COL 4.0
BITCOIN, BLOCKCHAIN, AND BEYOND!

followed by
ERC20 Ethereum Smart Contract Demo/Walkthrough

OVERVIEW

- What is a Blockchain?
- Bitcoin.
- Blockchain design considerations.
- Smart contract.
- ERC-20 Ethereum Smart Contract demonstration.

Tyler Pinckard

M

Zetta

GENERAL DYNAMICS

COFFEE SHIFT INC.

COFFEE THAT EMPOWERS PEOPLE

NORTHROP GRUMMAN

EMBRY-RIDDLE 1926 AERONAUTICAL UNIVERSITY

Ucla

UNITED STATES ARMY

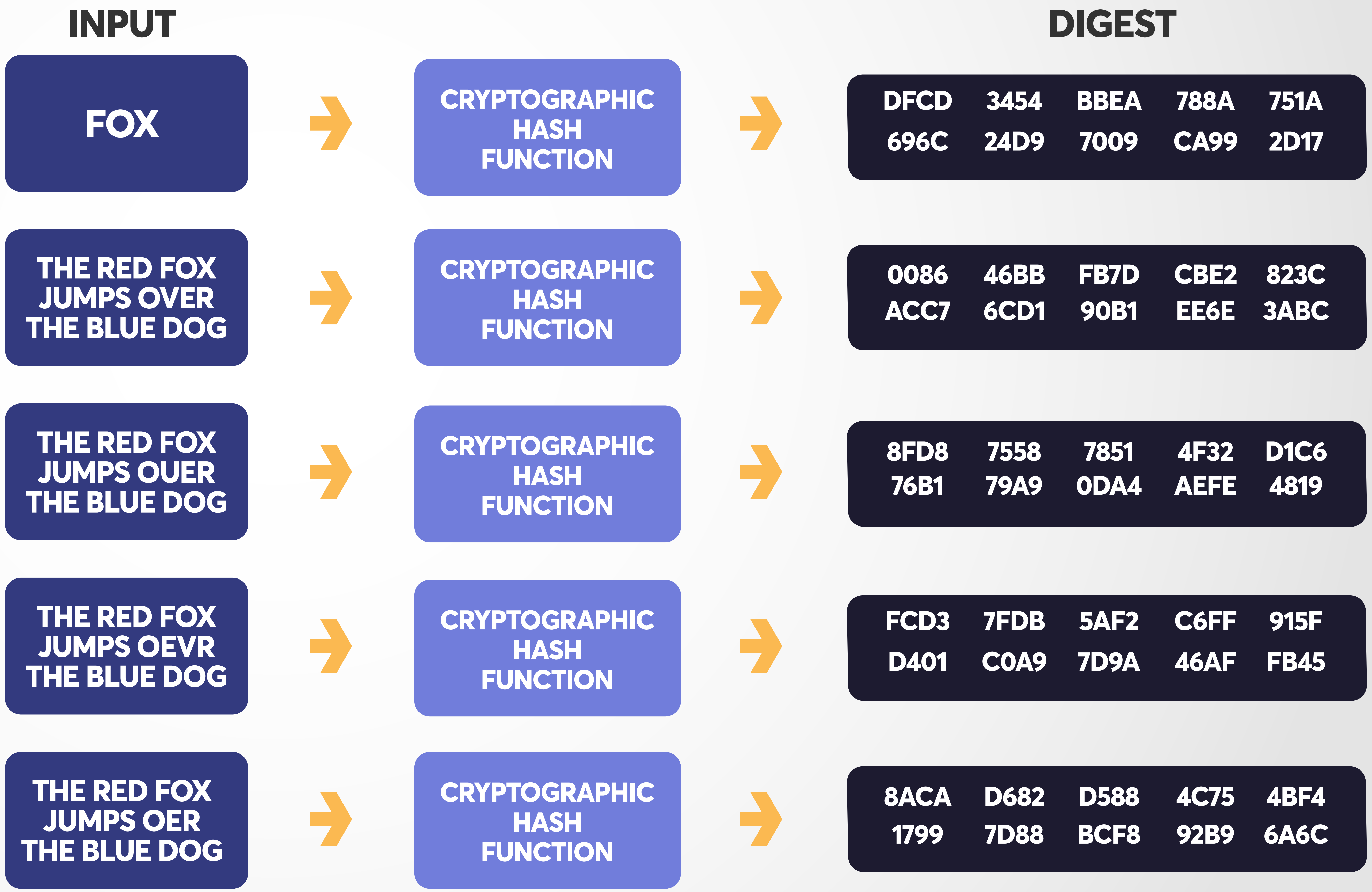
DISCLAIMER

- Check with professionals concerning the local regulations regarding cryptocurrencies and tokens ownership and issuance before jumping in.
- This information is provided for educational purposes only.
- You are responsible for your own actions. 🙂

QUICK INTO TO CRYPTOGRAPHY

Hash:

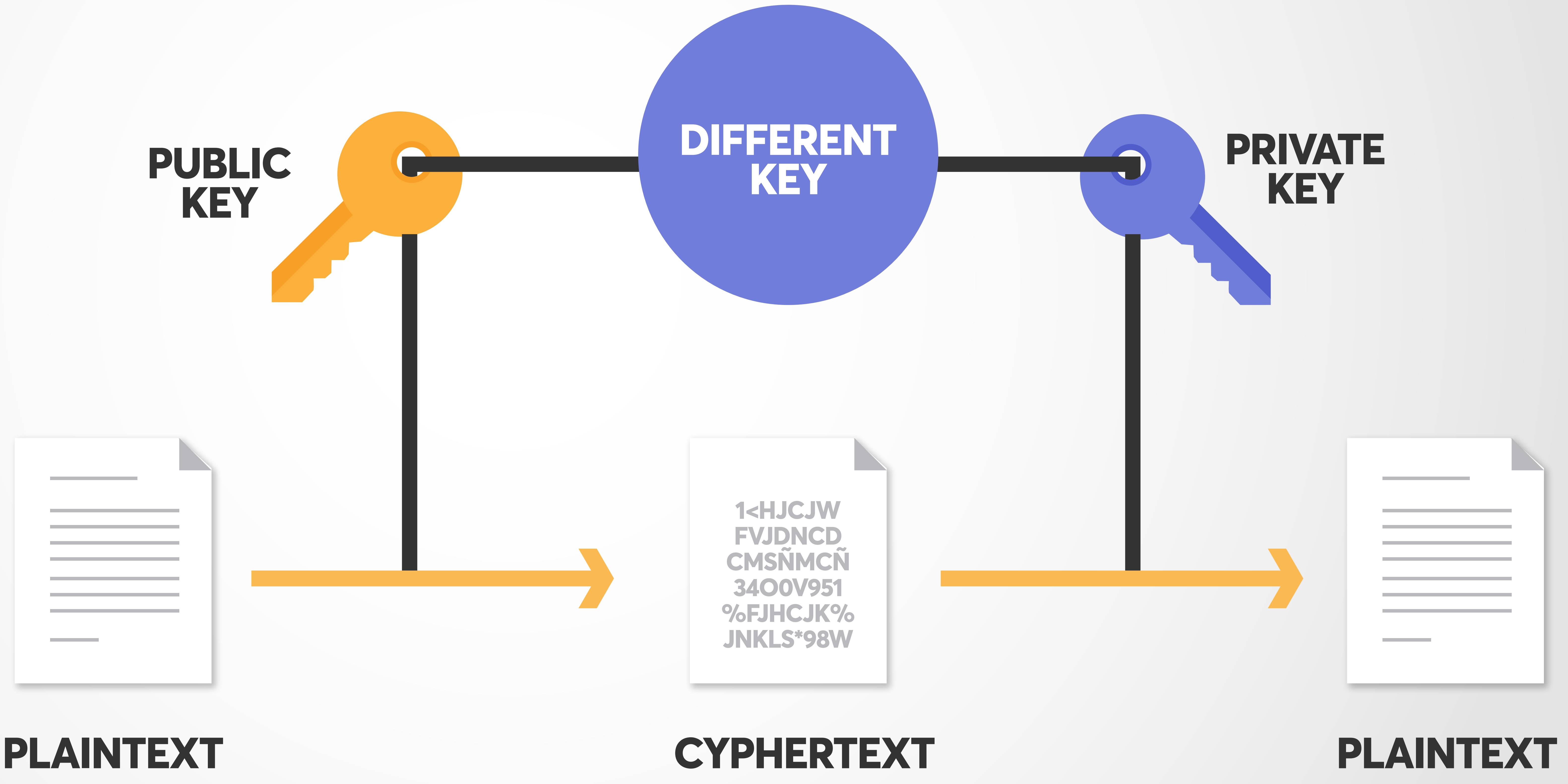
- One-way function maps arbitrary input to fixed length output.
- Very hard to reverse (ie-given the output, figure out the input).



INPUT		DIGEST
FOX	CRYPTOGRAPHIC HASH FUNCTION	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
THE RED FOX JUMPS OVER THE BLUE DOG	CRYPTOGRAPHIC HASH FUNCTION	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
THE RED FOX JUMPS OUER THE BLUE DOG	CRYPTOGRAPHIC HASH FUNCTION	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
THE RED FOX JUMPS OEVR THE BLUE DOG	CRYPTOGRAPHIC HASH FUNCTION	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
THE RED FOX JUMPS OER THE BLUE DOG	CRYPTOGRAPHIC HASH FUNCTION	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

QUICK INTO TO CRYPTOGRAPHY

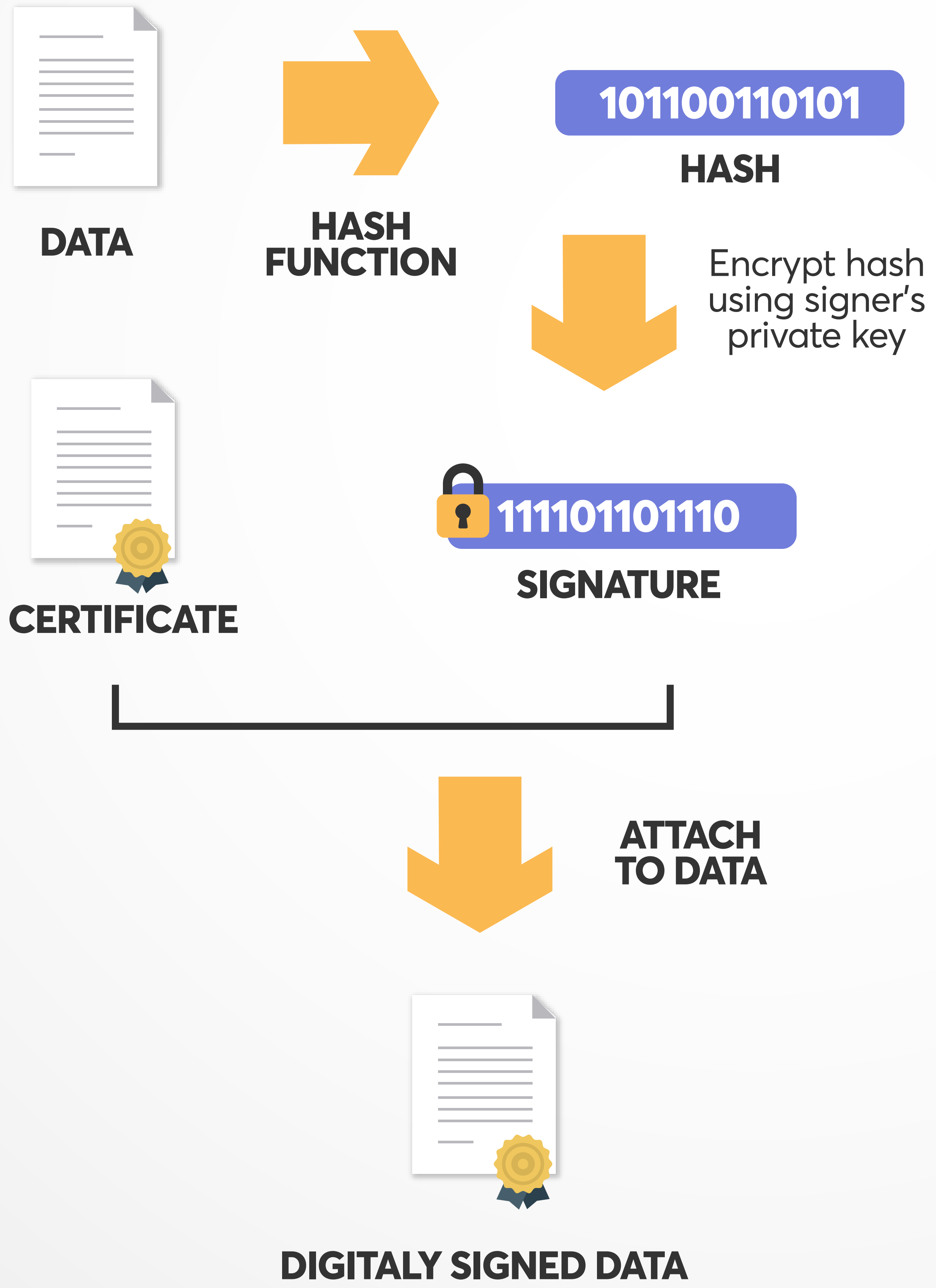
ASYMMETRIC CRYPTOGRAPHY:
Different keys used to encrypt and decrypt



QUICK INTO TO CRYPTOGRAPHY

CRYPTOGRAPHIC SIGNATURE:

SIGNING



DATA

HASH FUNCTION

101100110101

HASH

Encrypt hash using signer's private key

CERTIFICATE

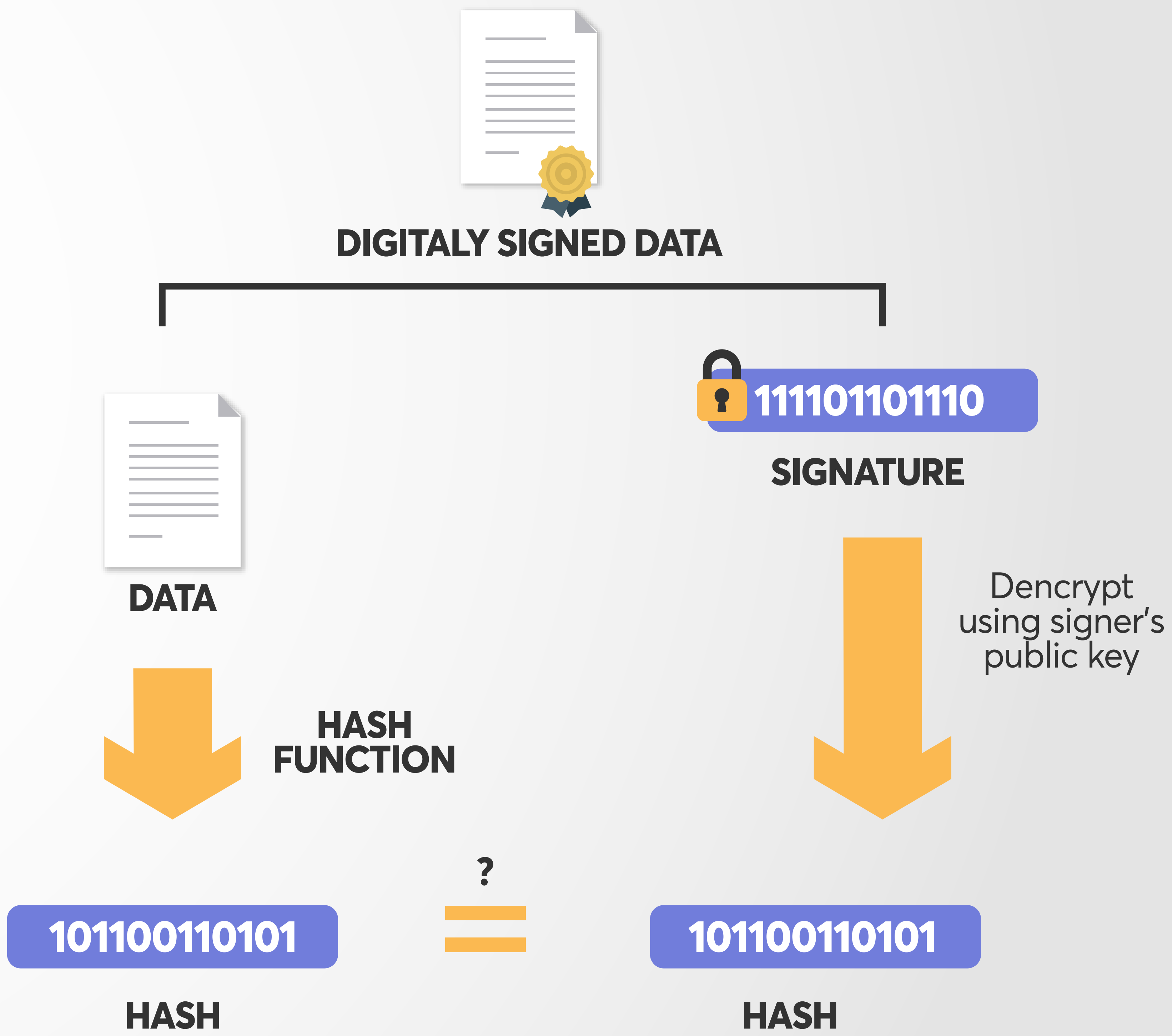
111101101110

SIGNATURE

ATTACH TO DATA

DIGITALY SIGNED DATA

VERIFICATION



DIGITALY SIGNED DATA

DATA

111101101110

SIGNATURE

HASH FUNCTION

Dencrypt using signer's public key

101100110101

HASH

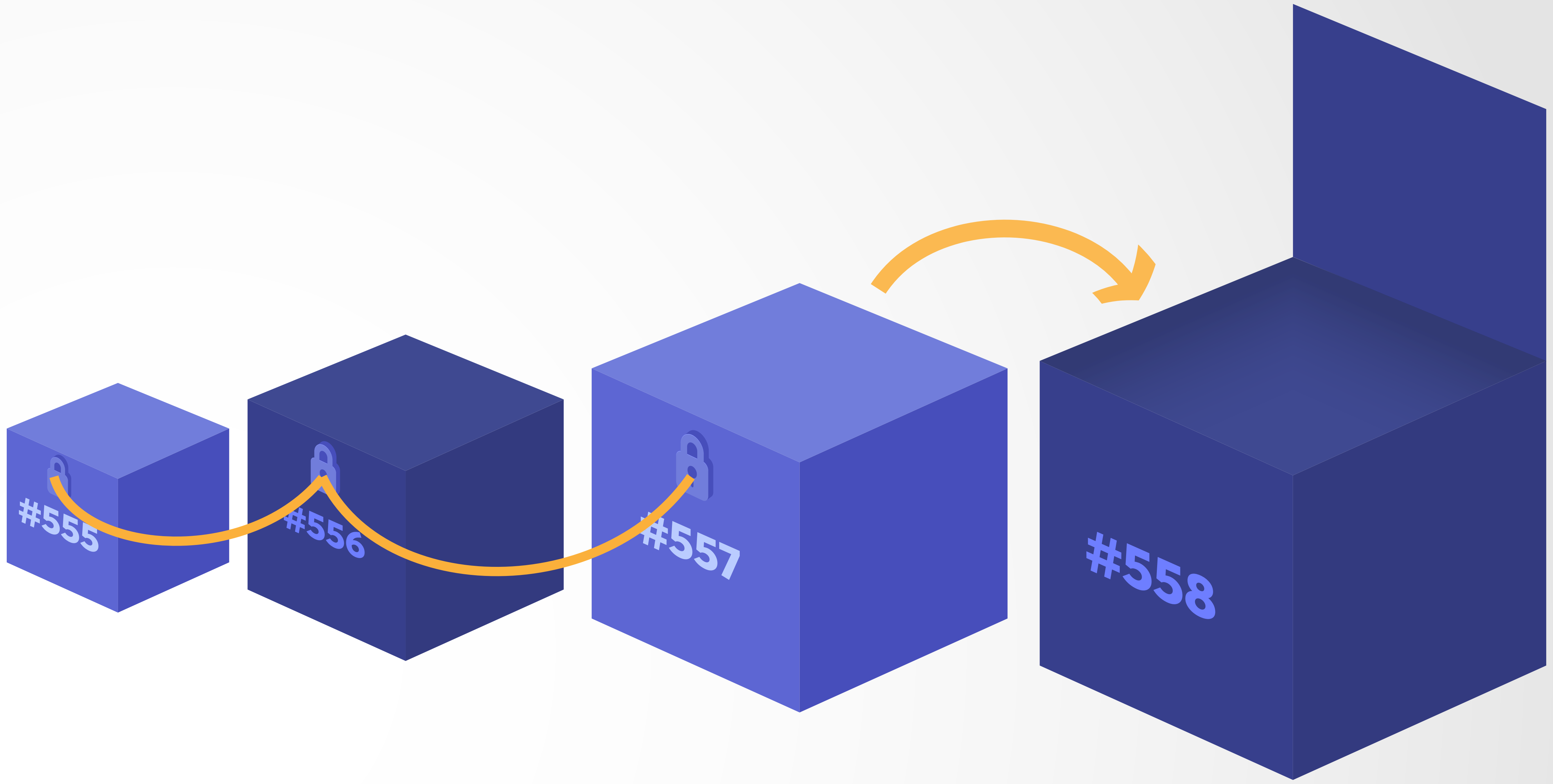
?

101100110101

HASH

IF THE HASHES ARE EQUAL, THE SIGNATURE IS VALID

WHAT IS A BLOCKCHAIN?

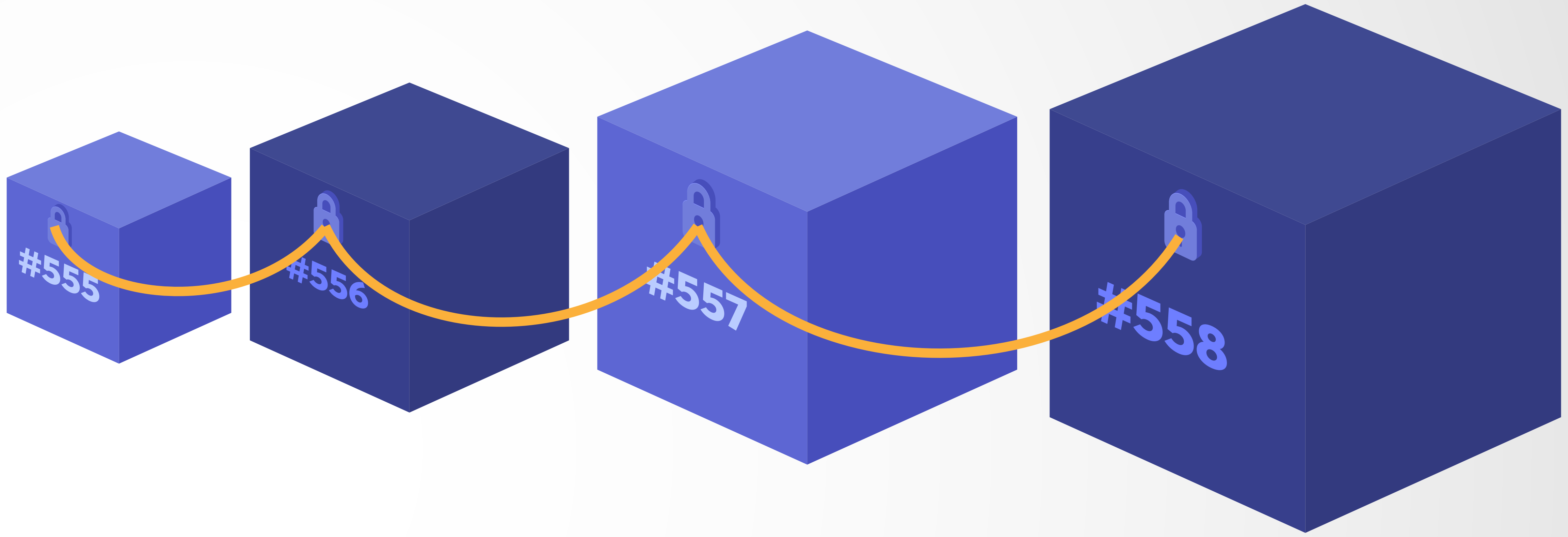


A blockchain is a way of storing information, such as transactions, as events on a timeline. So no matter how data is accessed, every action is recorded in a mathematical proof.

Distributed Ledger Technology, (aka - blockchains) record transactions immutably, and in order.

Enables users to trust the math instead of each other.

WHAT IS A BLOCKCHAIN?



Knowing that your transaction record is 100% accurate across assets means you can always provide evidence that activity has been correctly reconciled with high assurance.

The blockchain record proves attestations (i.e., Tyler promised to send Chris $100)

The math holds cheaters accountable and prevents double spending (or data manipulation)

BLOCKCHAIN CHARACTERISTICS

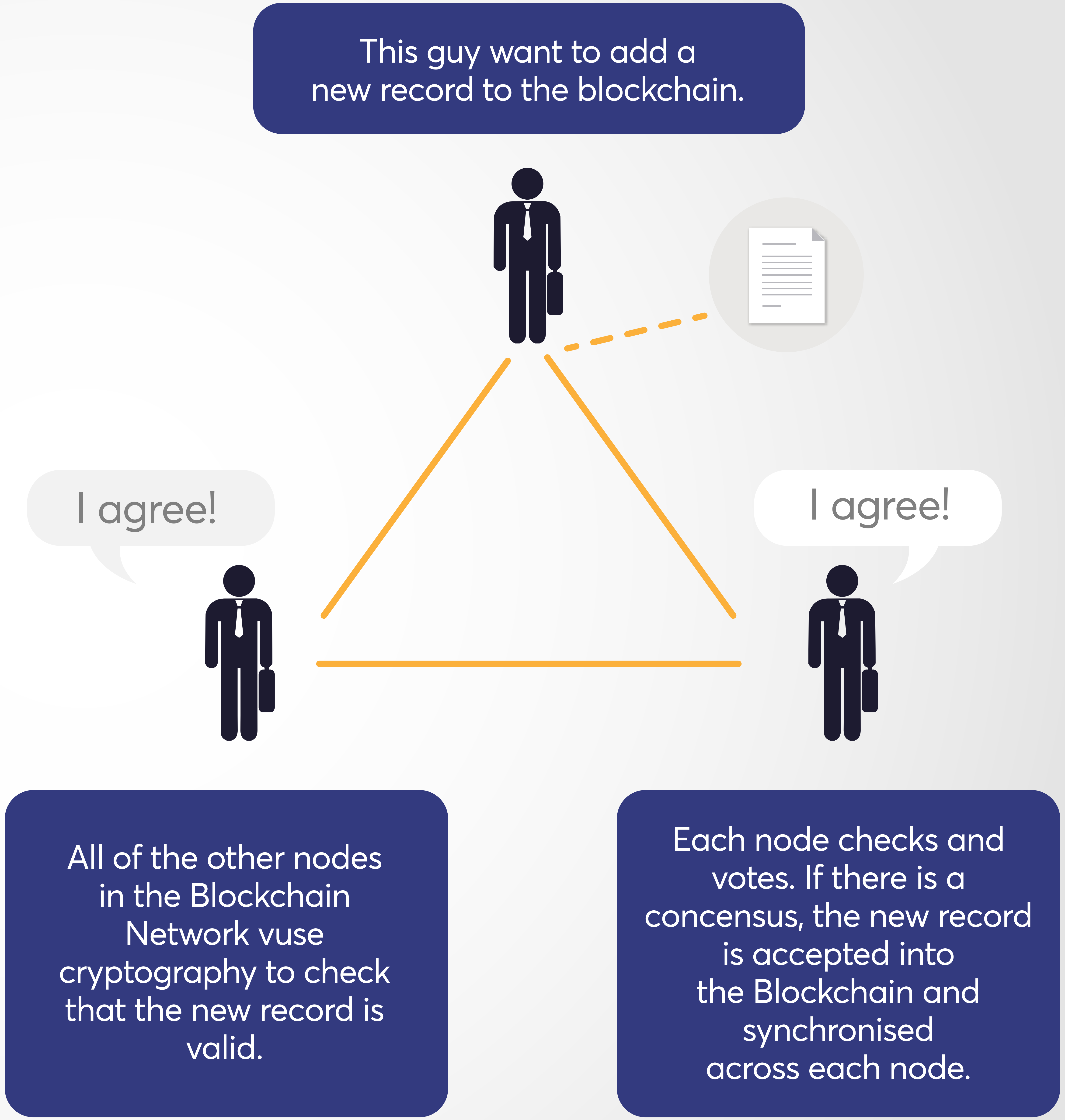
Blockchain elements:

- Replicated ledger
- Cryptography
- Consensus
- Business Logic

PUBLIC PERMISSIONLESS	PRIVATE PERMISSIONED
Bitcoin Ethereum	Ripple Hyperledger
All information on blockchain accessible by everyone else at all times Authentication required in order to participate Verify “who” you are (control private keys)	Different classes of users/nodes You must be authorized (with the oligarchy) to join the party

CONSENSUS

- Consensus about what constitutes an accurate record can be achieved in several ways
- Not a new problem in distributed systems



This guy want to add a new record to the blockchain.

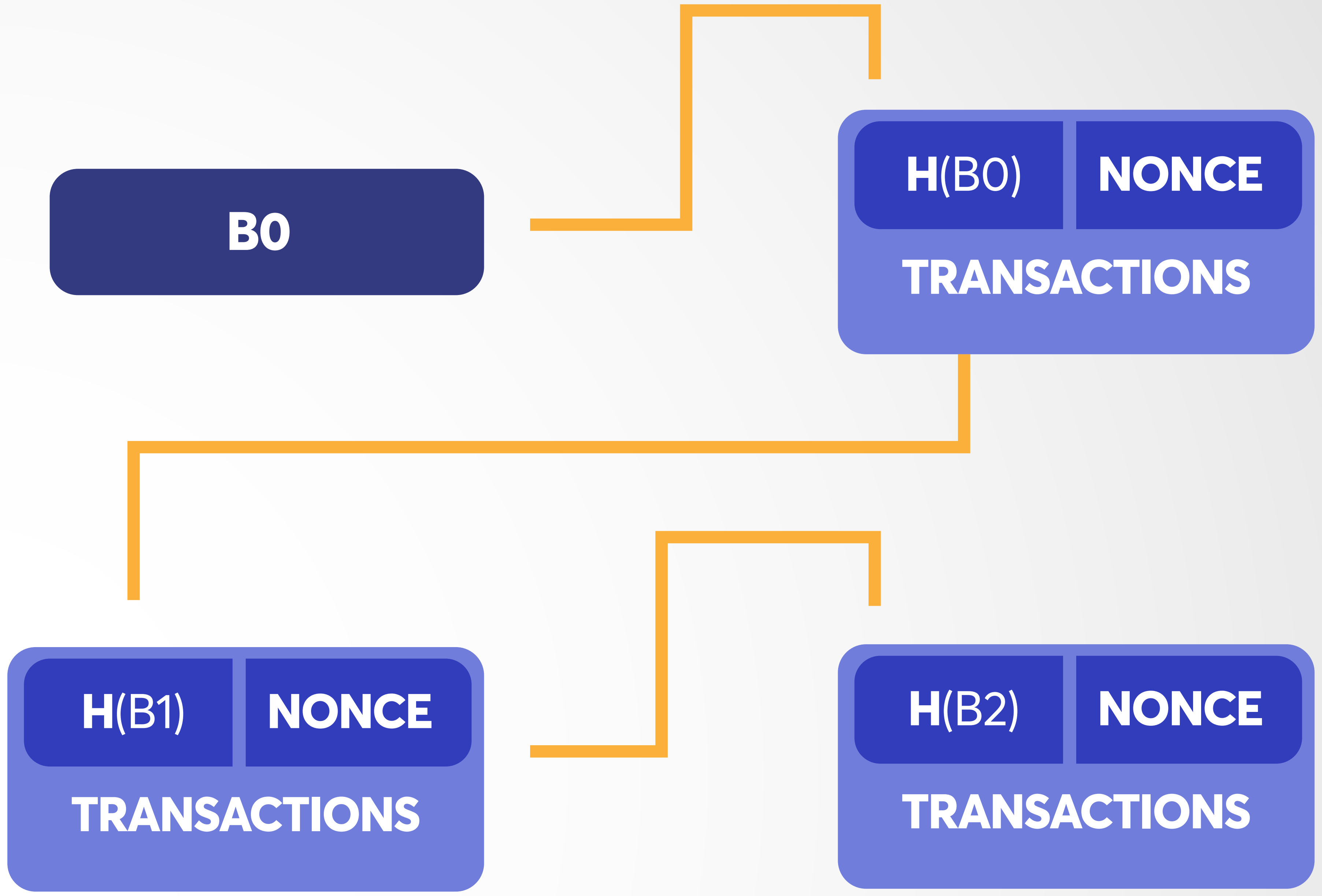
All of the other nodes in the Blockchain Network vuse cryptography to check that the new record is valid.

Each node checks and votes. If there is a concensus, the new record is accepted into the Blockchain and synchronised across each node.

TAKING A STEP BACK…
THE BITCOIN BEGINNINGS:

- Described by Satoshi Nakamodo white paper in 2008 - Network launched in 2009.
- Units of value (bitcoin) introduced via 'mining' as a reward to the people who verify the cryptographic hash computations to secure the network.
- Bitcoin is a Permissionless P2P- Anyone can join, participate in the network, wallets start with zero balance.
- Entirely new cryptographic trust model: Trust NO ONE.

PROOF OF WORK



- Users submit transactions to node(s)
- Node prepares blocks
  - List of valid transactions (tx)
  - All tx valid
- Race to find low hash value (the work)
  - Nodes try different nonce values until they find one that produces a hash that is of a sufficiently low value, starting with a series of zeros “00000000”.
  - Block difficulty is adjusted by adjusting how low they need to guess in order to “win” the block
  - Impossible to guess; effectively randomizes block round leade.
  - Winner’s proposed block becomes actual block and winning node gets block reward (currently 12.5 BTC - next drop in 2020)

BLOCKCHAIN CHARACTERISTICS

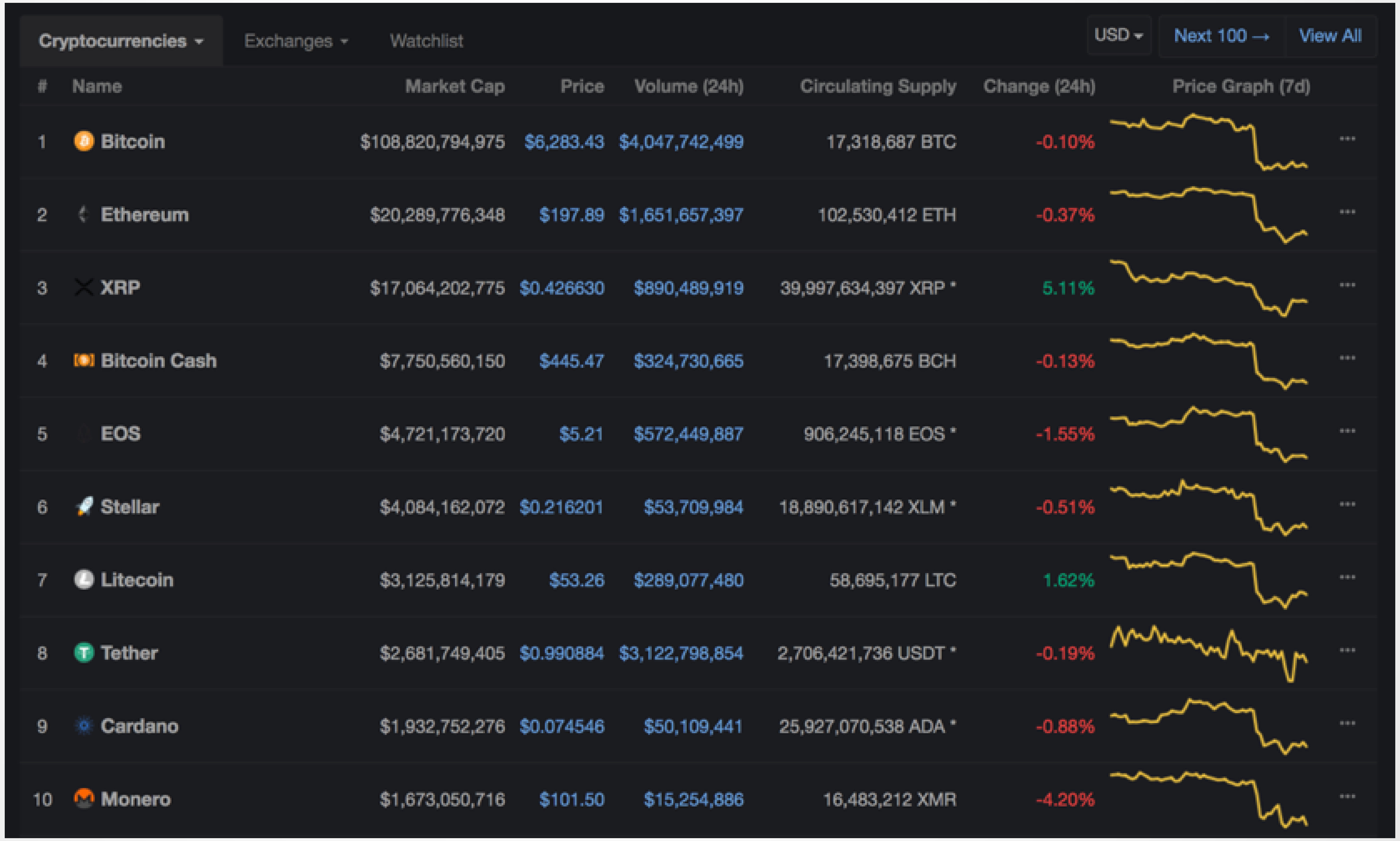
- Only forward, never backward
- Security of private keys is paramount
- Tamper Evident
- Double Spend
- Sybil Attack
- Smart Contracts

PUBLIC NETWORK NOTABLES

- Permissionless networks require decentralization.
  - Side affect is that no central entity has the authority to edit the ledger.
  - ie: unable to be controlled by governments.
- Governance Structure.
  - How are changes incorporated into the blockchain code?
  - Who decides?

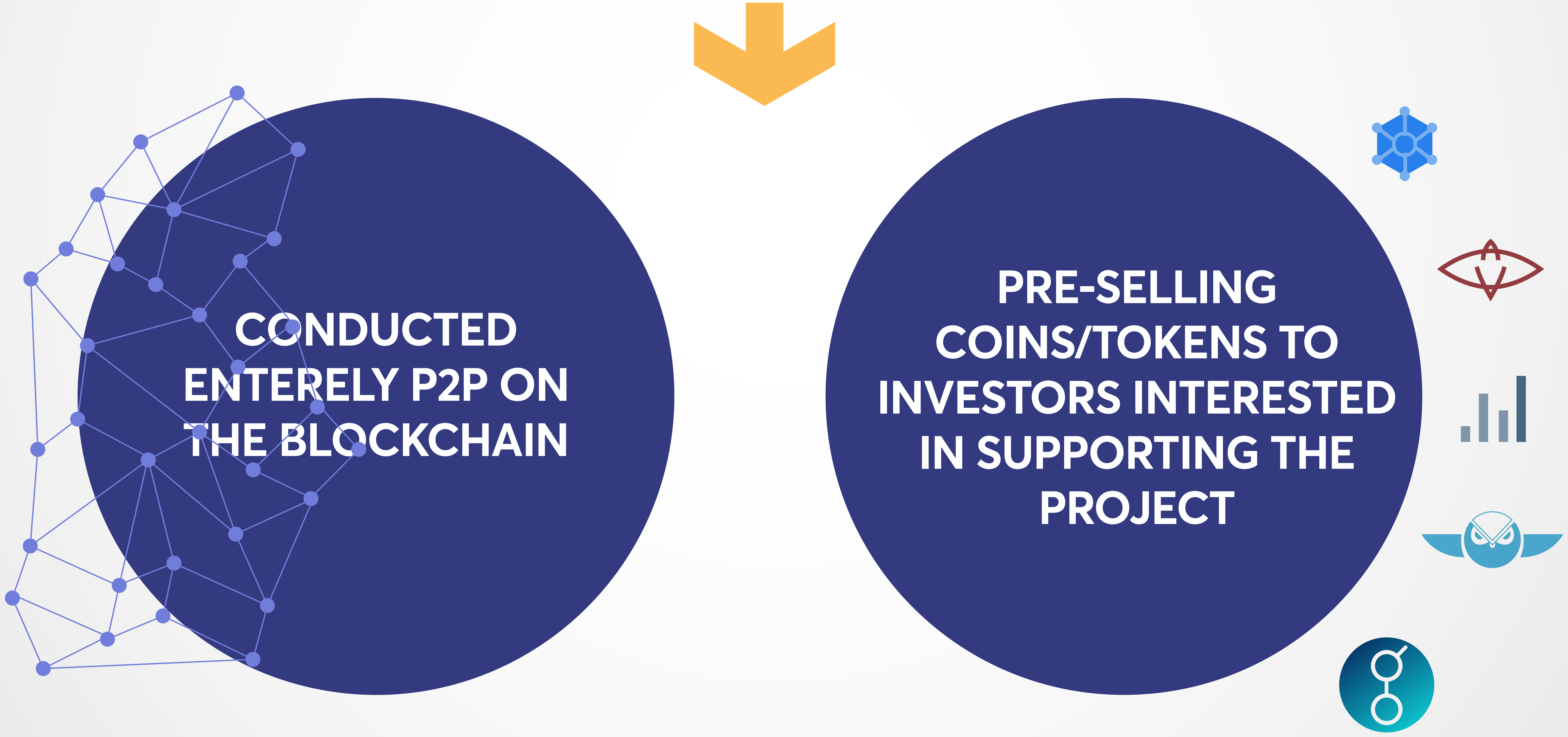
CRYPTOCURRENCIES

Tokens?
ICO?
ERC-20



#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$108,820,794,975	$6,283.43	$4,047,742,499	17,318,687 BTC	-0.10%	
2	Ethereum	$20,289,776,348	$197.89	$1,651,657,397	102,530,412 ETH	-0.37%	
3	XRP	$17,064,202,775	$0.426630	$890,489,919	39,997,634,397 XRP *	5.11%	
4	Bitcoin Cash	$7,750,560,150	$445.47	$324,730,665	17,398,675 BCH	-0.13%	
5	EOS	$4,721,173,720	$5.21	$572,449,887	906,245,118 EOS *	-1.55%	
6	Stellar	$4,084,162,072	$0.216201	$53,709,984	18,890,617,142 XLM *	-0.51%	
7	Litecoin	$3,125,814,179	$53.26	$289,077,480	58,695,177 LTC	1.62%	
8	Tether	$2,681,749,405	$0.990884	$3,122,798,854	2,706,421,736 USDT *	-0.19%	
9	Cardano	$1,932,752,276	$0.074546	$50,109,441	25,927,070,538 ADA *	-0.88%	
10	Monero	$1,673,050,716	$101.50	$15,254,886	16,483,212 XMR	-4.20%	

ICO
Crowd-funding Method

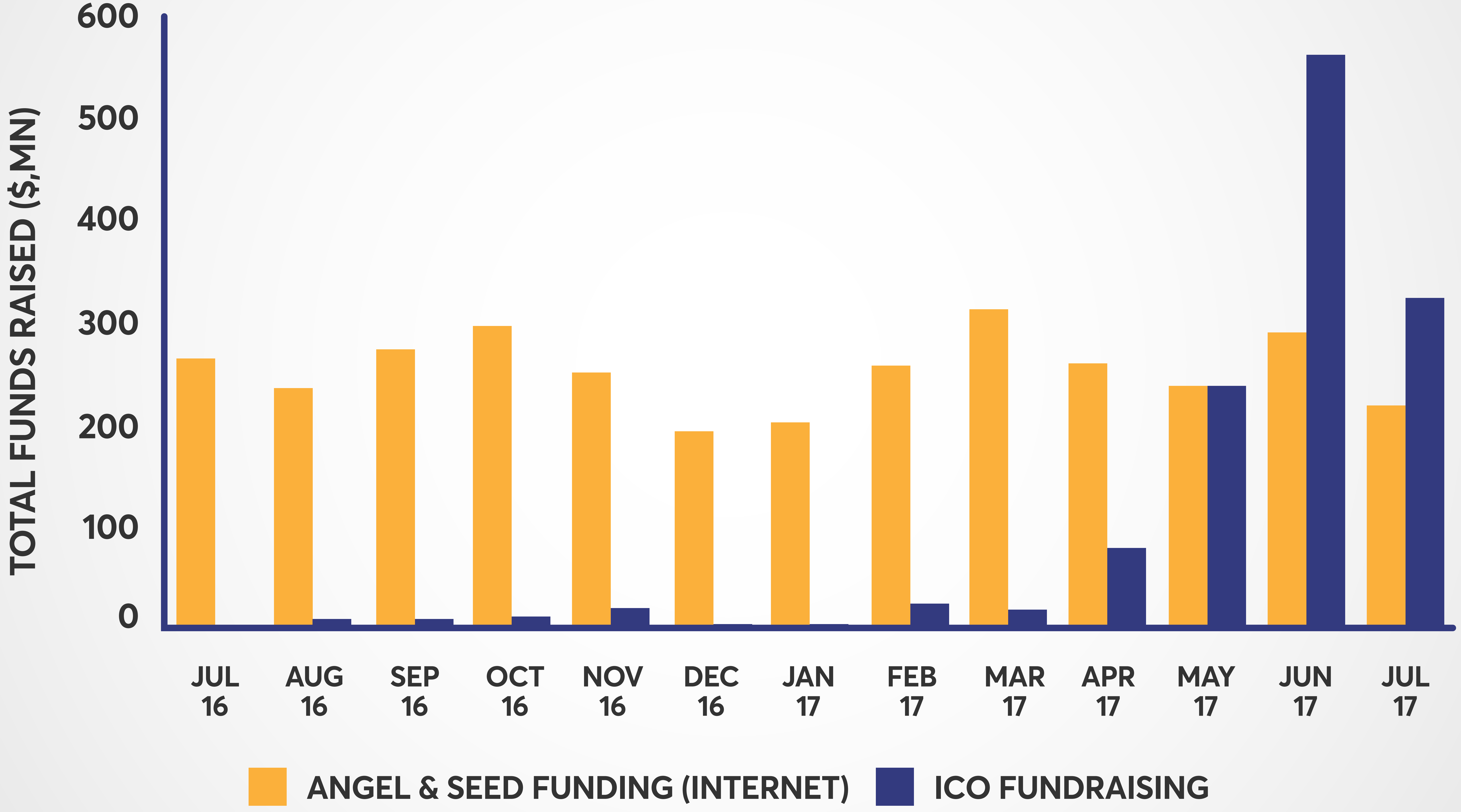


CONDUCTED ENTERELY P2P ON THE BLOCKCHAIN

PRE-SELLING COINS/TOKENS TO INVESTORS INTERESTED IN SUPPORTING THE PROJECT

EXHIBIT 8: THE PACE OF ICO FUNDRAISIN HAS NOW SURPASSED ANGEL & SEED STAGE INTERNET VC UNDING GLOBALLY

Total Funds Raised By Month ($, Millions)



Note: ICO fundraising as of July 18th, 2017 per Coin Schedule, Angel & Seed VC fnding data as of July 31st, 2017 and does not include "crowfunding" rounds.
Source: CoinSchedule, CD Insights, Goldamn Sachs Global Investment Research.

TECHNICAL PORTION:
Erc20 Smart Contract

- Inspiration: Moritz Neto's ICO Guide

- Issue smart contract on Etherum Ropstien test network

- Requirements:
  - Ethereum Address **(https://www.myetherwallet.com)**
  - Some Ethereum
  - A text editor **(Sublime / Atom / Code)**
  - Solidity contract
(https://github.com/bitfwdcommunity/ICO-tutorial/blob/master/ico-contract.sol)

QUESTIONS?

RESOURCES

- https://medium.com/@bleecoin/ico-guide-for-complete-beginners-df535b44c81b
- https://www.slideshare.net/ITU/blockchain-cryptography-and-consensus
- https://medium.com/elrondnetwork/yabp-yet-another-blockchain-primer-bce90fb3233
- https://medium.com/@jgm.orinoco/understanding-erc-20-token-contracts-a809a7310aa5
- https://medium.com/bitfwd/how-to-do-an-ico-on-ethereum-in-less-than-20-minutes-a0062219374
- https://simple.wikipedia.org/wiki/Cryptographic_hash_function

BACKUP SLIDES

CONSENSUS ALGORITHMS

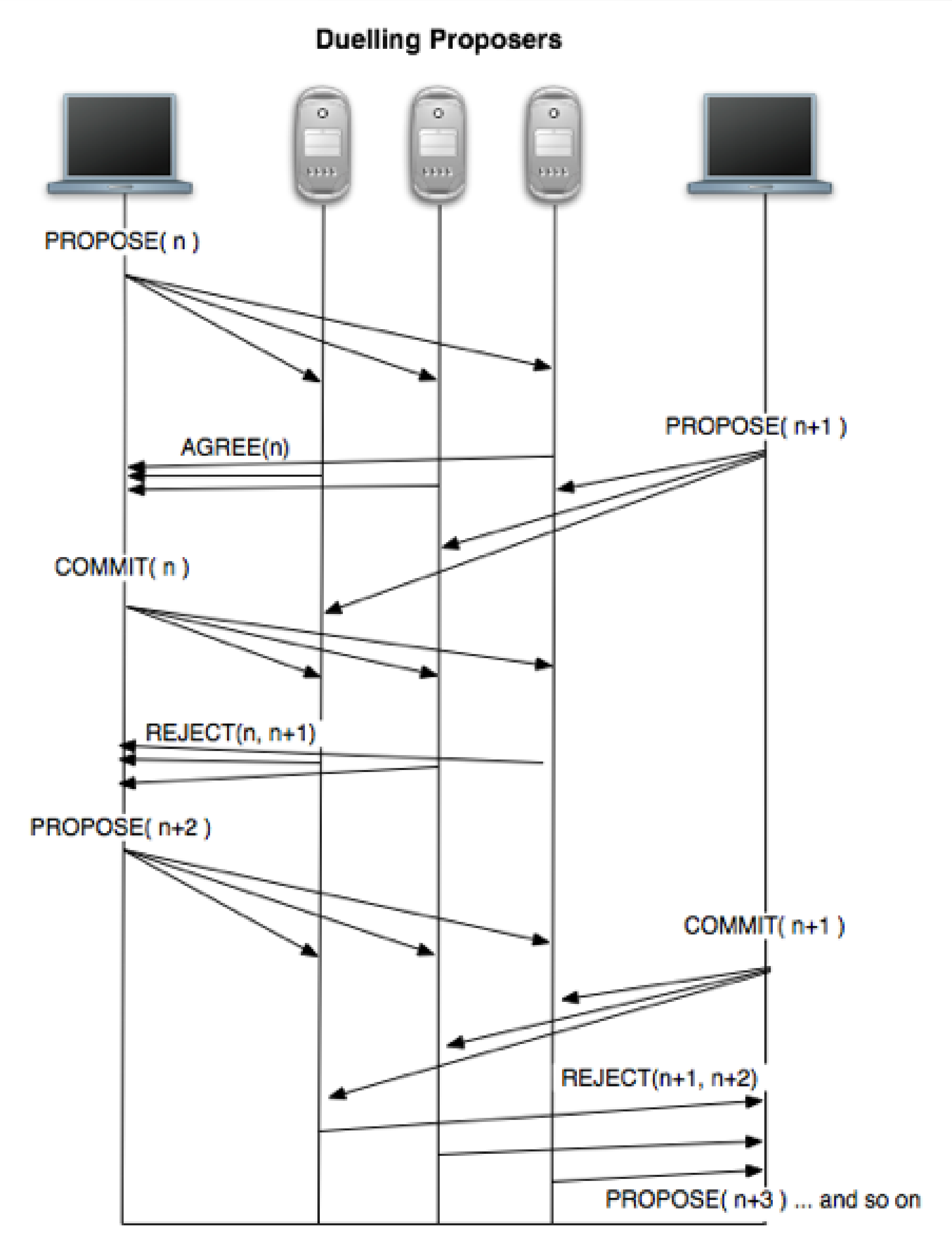
- Defined by how each node reacts to one or more of the following items:
  - Response time (latency)
  - How many of them responded (aliveness)
  - What their opinion of ‘truth’ is (voting)

- Bitcoin - play by the rules and you may get to be king for a day!

- Permissioned systems typically report 10-1000x performance over permissionless, as they authenticate participates and can assume more trust during operation.

CONSENSUS ALGORITHMS

- Byzantine Fault Tolerance well studied in computer science.
  - Paxos (and derivatives).
  - Raft, Cubby, etc.
- Very Different for Permissioned vs. Permissionless!
  - Permissioned systems.
    - Non adversarial participants.
    - Only known and vetted nodes are allowed to join.
    - Often proof of stake.
  - Permissionless
    - Anyone can spin up a node instance and contribute to the network.
    - ie- bitcoin w/ proof of work.



BLOCKCHAIN CHARACTERISTICS

REPLICATED LEDGER

- History of all transactions.
- Append-only with immutable past.
- Distributed and replicated

CRYPTOGRAPHY

- Integrity of ledger
- Autenticity of transactions
- Privacy of transactions
- Identity of participantes

CONCENSUS

- Decentralized protocol Shared control tolerating disruption
- Transactions validated

BUSINESS LOGIC

- Logic embeddeb in the ledger
- Excecuted together with transactions
- From simple “coins” to self-enforcing “smart contracts”

BLOCKCHAIN SYSTEM DESIGN CONCERNS

- Distributed system- multiple, disparate actors
  - Information takes time to propagate
  - Speed of Light - Network Latency

- Not everyone has the same set of “facts” at the same time
  Time is a relative, each participant has their own perspective.

- How to keep the network synchronized?
- How to prevent double spend?