Khwopa
College of
Engineering

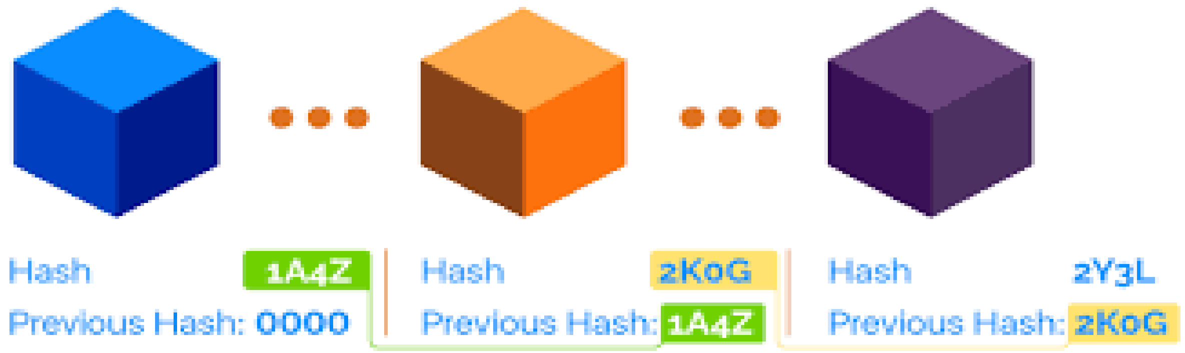
BLOCKCHAIN

Abhinav Aryal
(KCE074BCT005)

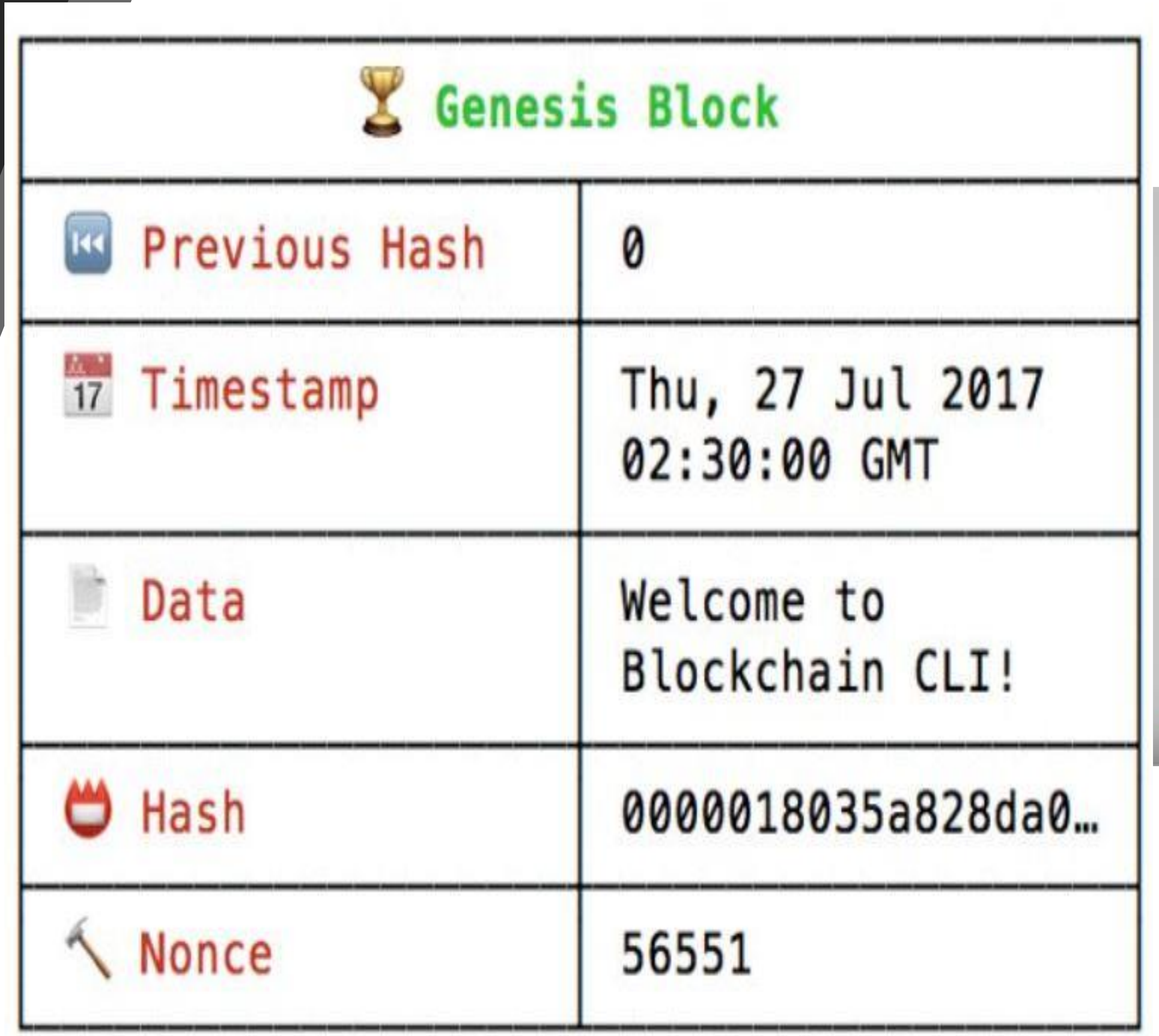
2020-09-22

What is blockchain?

A blockchain is an open, distributed ledger that can record transaction between two parties efficiently and in verifiable and permanent way without the need of central authority

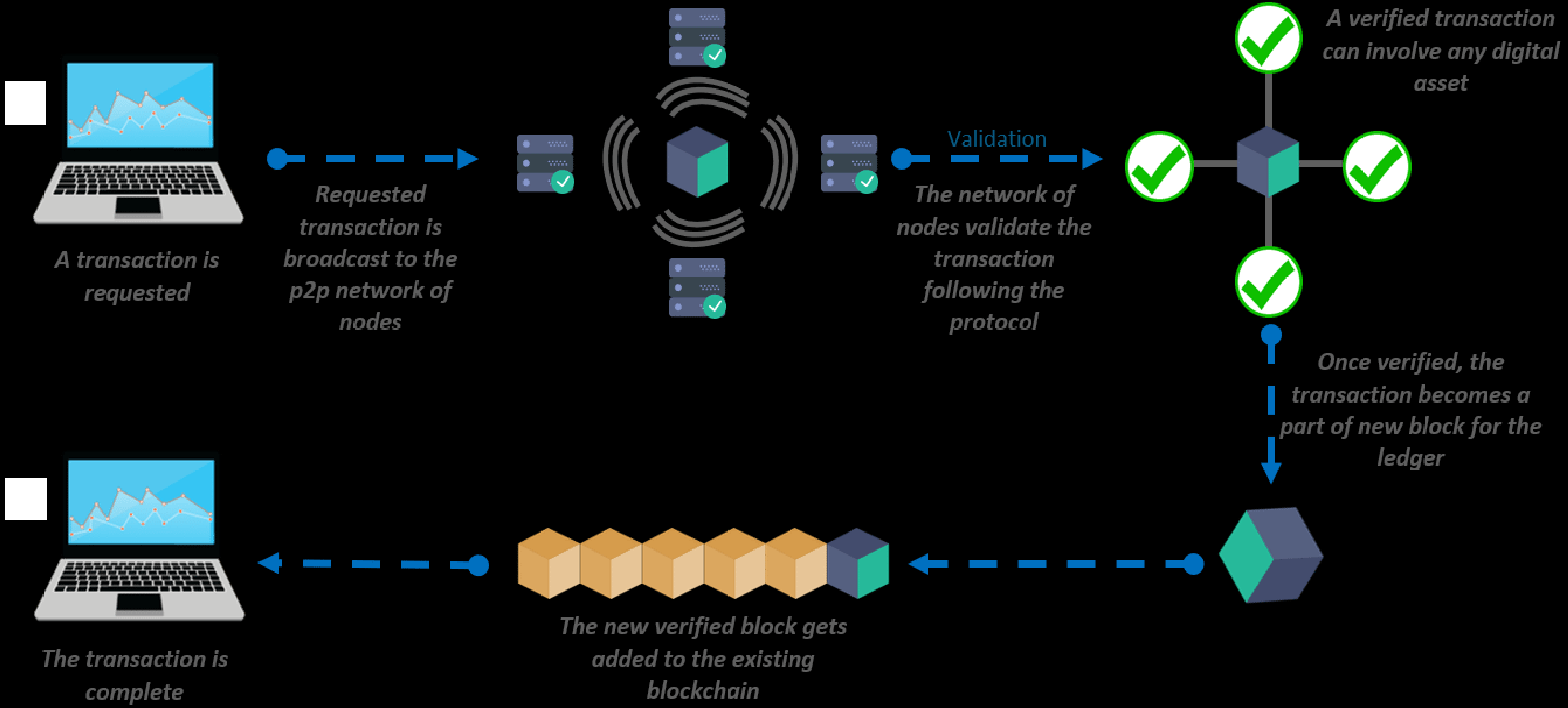


What does blockchain contain?



Genesis Block	
Previous Hash	0
Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
Data	Welcome to Blockchain CLI!
Hash	000018035a828da0…
Nonce	56551

How does blockchain work?



A transaction is requested

Requested transaction is broadcast to the p2p network of nodes

Validation

The network of nodes validate the transaction following the protocol

A verified transaction can involve any digital asset

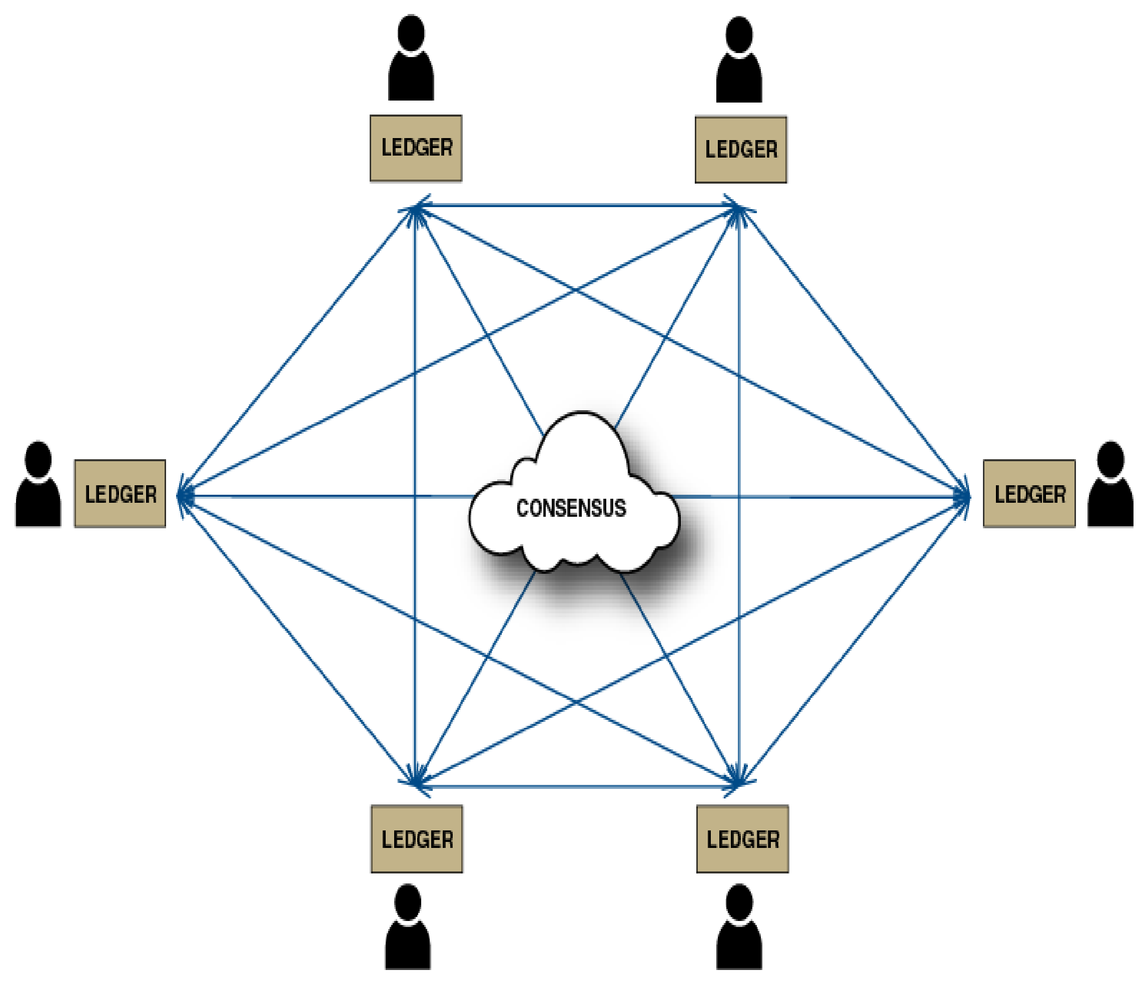
Once verified, the transaction becomes a part of new block for the ledger

The new verified block gets added to the existing blockchain

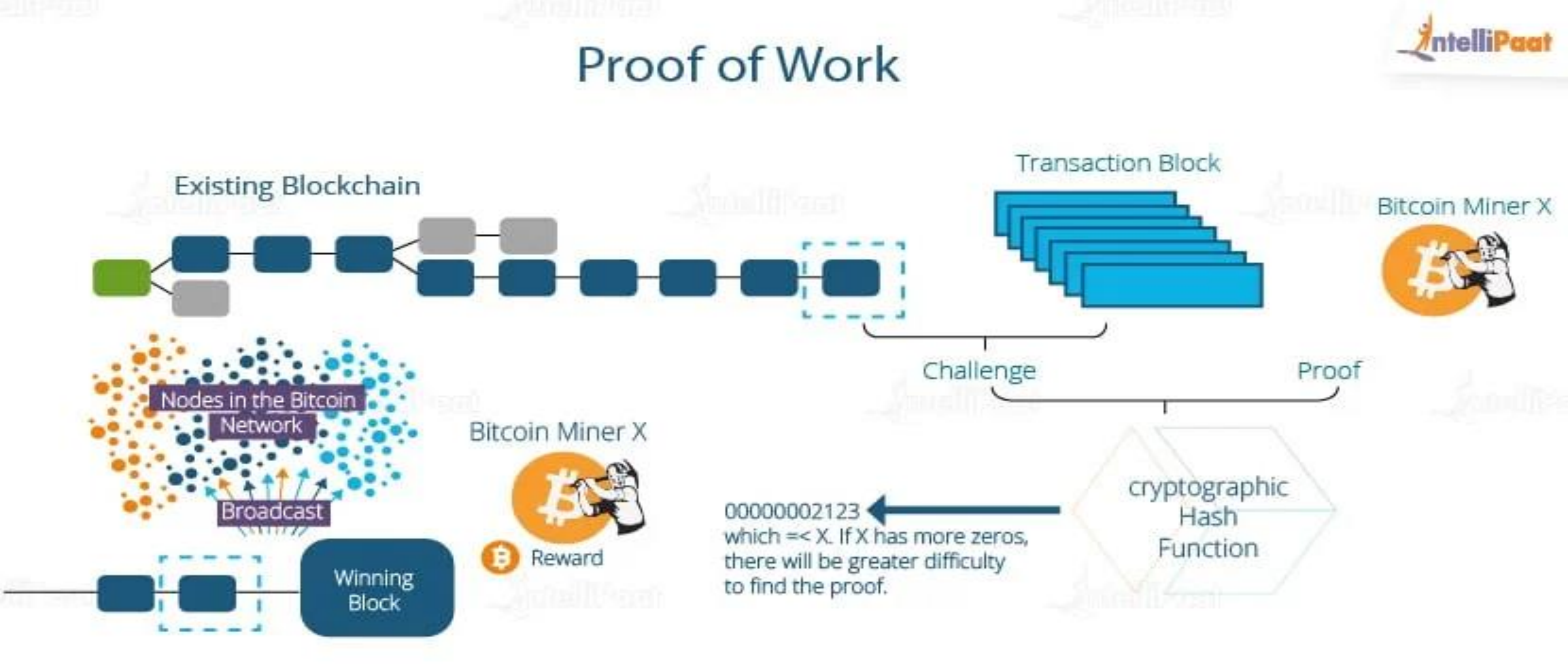
The transaction is complete

Distributed Consensus Protocol

- Consensus is the process by which peers agree to addition of the next block in the blockchain
- Distributed Consensus ensure that different nodes in the network see the same data at nearly the same point of time. Hence, in case of any failure the system can still provide a service as the data is decentralized.



Proof of work



Cryptographic Hashing

- A hashing algorithm is a computational function that condenses input data into a fixed size.
- The result of the computation is the output called a *hash* or a *hash value*.
- Map any size data(x) to a fixed size (h(x))
- H(x) can be calxulated from x but the reverse is not possible.

Cryptographic Hash Function Properties

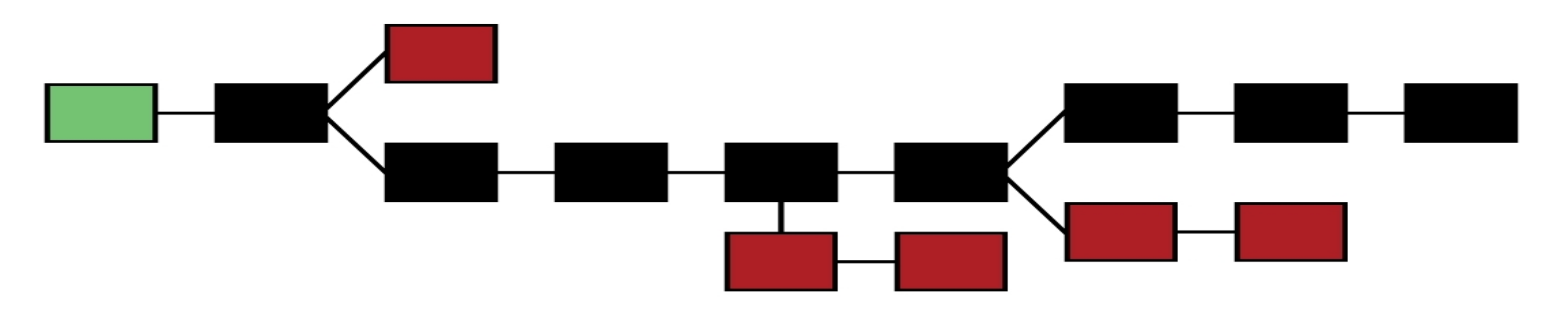
- Deterministic
- Pseudo-random
- Avalance effect
- One-way function
- Collison Resistant

Stabdard Hashing Algorithm

- **D 5:** It produces a 128-bit hash.
- **SHA 1**: produces a 160-bit hash
- **SHA 256:** Produces a 256-bit hash.
    - Bitcoin currently uses the double hash SHA-256.
- **Keccak-256:** Produces a 256-bit
    - Currently used by Ethereum

Blockchain as tree

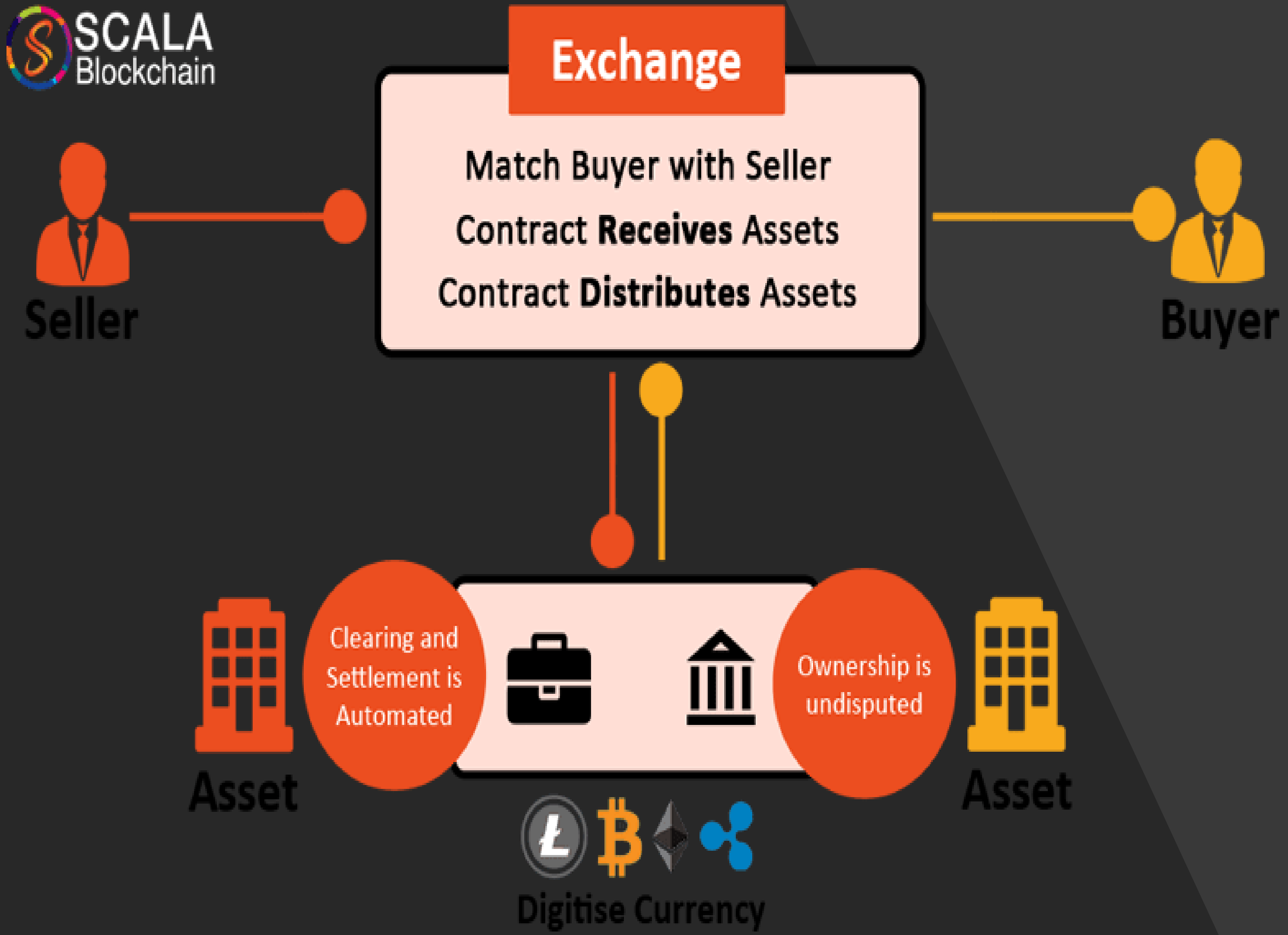
- Suppose two miners found the hash at the same time. Then they would add the new block to the chain and traverse to the whone node of network.



- The longest chain (black) is accepted, and the rest orphan(red) blocks are rejected

Smart contract

- Smart contracts are lines of code that are stored on a blockchain.
- It automatically execute when predetermined terms and conditions are met.



Blockchain Advantages

1. Speed:

- Faster transaction time

2.Security:

-Involvement of fewer intermediaries

-less required oversight

3.Effiency:

-Immutable records

Thank you!