What is **Blockchain**

Other Than Being Really Cool Sounding

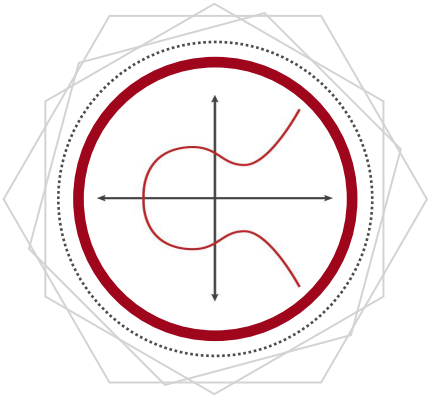
Blockchain Has

Two Main Parts

xsolus

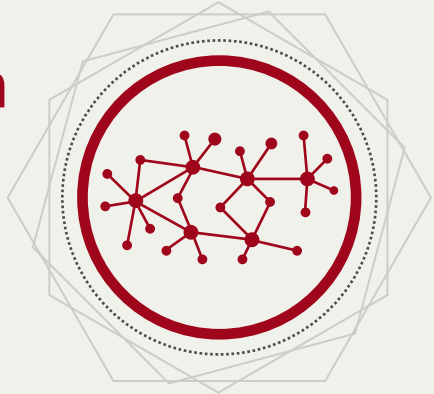
Cryptography

Message Integrity



Decentralization

Ledger Consistency and Immutability



Cryptography

One-way cryptography (hashing) uses an algorithm to encrypt the data

Symmetric cryptography uses the same key (code) to encrypt/ decrypt

Asymmetric cryptography uses a key to encrypt and a different key to decrypt. One type of asymmetric cryptography is public-key/private-key cryptography

Asymmetric Cryptography

- Public-key/Private-key cryptography uses a pair of keys that go both ways

Public-key can encrypt data that only the private-key can decrypt

Private-key can encrypt data that only the public-key can decrypt

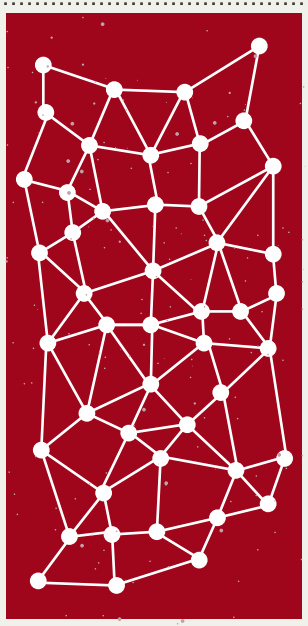
- Share your public-key so anyone can encrypt data that only your private-key can decrypt; or encrypt data with your private-key that anyone with your public-key can decrypt

Ensure Message Integrity

- Public-key/private-key cryptography allows a concept called signing
- Something encrypted by your private-key can be decrypted by anyone with your public-key
- If you send a message along with a private-key encrypted version of your message, anyone with your public-key can decrypt it and ascertain that it was you who sent it and that it has not been altered
- To make things easier, we compress the message into what's called a hash, and then encrypt the hash with our private key.
- Again anyone can compress the message into the same hash, decrypt your encrypted hash with your public key and see that they are the same.

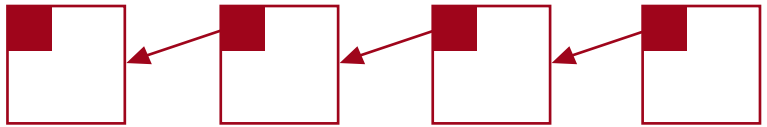
Decentralized Ledger

- If we want to keep a record of signed transactions that no one party can alter, destroy, or even question, we need many custodians of the same data
- Everyone can exchange new transactions and add it to their records
- Transactions need to be validated to make sure they don’t violate rules of the road (ie. debits don’t exceed credits)
- A network of nodes is used to automatically exchange and validate new transactions and add them to their records



Ensuring Consistency

- A system of hashes and links is used to make sure that no data is corrupted or altered
- Blocks are a collection of transactions
- Blocks are compressed into a hash
- Each block refers to the hash of the block before
- The previous block reference becomes parts of the hash of the current block
- No data in any previous block can be changed without changing the hash of that block and every block that follows it
- This is what we call a blockchain



Handling Disagreements

- There is the possibility of disagreements in our decentralized ledger
- Transaction ordering can be important when validating transactions
  - Credits total $500,000, but two debits for $400,000 come in, which one to validate?
- Our decentralized ledger needs some way to decide
- We call this consensus
- Typically the nodes engage in some sort of challenge to see who will be the authority to make the decision
- Challenges are what we call a consensus algorithm or protocol

Consensus

- Proof of Work (PoW) that makes all nodes try to guess a number that hashes with the rest of the block header to equal a number below a set number (difficulty); requires a lot of wasted energy
- Proof of Stake (PoS) that makes all nodes show that they have some stake (own coin) in the system to be given the right to be the authority with a frequency commensurate with their stake
- Delegated Proof of Stake (DPoS) that makes all nodes with a stake elect a representative, with the number of votes commensurate with their stake
- Proof of Luck (PoL) that makes all nodes buy one or more tickets, and have a chance to win commensurate with the number of tickets

Putting It All Together

- Submit a transaction
- Nodes exchange the transaction
- Nodes validate the transaction
- Nodes assemble transactions into a block, referencing the previous block
- Nodes challenge each other to take authority to reach consensus
- Nodes accept the block of the winner
- And then it continues and can’t be stopped

Presented by Eric Hey

www.xsolus.com