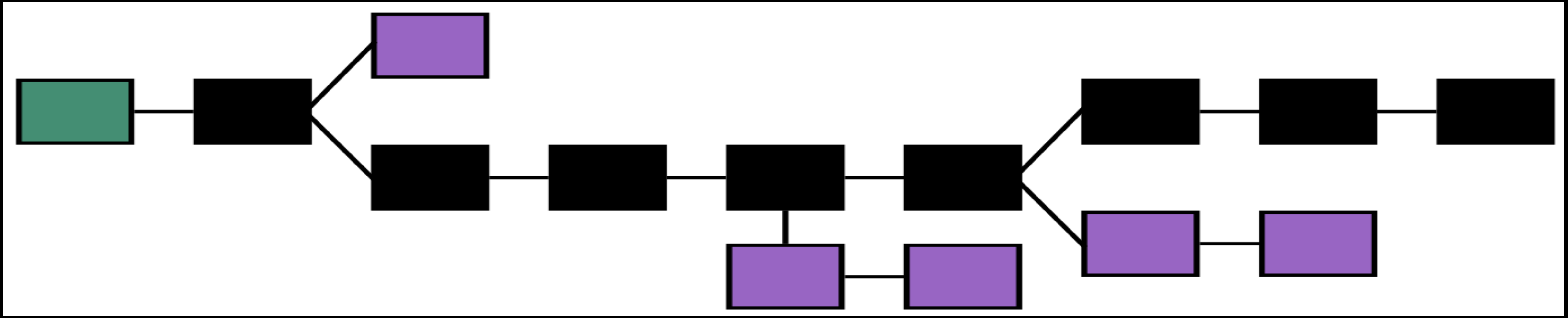
Communicate the record (ledger) of ownership to all


Yap
Islands
290 Miles
(469 Kilometers)
Palau
YAP TRENCH



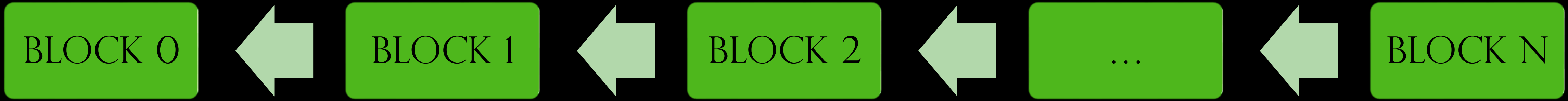
Important Observations about Rai stones

- Scarce
- Difficult to mine (quarry)
- Expend resources to produce money
- Hard to forge (counterfeit)
- Hard to divide (destroy)
- Hard to move (keep a ledger of ownership instead of transferring physical possession)



Blockchain Basics

What is Blockchain?



Technical Definition

A blockchain is a linked list that is built with hash pointers instead of regular pointers.

Socio-political-economic-semi-technical libertarian definition

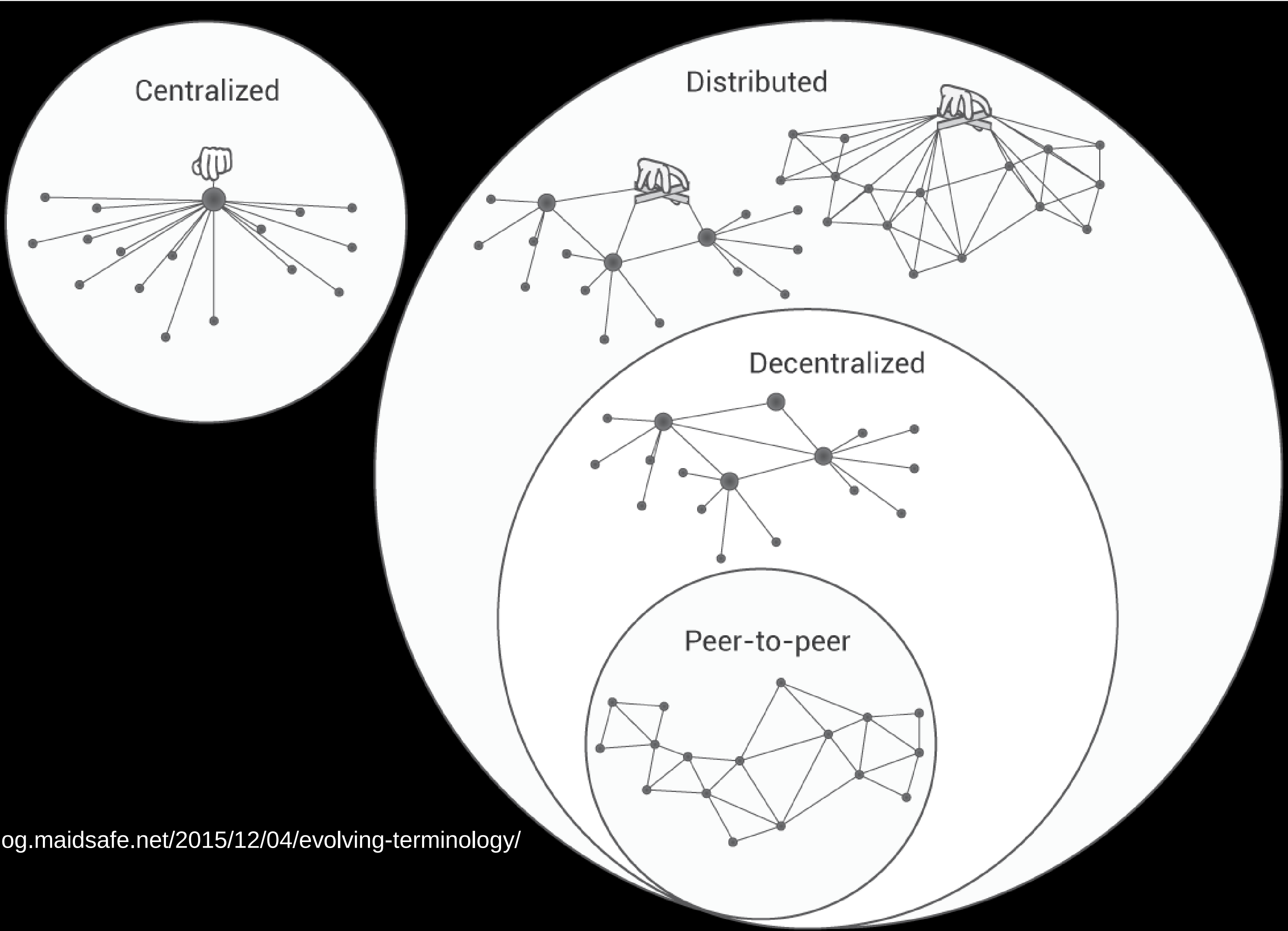
A blockchain is an open*, borderless, decentralized, public, trustless, permissionless, immutable record of transactions

Financial-accounting definition

A blockchain is a public, distributed ledger of peer-to-peer transactions

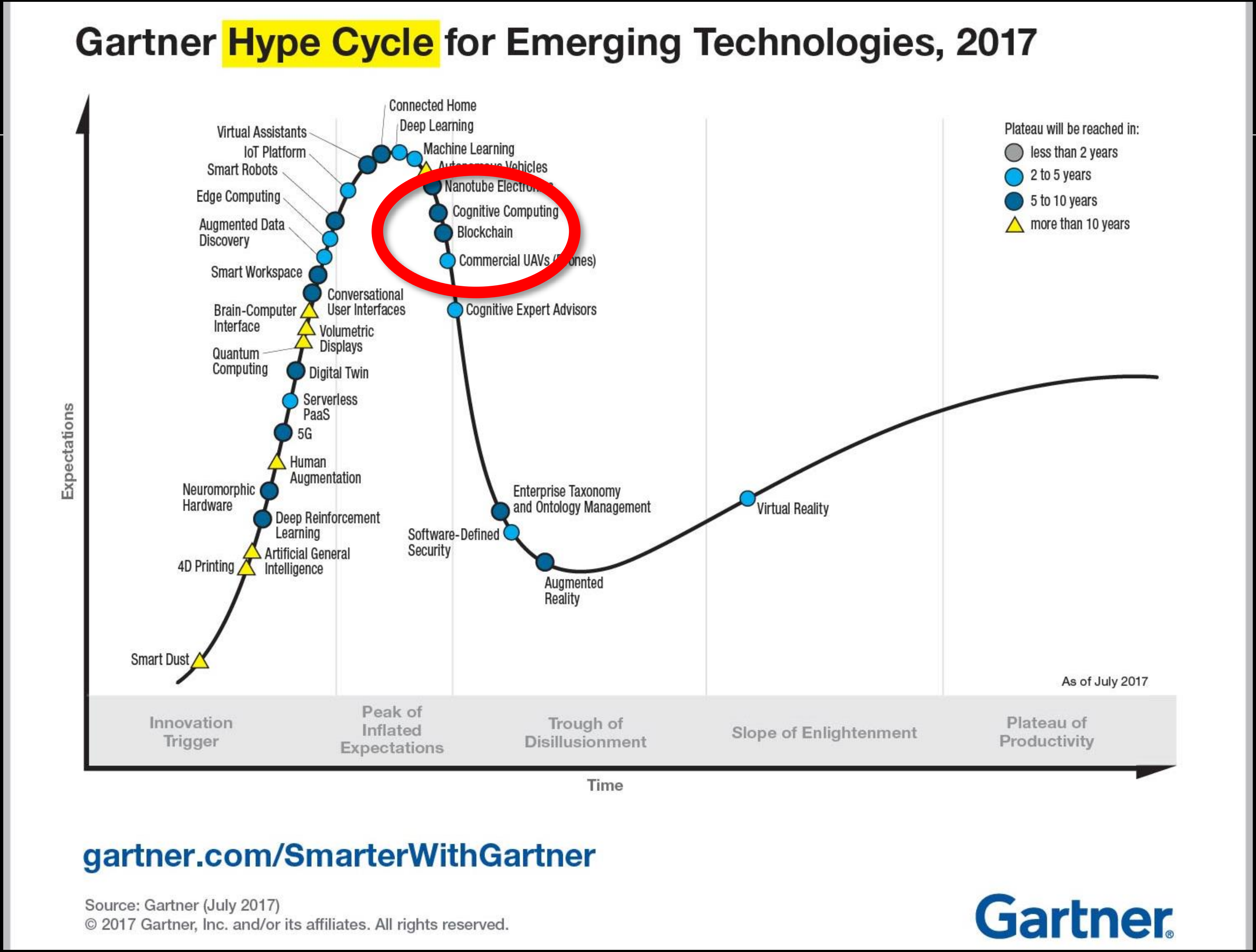
* All terms in red are open to debate

Types of networks (from the viewpoint of control)



https://blog.maidsafe.net/2015/12/04/evolving-terminology/

Hype cycle



Source: Gartner (July 2017)

Why Blockchain?

Enhanced security. Resists hacking by decentralizing the data storage layer. Spread the data thin, make it more difficult to attack. It is easier to attack a single central database than to attack numerous copies of the decentralized database.

Append only. No updates and deletes. Makes it an immutable record of historical facts. Proof of State.

Can be used to store anything of value that can be digitized.

Improves efficiencies in transaction clearing especially when dealing with multiple agencies.

Lowers transaction fees

No central authority means no central trust. The blockchain itself provides digital trust. It is trustless. Disintermediation.

Open and transparent. All transactions in history can be seen, tracked, and validated by anyone.

May become the ultimate proof of value ownership, bypassing governments, corporations, individuals, and criminals.

Provides powerful audit trails.

Some definitions

Ledger

Records transactions

Trustless

No requirement for a trusted intermediary. The trust is in the software/network even when peers are outright malicious.

Cryptographic Identity

Peers assume any number of cryptographic identities. No central authority issues identity.

Immutable

Once committed, data cannot be changed. No updates. Only append.

Consensus

The network uses consensus (some form of agreement) to add data to the blockchain

Censorship resistant

Anyone can join. Transactions/nodes/users cannot be censored so long as they adhere to protocol rules

Distributed/decentralized

- Peer-to-peer network
- No single point of control or failure
- Peers can join and leave as they wish
- Network functions even when peers may be
  - Selfish
  - Competitive
  - Adversarial
  - Malicious

Where is blockchain?

It is decentralized

Nodes on the network hold copies of the blockchain (not all nodes need to have the entire copy)

When a new block is relayed, the other nodes validate it and add it to their blockchain

You can think of it as nodes (participants) each having a copy of the entire database of transactions

Any attempt to tamper with the history of the database will be evident to all other nodes and they will immediately reject the change

All nodes abide by the same consensus rules that govern the creation and validation of transactions. Otherwise other nodes will reject the offending transaction

Proof of State

The blockchain provides a Proof of State:

- Existence: system of record, with timestamp
- Ownership: who owns what
- Integrity: no double spend of digital assets
- Provenance: history of owners
- Traceability: trail of movement

Where is Blockchain?

Explorers for Bitcoin blockchain

- https://blockchain.info/
- https://blockexplorer.com/
- https://www.blocktrail.com/BTC
- http://blockr.io/

You can install the bitcoin blockchain on your own computer

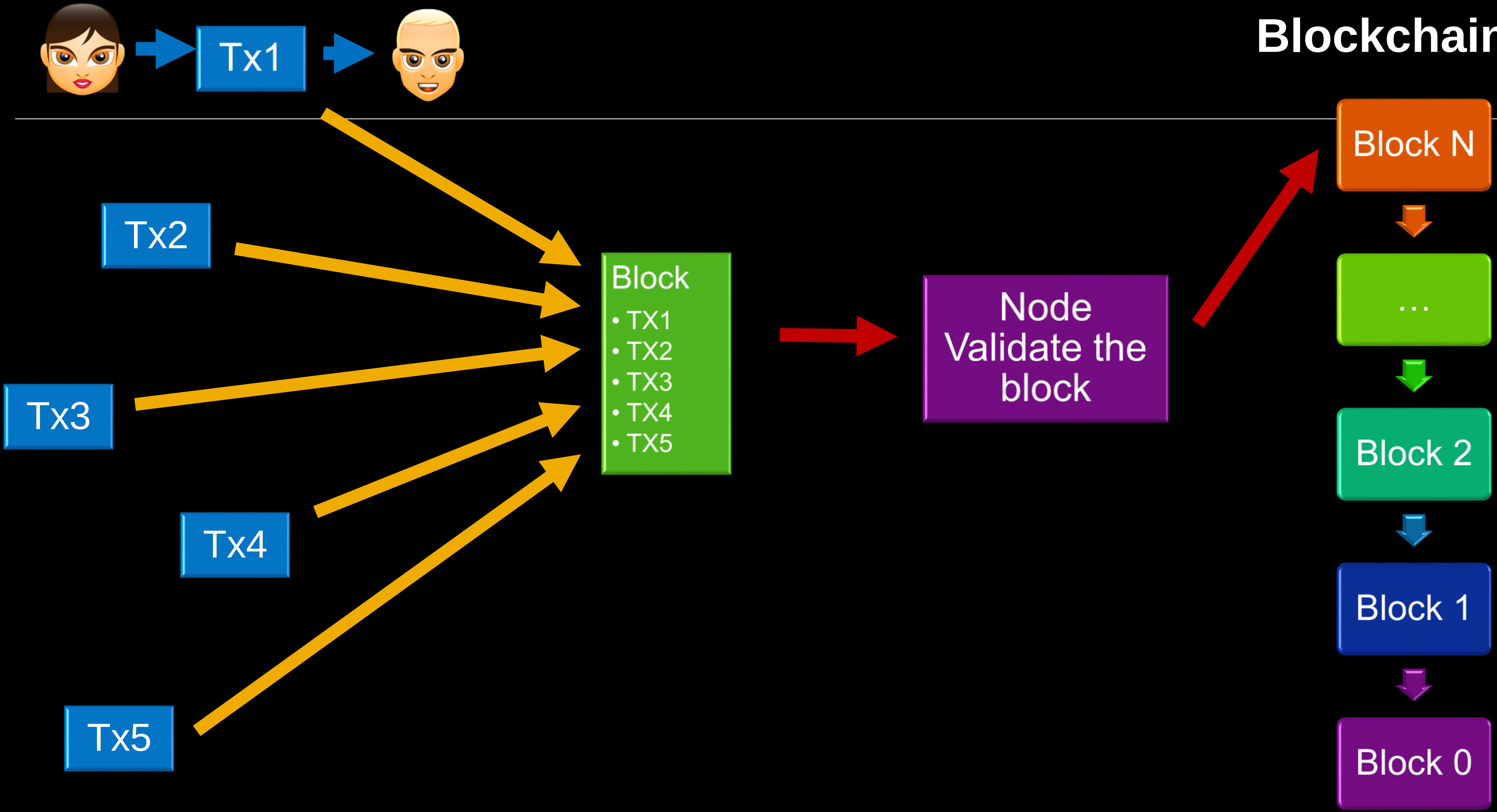
Download and install bitcoin core
https://bitcoin.org/en/download

Then let it gather the bitcoin blockchain. It validates all transaction and blocks (this can take days) in the entire history of bitcoin

The current bitcoin blockchain is over 150GB
https://bitinfocharts.com/

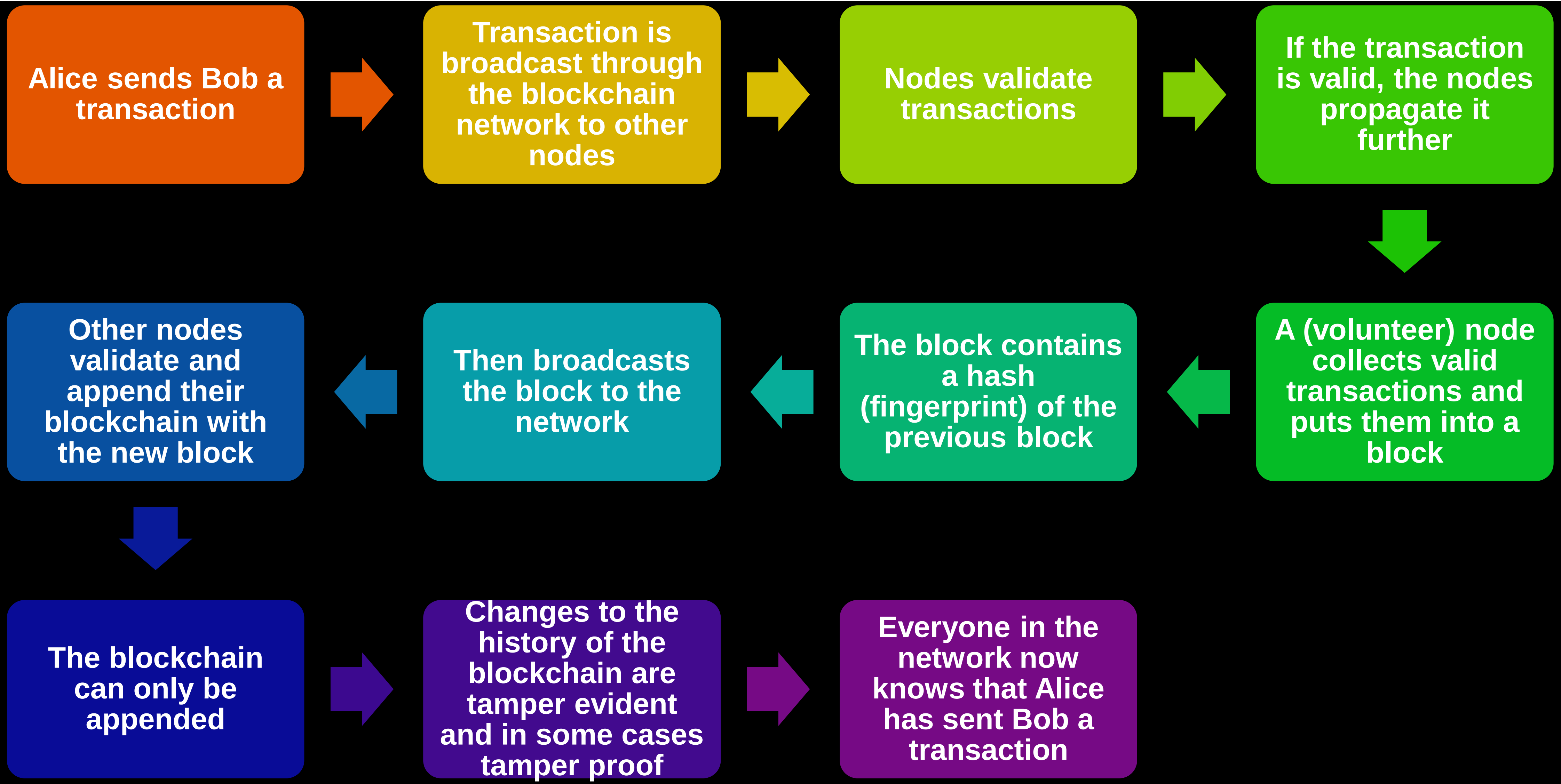
Another option is to install a wallet and let it download the blockchain

Blockchain



Tx1
Tx2
Tx3
Tx4
Tx5
Block
• TX1
• TX2
• TX3
• TX4
• TX5
Node Validate the block
Block N
…
Block 2
Block 1
Block 0

How is a Blockchain built



Alice sends Bob a transaction

Transaction is broadcast through the blockchain network to other nodes

Nodes validate transactions

If the transaction is valid, the nodes propagate it further

A (volunteer) node collects valid transactions and puts them into a block

The block contains a hash (fingerprint) of the previous block

Then broadcasts the block to the network

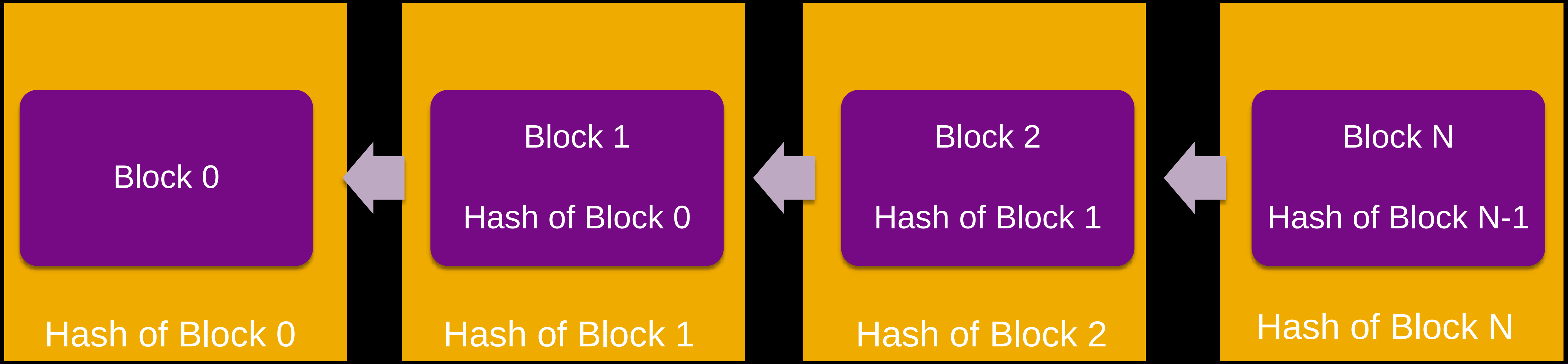
Other nodes validate and append their blockchain with the new block

The blockchain can only be appended

Changes to the history of the blockchain are tamper evident and in some cases tamper proof

Everyone in the network now knows that Alice has sent Bob a transaction

Blockchain structure



Block 0

Hash of Block 0

Block 1

Hash of Block 0

Hash of Block 1

Block 2

Hash of Block 1

Hash of Block 2

Block N

Hash of Block N-1

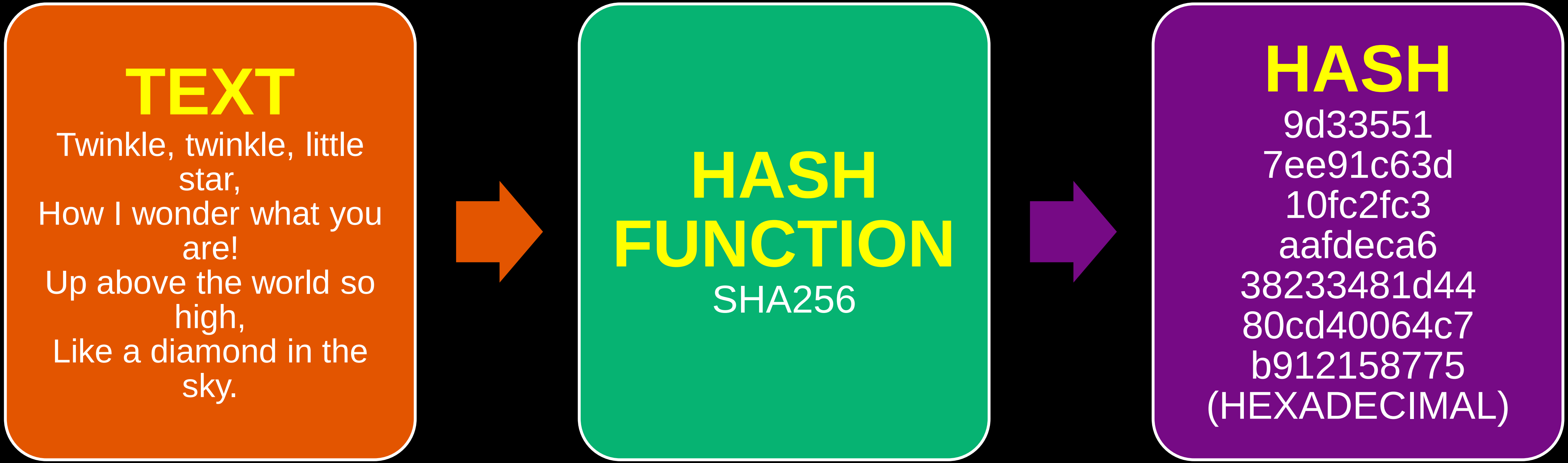
Hash of Block N

Hash ~ Fingerprint

Hashing

Hashing is the conversion of data of *any* size through a hash function into data of fixed size

e.g. SHA256 is one example of hash function (created by NSA). It generates a 256 bit hash of 1s and 0s



TEXT

Twinkle, twinkle, little star,
How I wonder what you are!
Up above the world so high,
Like a diamond in the sky.

HASH FUNCTION

SHA256

HASH

9d33551
7ee91c63d
10fc2fc3
aafdeca6
38233481d44
80cd40064c7
b912158775
(HEXADECIMAL)

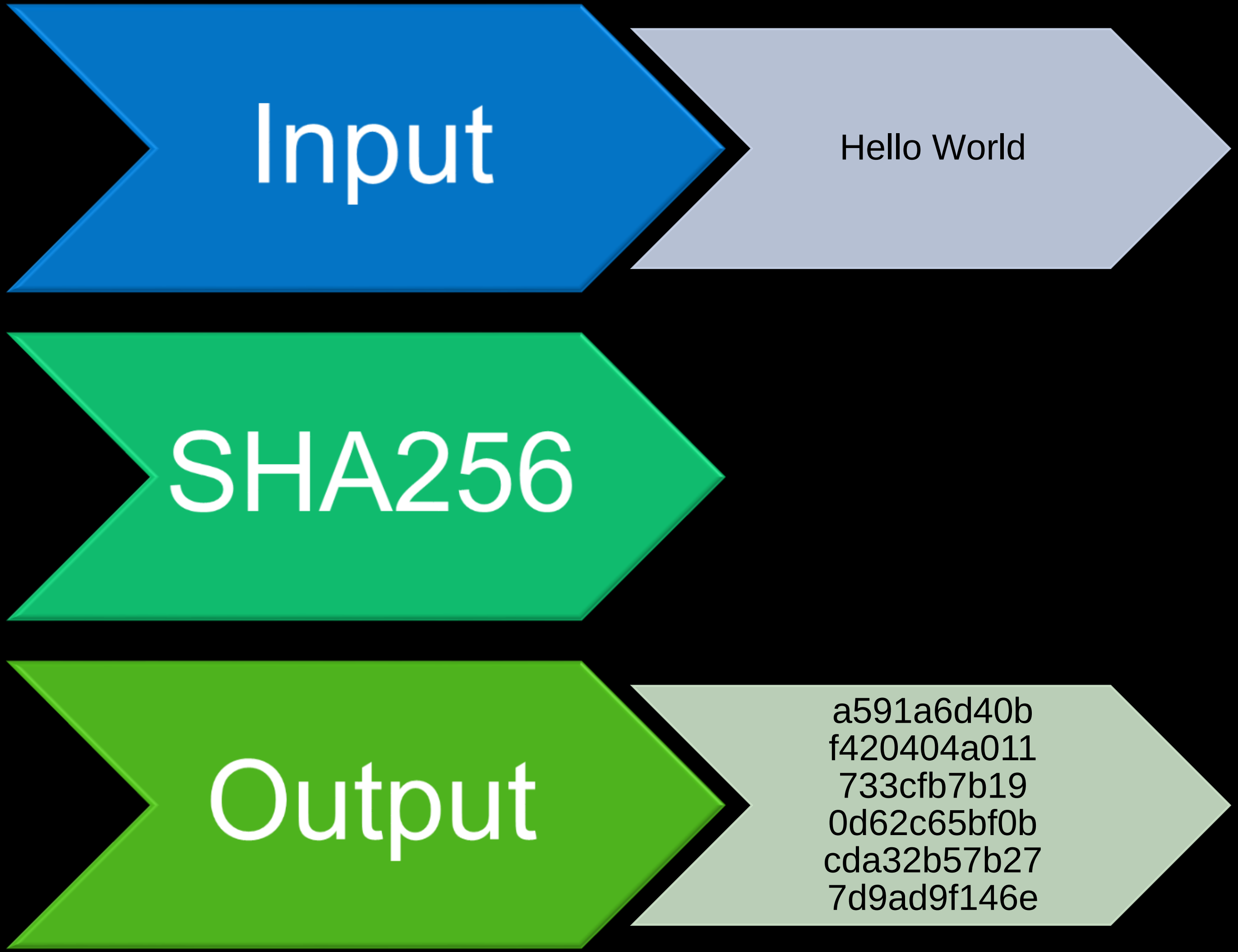
Properties of Hash function

Deterministic – same input yields same output. This can be used to verify that two documents are the same

Non-invertible – Given the hash, one cannot discover the input

Uniform – the probability of a hash value is the same as any other. This helps in creating a puzzle that has no solving strategy except brute force. Big data analytics cannot help here.

Collision resistance – it is infeasible to find two inputs that yield the same hash



Input

Hello World

SHA256

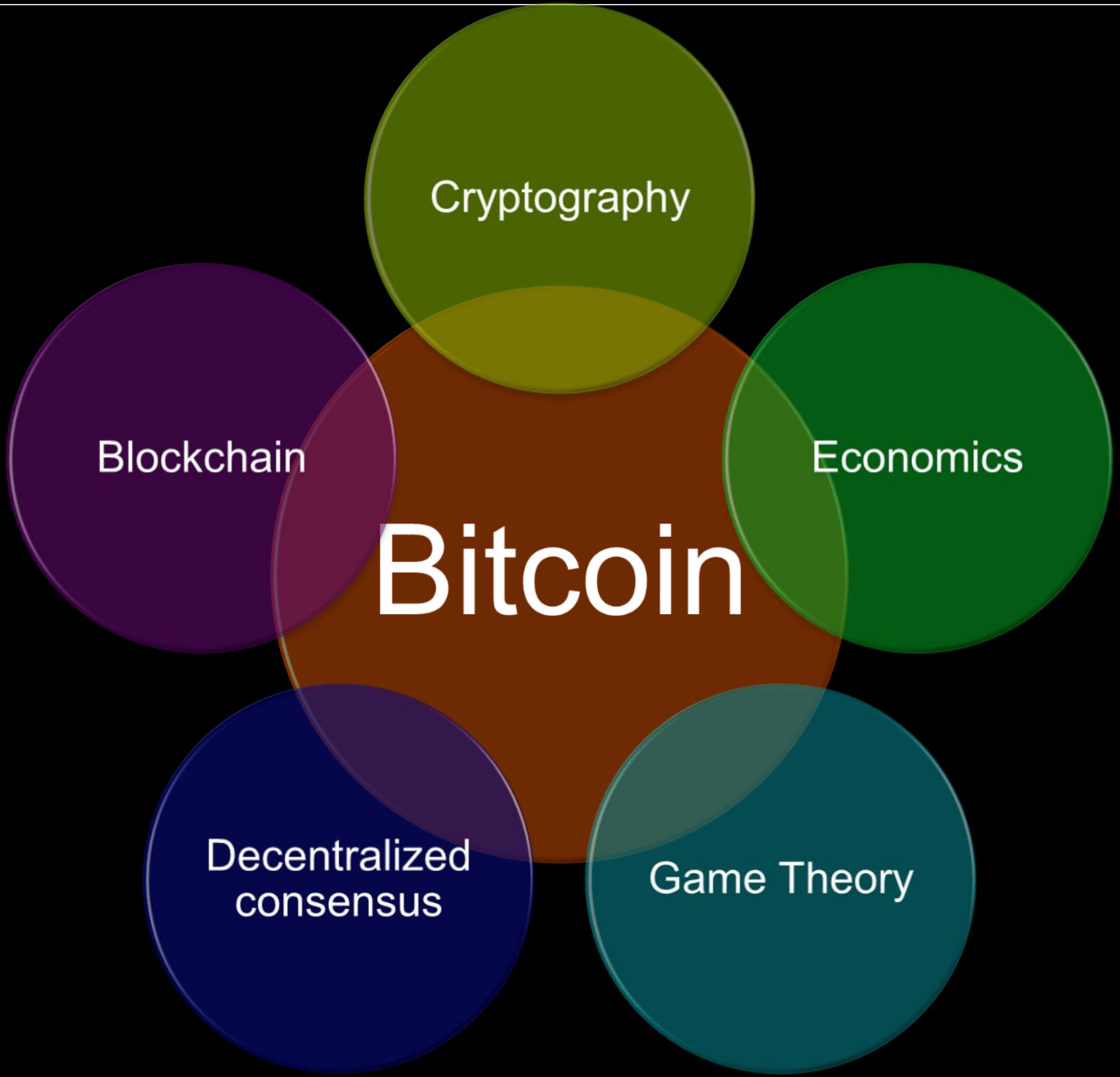
Output

a591a6d40b
f420404a011
733cfb7b19
0d62c65bf0b
cda32b57b27
7d9ad9f146e

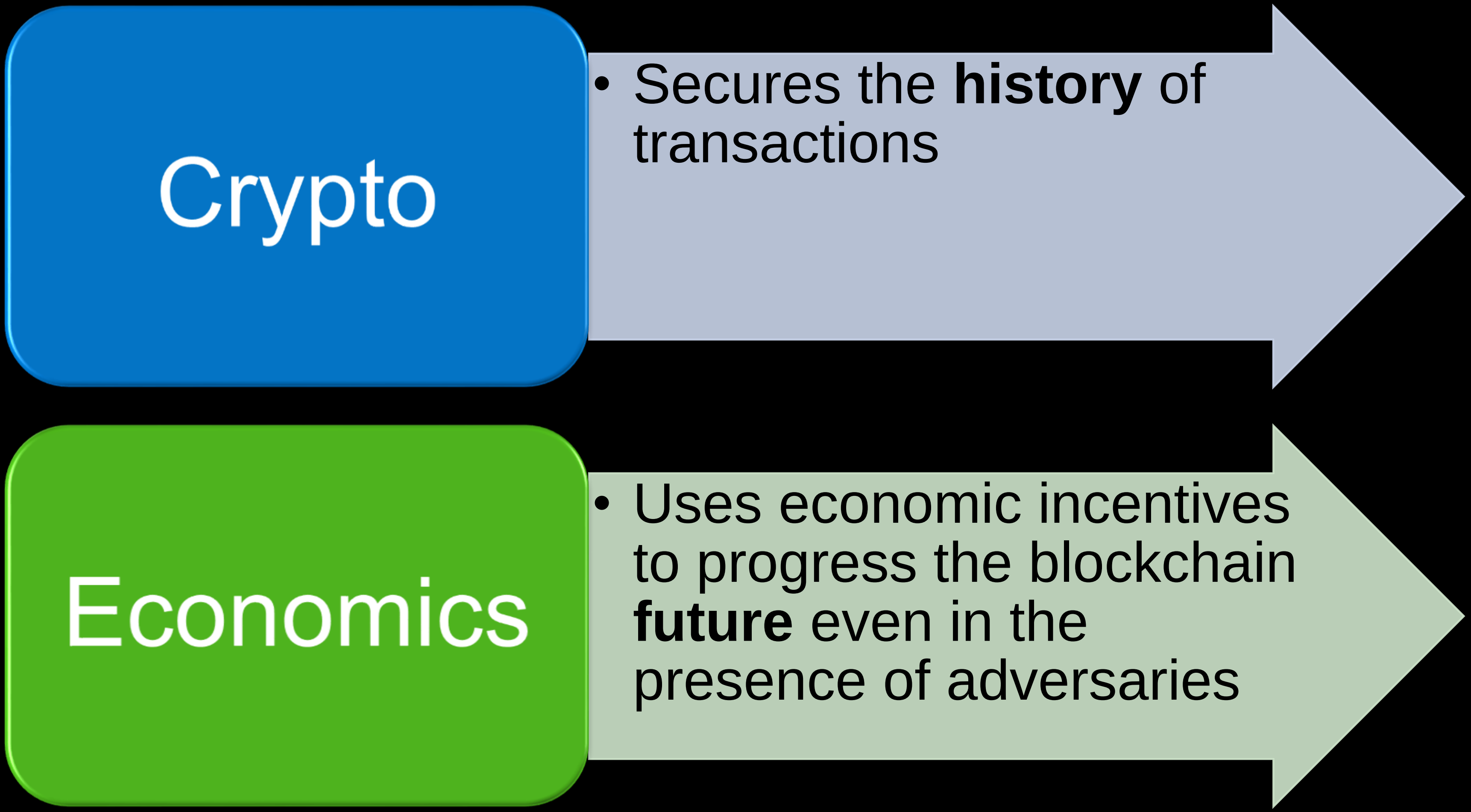
Bitcoin

“In Us We Trust”

Bitcoin is like cake, it is a brilliant invention that combines several ingredients (advances in technology) in a totally unique way



Cryptoeconomics



Crypto

- Secures the **history** of transactions

Economics

- Uses economic incentives to progress the blockchain **future** even in the presence of adversaries

What is Bitcoin?

The online post announcing the white paper that became bitcoin http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Created in Jan 2009 with the first bitcoin being issued (created, mined)

It is described as a cryptocurrency. *Crypto* – secured by advanced cryptography (in the absence of a central trusted authority). *Currency* – a medium of exchange, a system of money.

Created by Satoshi Nakamoto, most likely a pseudonym for a person or persons.

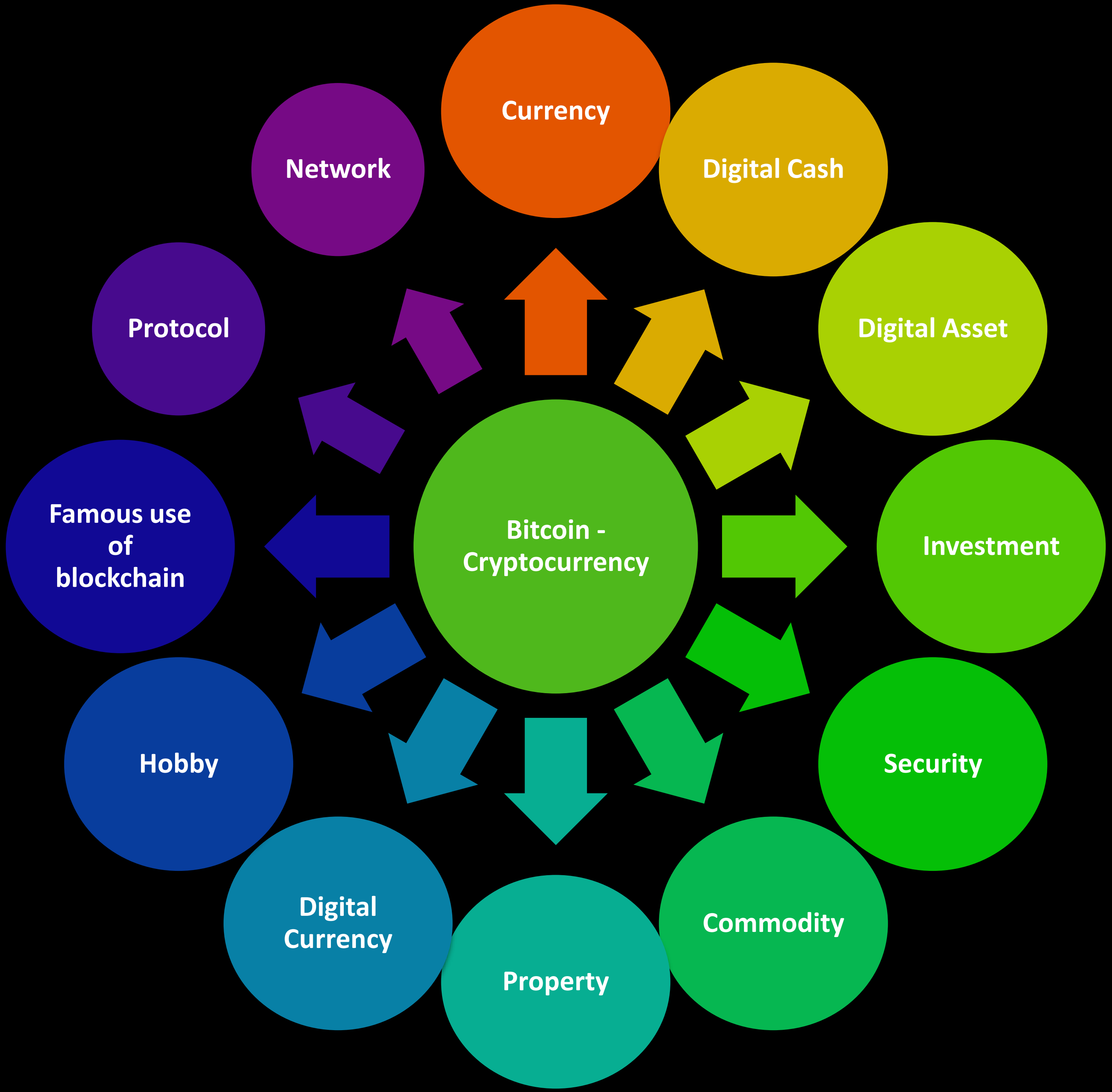
Transact by sending and receiving bitcoins using a public address (like an email address)

Private key is used to unlock and sign bitcoin transactions.

Owner of the private key is the owner of the bitcoin. Possession (of private key) is ownership.

No concept of accounts. Only transactions.

It exists completely digitally. No physical manifestation of bitcoin



Bitcoin - Cryptocurrency

Currency

Digital Cash

Digital Asset

Investment

Security

Commodity

Property

Digital Currency

Hobby

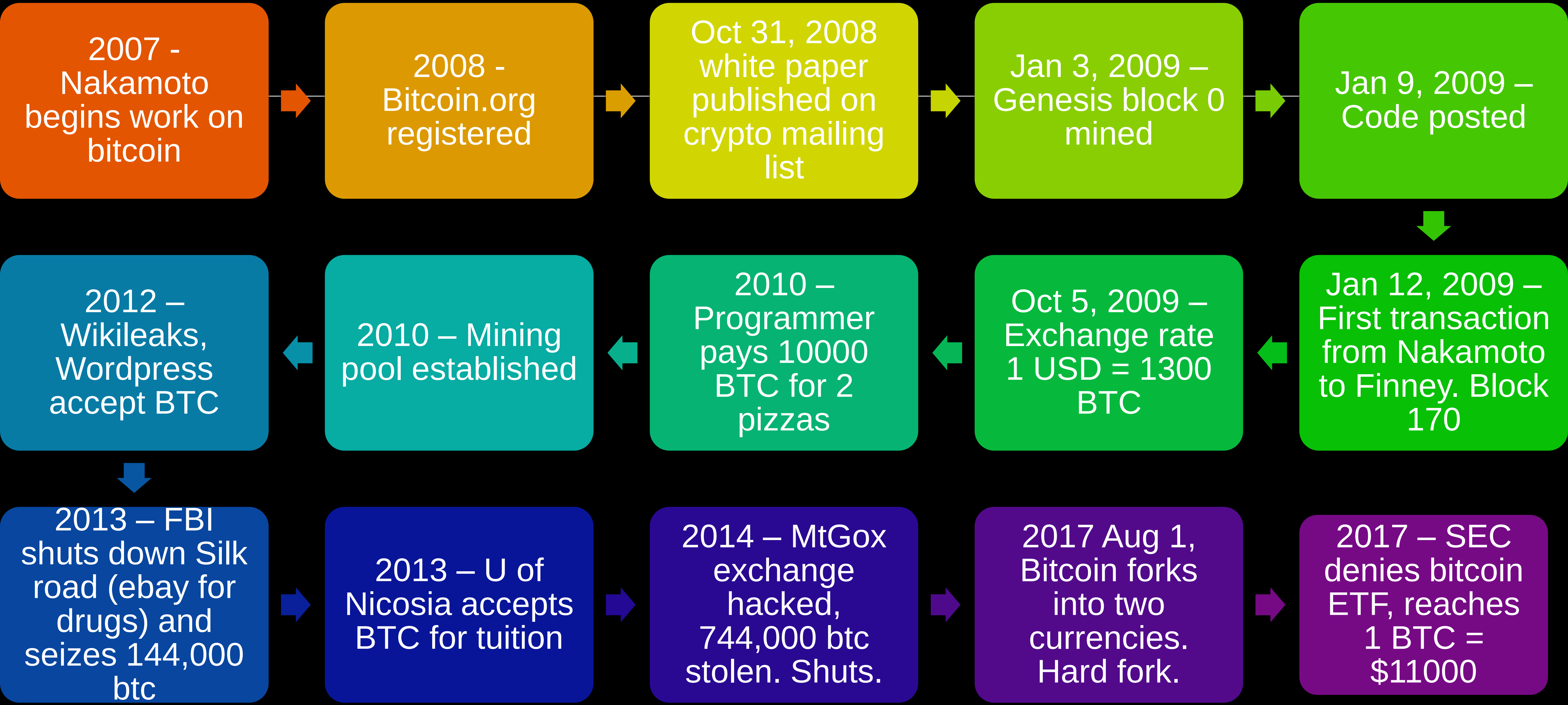
Famous use of blockchain

Protocol

Network

Properties of Bitcoin

- Open
- Fast
- Permissionless
- Pseudonymous
- Secured by cryptography
- Recorded on the public blockchain, tracebility
- Fungibile (?)
- Global
- Decentralized
- Peer-to-peer
- Volatile (fiat)
- Divisible
- Trustless
- No intermediary
- Limited supply



2007 - Nakamoto begins work on bitcoin

2008 - Bitcoin.org registered

Oct 31, 2008 white paper published on crypto mailing list

Jan 3, 2009 – Genesis block 0 mined

Jan 9, 2009 – Code posted

Jan 12, 2009 – First transaction from Nakamoto to Finney. Block 170

Oct 5, 2009 – Exchange rate 1 USD = 1300 BTC

2010 – Programmer pays 10000 BTC for 2 pizzas

2010 – Mining pool established

2012 – Wikileaks, Wordpress accept BTC

2013 – FBI shuts down Silk road (ebay for drugs) and seizes 144,000 btc

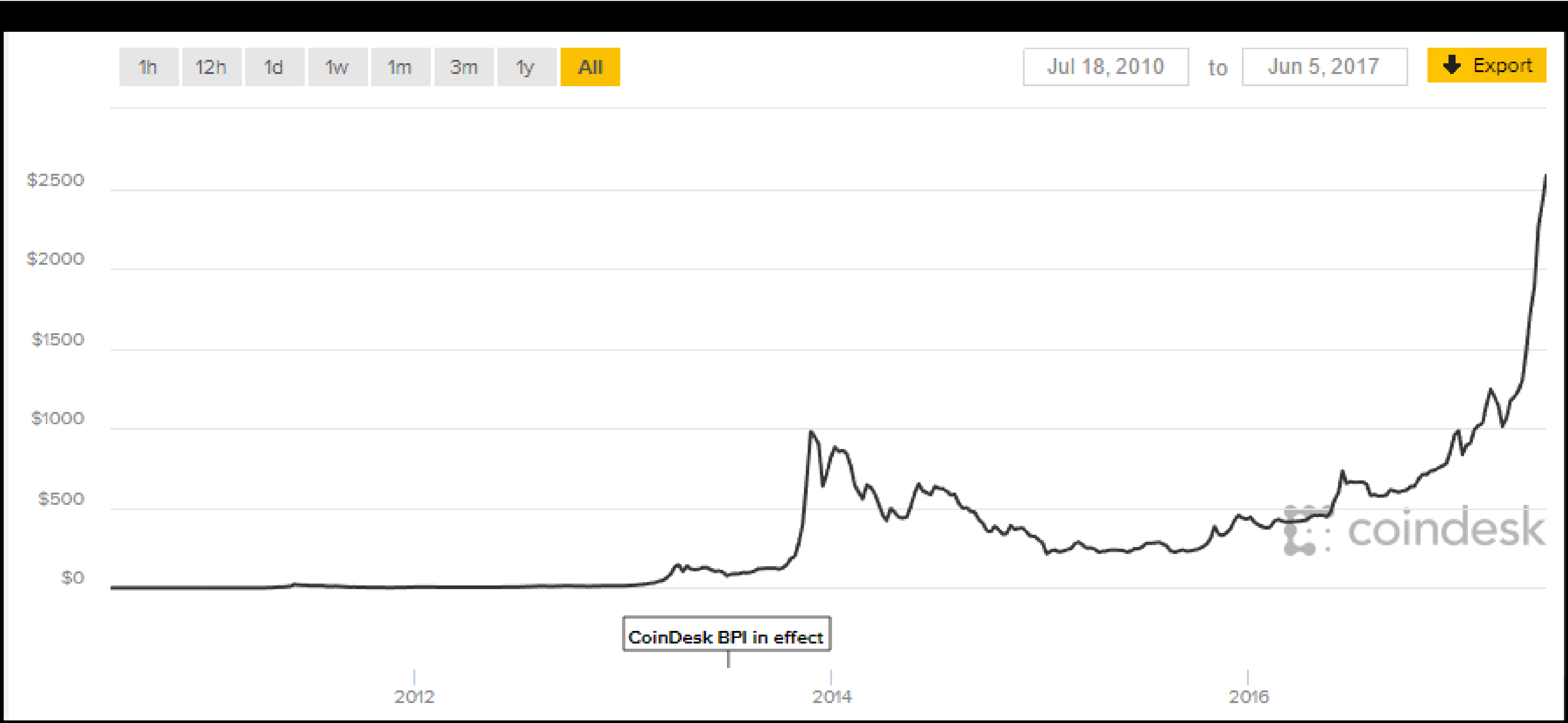
2013 – U of Nicosia accepts BTC for tuition

2014 – MtGox exchange hacked, 744,000 btc stolen. Shuts.

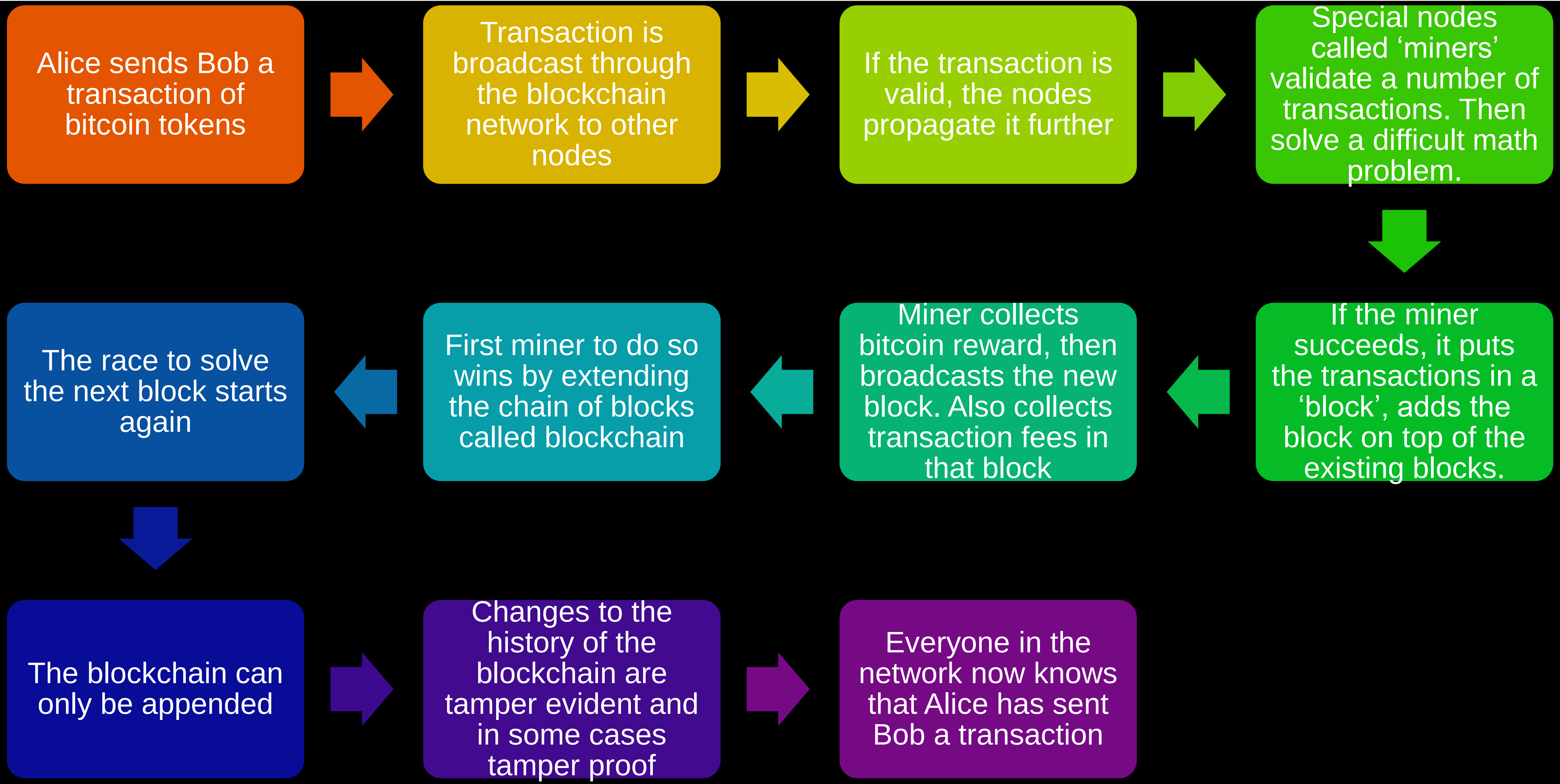
2017 Aug 1, Bitcoin forks into two currencies. Hard fork.

2017 – SEC denies bitcoin ETF, reaches 1 BTC = $11000

Exchange rate with Fiat



How does Bitcoin work



Alice sends Bob a transaction of bitcoin tokens

Transaction is broadcast through the blockchain network to other nodes

If the transaction is valid, the nodes propagate it further

Special nodes called ‘miners’ validate a number of transactions. Then solve a difficult math problem.

If the miner succeeds, it puts the transactions in a ‘block’, adds the block on top of the existing blocks.

Miner collects bitcoin reward, then broadcasts the new block. Also collects transaction fees in that block

First miner to do so wins by extending the chain of blocks called blockchain

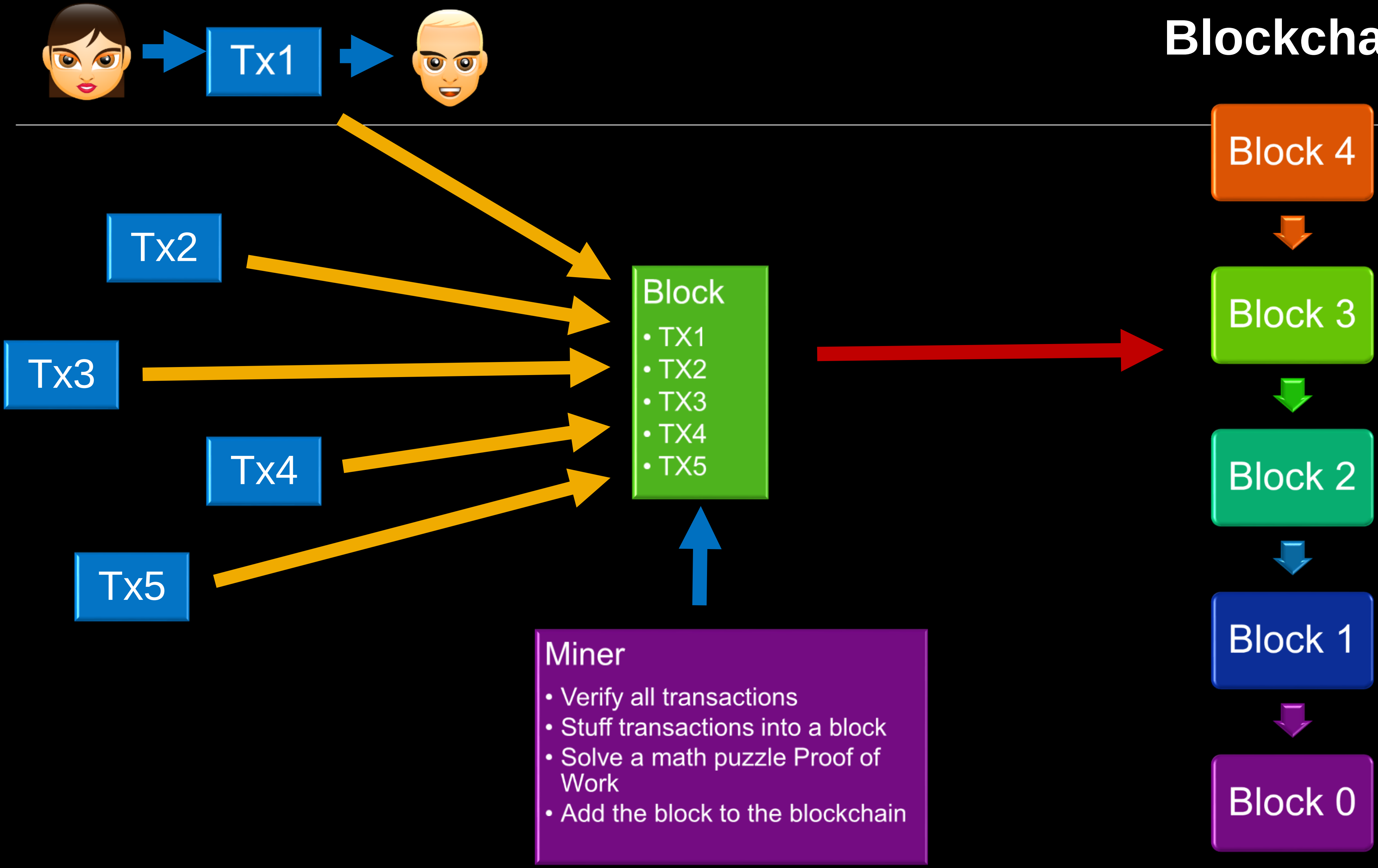
The race to solve the next block starts again

The blockchain can only be appended

Changes to the history of the blockchain are tamper evident and in some cases tamper proof

Everyone in the network now knows that Alice has sent Bob a transaction

Blockchain



Block

- TX1
- TX2
- TX3
- TX4
- TX5

Miner

- Verify all transactions
- Stuff transactions into a block
- Solve a math puzzle Proof of Work
- Add the block to the blockchain

Cost of transactions

Transaction fees are paid by the sender and are voluntary

Transactions are broadcast to the entire bitcoin network but are only confirmed when it is included in a block

The fees are collected by the miner who mines the block in which the transaction is included

The sender can incentivize the miner to include their block by including higher transaction fee

A low fee transaction may have to wait for several blocks before it is included into to a block by a miner

As mining reward reduces and bitcoin participation increases, the transaction fees will be the majority incentive for miners

Divisibility (granularity)

1 Bitcoin is (currently) divisible to eight decimal places.

1 bitcoin = 100,000,000 satoshis

With over 16 million bitcoins mined so far, that is 1,600,000,000,000,000 = 1.6 quadrillion satoshis. The value of a satoshi will adjust to accommodate the bitcoin economy (just as other fiat currencies).

A transaction can send any amount of bitcoin (no upper or lower limit)

Bitcoin monetary system

Bitcoin has a limited supply of money (21 million is the max, to be mined over time).

The amount of bitcoin that can be created out of nothing is limited and controlled by software.

The amount of bitcoin in circulation is equal to or less than that which has been mined (some bitcoins are lost or destroyed accidentally).

HOWEVER, there is nothing to keep a bitcoin exchange from behaving like a traditional bank and lend IOU ‘bitcoin’ to customers with a promise of withdrawal on demand.

BUT, the monetary base of bitcoin is controlled and predictable.

Bitcoin Supply and asymptote

When a miner “mines” (discovers) a block, it gets a block reward in BTC. In 2009, the award was 50 BTC. It is 12.5 bitcoin now. The miner also collects all of the *transaction fees* for the block they mined.

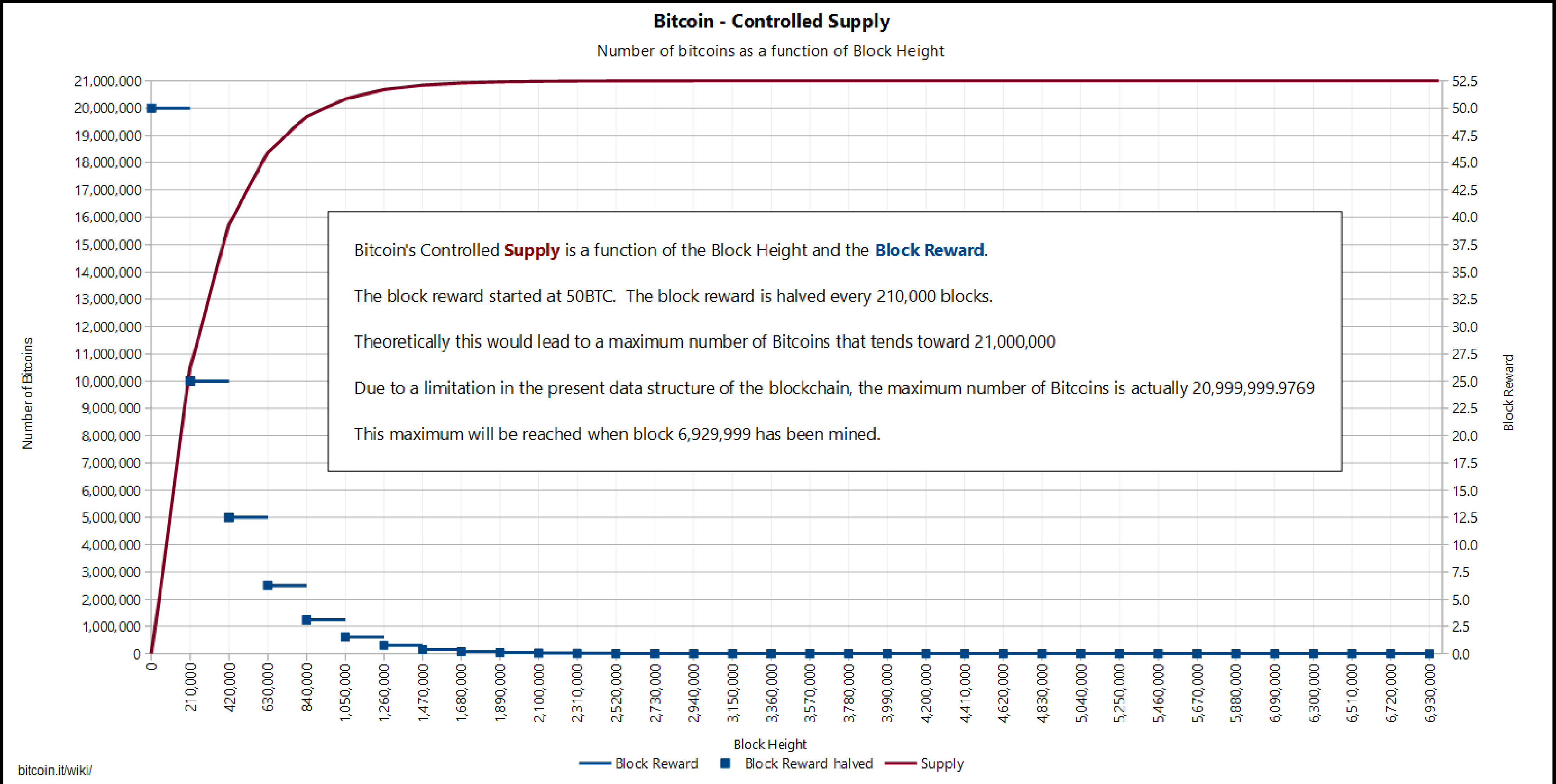
A block is mined every 10 mins on average.

Every 210000 blocks, the reward is halved to slowly diminish the reward and therefore limit the total supply of bitcoins.

Because this geometric series halves every 4 years, it has an asymptote of 21 million bitcoin. The last bitcoin will be mined in approx. in the year 2140

https://plot.ly/~BashCo/5.embed?share_key=ljQVkaTiHXjX2W41UiqzCn

As usage gets wide spread, the cryptocurrency appreciates in value. It is a deflationary currency!



Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height

Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png

Mining

Nodes can become miners. This is what they do:

1. **Listen to transactions on the bitcoin network**
2. **Keep the current version of the blockchain**
3. **Validate transactions, assemble them into a block. Include a reward for yourself (that transaction is called coinbase)**
4. **Hash the block header with a nonce until the hash meets a target difficulty**
5. **Broadcast the block you have mined to the network.**
6. **Hope the network accepts your block. Then you can spend the block reward after 100 blocks**

Proof of Work

A proof-of-work (POW) system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. (Wikipedia)

Bitcoin uses Hashcash PoW

In Bitcoin, the PoW is difficult (costly) to produce but easy to verify by others. It is a random process with very low (adjustable) probability (search within a uniform distribution, needle in a haystack)

The Great Pyramid of Giza – 5,000,000,000 KGs

Proof of work

The Proof of Work is a brute force search for nonces so that the hash of the block header meets a certain target difficulty.

By expending resources (hardware, electricity, cooling) miners race to solve the hashing puzzle. The winner claims the bitcoin reward by announcing that they have performed the Proof of Work

The cumulative Proof of Work in the blockchain is what secures the blockchain and makes it tamper proof and immutable

Current mining activity https://blockchain.info/charts/hash-rate

The target difficulty adjusts approx. every two weeks to reflect the total hashing power and the average time to mine the block to be 10 minutes

How to acquire bitcoin*

Mine it yourself (impractical)

Join a mining pool

Buy it on an exchange with fiat currency

Offer your services

Use a BTM (bitcoin ATM)

On the street. Trade using localbitcoins.com (face to face)

*** ALL have pros and cons. Beware!!***

Storing and using bitcoin

One feature (goal?) of bitcoin is that a user is their own bank (in the absence of intermediaries)

The disintermediation puts the responsibility of storing, using and protecting bitcoin solely in the hand of the user

Wallets are used to store bitcoin

To send bitcoin, use your wallet to find unspent transactions and then use a public address of the received to send bitcoin

The wallet keeps track of balances (no account)

Ethereum

Proposed by Vitalik Buterin in 2013 (when he was 19 years old)

A decentralized network to run smart contracts (software)

A more technical definition – Ethereum is a distributed state machine (a global computer) with no single point of control.

Compare this definition to the standard client/server architecture.

So computers in this decentralized network run your program instead of a central (trusted) server.

Ether is the currency to pay for your contract to be executed on the blockchain

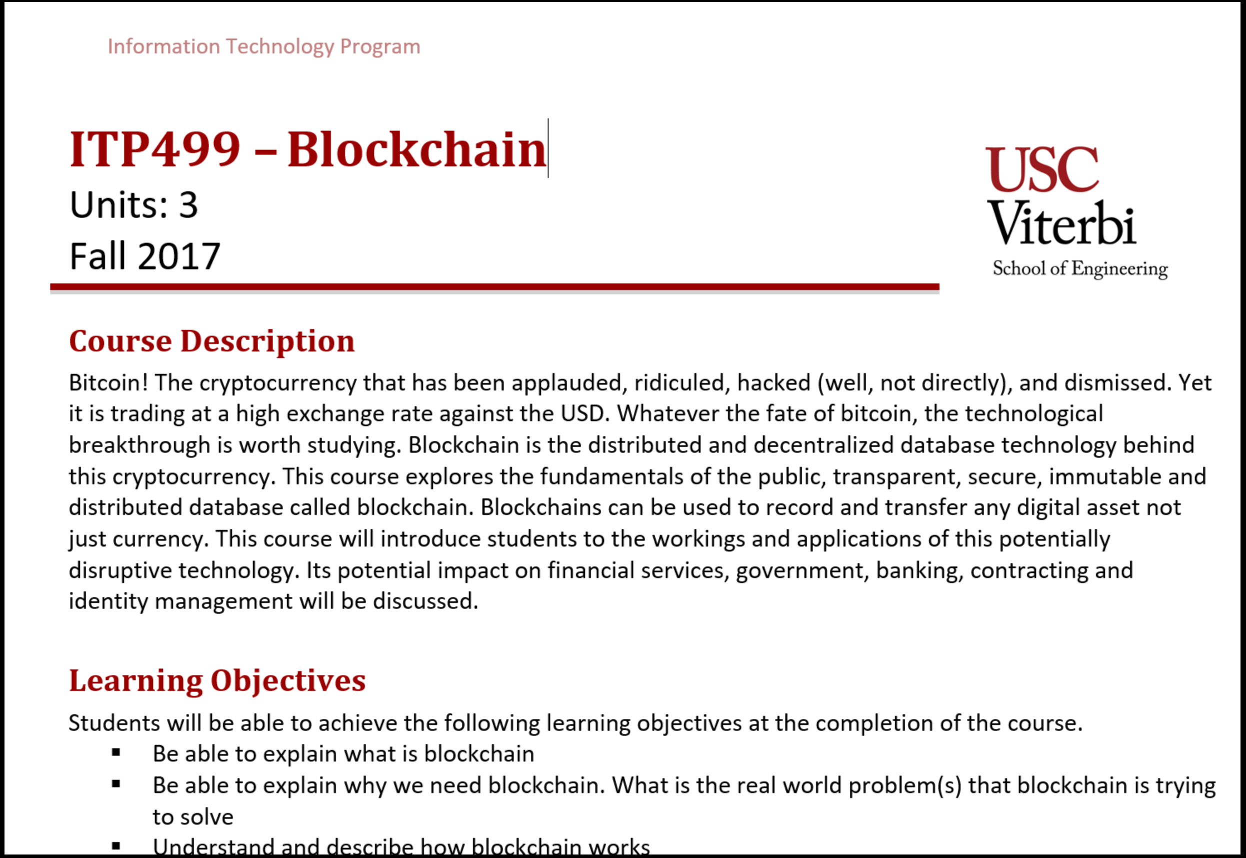
Final Thoughts

Curriculum bootstrap

Decided to jump head first into the deep end of the pool…by…

Taught a Special Topics 3-unit course on *Blockchain* this Fall. No prerequisites, open to all students. Class was full for Fall 2017!

Teaching again in Spring 2018.



Information Technology Program

ITP499 – Blockchain

Units: 3

Fall 2017

USC
Viterbi
School of Engineering

Course Description

Bitcoin! The cryptocurrency that has been applauded, ridiculed, hacked (well, not directly), and dismissed. Yet it is trading at a high exchange rate against the USD. Whatever the fate of bitcoin, the technological breakthrough is worth studying. Blockchain is the distributed and decentralized database technology behind this cryptocurrency. This course explores the fundamentals of the public, transparent, secure, immutable and distributed database called blockchain. Blockchains can be used to record and transfer any digital asset not just currency. This course will introduce students to the workings and applications of this potentially disruptive technology. Its potential impact on financial services, government, banking, contracting and identity management will be discussed.

Learning Objectives

Students will be able to achieve the following learning objectives at the completion of the course.

- Be able to explain what is blockchain
- Be able to explain why we need blockchain. What is the real world problem(s) that blockchain is trying to solve
- Understand and describe how blockchain works

Learn More

Projects to watch

- Hyperledger – SAP - https://www.hyperledger.org/
- Ethereum - https://www.ethereum.org/

Books to read

- Easy read – *Blockchain Revolution*, Don Tapscott and Alex Tapscott (father/son team, TED talks, tech evangelists)
- Technical book - *Bitcoin and Cryptocurrency Technologies*: A Comprehensive Introduction, Arvind Narayanan
- Very Technical Book - *Mastering Bitcoin*, Andreas M. Antonopoulos

MOOCs and courses to attend

- Coursera course (highly technical) - https://www.coursera.org/learn/cryptocurrency
- Stanford course (highly technical) - https://crypto.stanford.edu/cs251/
- MIT course - http://blockchain.media.mit.edu/syllabus.html

People to follow

- Andreas Antonopoulos (Technologist and bitcoin evangelist) https://antonopoulos.com/ and https://www.youtube.com/user/aantonop
- Vitalik Buterin on youtube, inventor of Ethereum, genius wizard