Presentation on Blockchain Technology

Overview

- Brief History
- What is Blockchain technology?
- Goals of Blockchain
- Cutting the Middleman
- Building Consensus
- Creating Witnesses
- Key Features
- Strengths
- Weaknesses
- Challenges

Brief History

- On October 31, 2008, *Satoshi Nakamoto* released the Bitcoin White Paper outlining a purely peer to peer electronic cash/digital asset transfer system.
- This is the first popular implementation of Blockchain and is attributed as birthing today's Blockchain industry.
- Since then, additional Blockchains have been popularized, Ethereum, various Hyperledger project solutions, as well as numerous others including "Blockchain like" solutions such as *GuardTime's KSI* products

What is Blockchain technology?

A technology that;

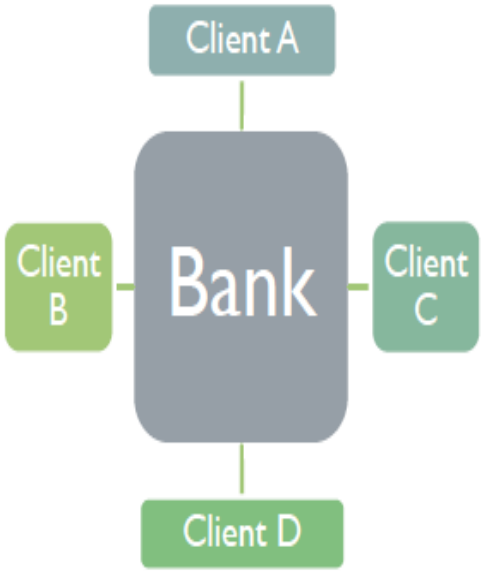
- permits transactions to be gathered into blocks and recorded;
- cryptographically chains blocks in chronological order; and
- allows the resulting ledger to be accessed by different servers.

Goals of Blockchain

- Creating a secure network that is capable of executing , verifying , and reaching consensus on the state of shared data without the need for a trusted third-party intermediary.
- Ensuring that data can’t be changed after it has been accepted by the network (known as tamper-resistance, sometimes mistakenly called immutability).
- Verifying that the parties sending data or executing transactions have the means and authority to do so (authentication).

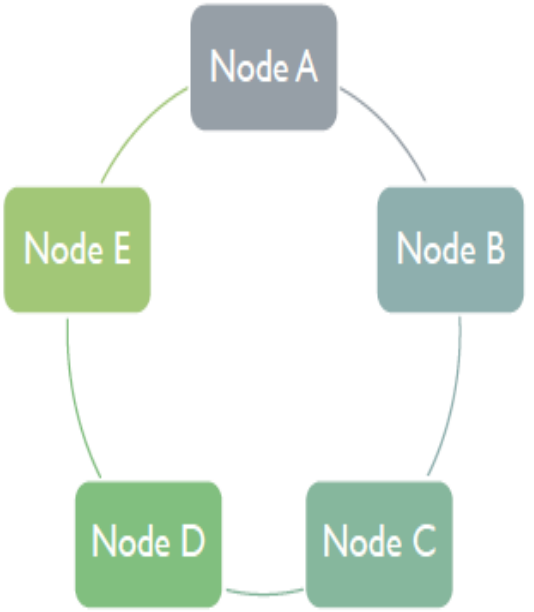
WHAT IS A DISTRIBUTED LEDGER?

Centralized Ledger



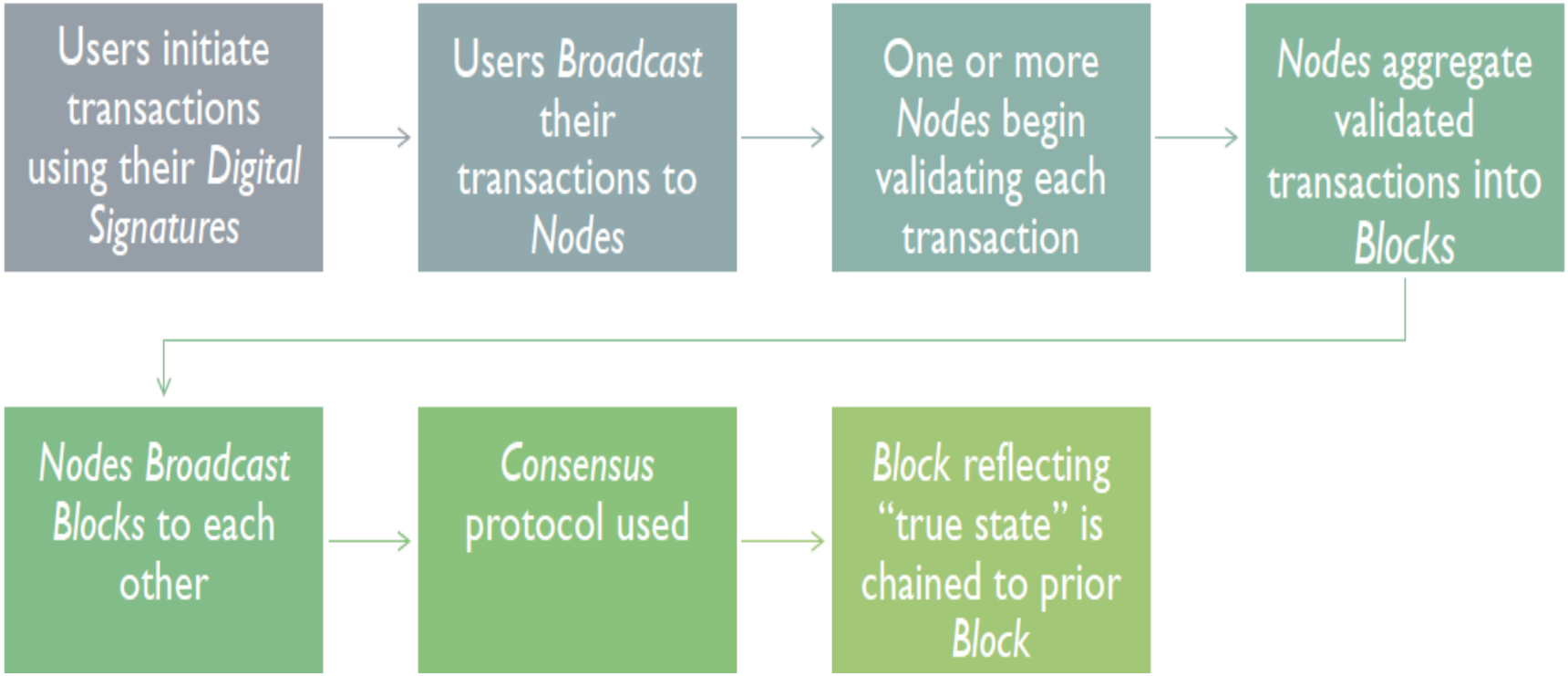
- There are multiple ledgers, but Bank holds the "golden record"
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if discrepancies arise

Distributed Ledger

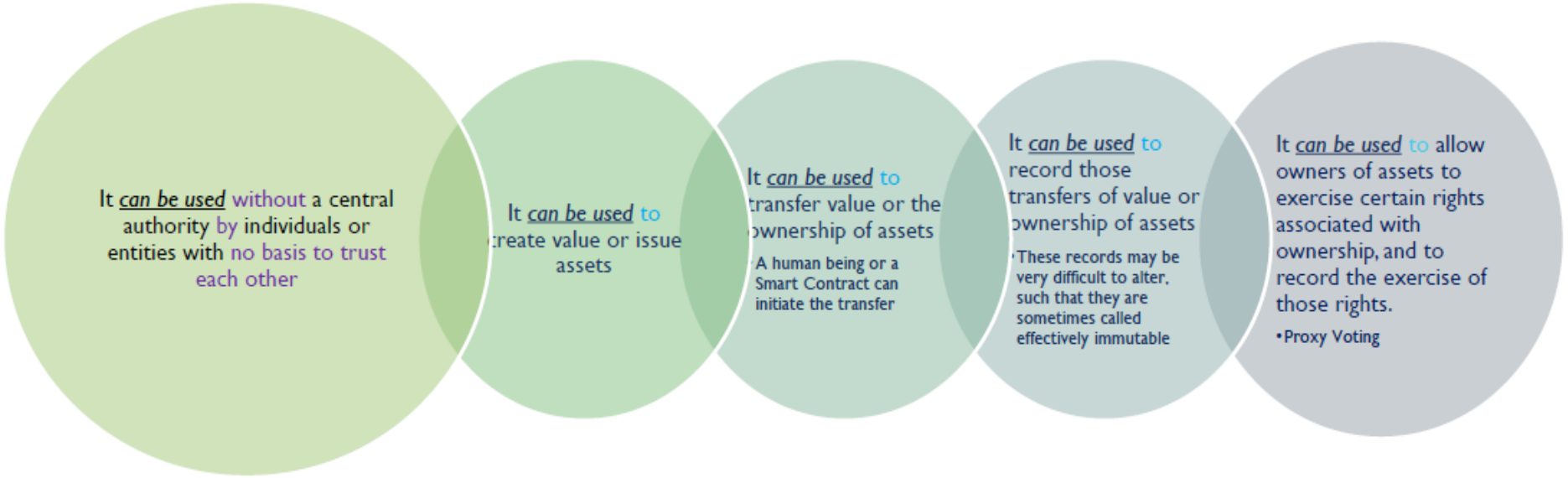


- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving consensus."

HOW MIGHT A DISTRIBUTED LEDGER WORK?



THE POWER OF DISTRIBUTED LEDGERS



The degree of trust between users determines the technological configuration of a distributed ledger.

HOW MIGHT DISTRIBUTED LEDGER PROPOSALS DIFFER?

Participation	*Open*	*Closed*
Permission	*Permissionless*	*Permissioned*
Ledger Design	*One ledger*	*One ledger or Segregated ledgers*
Validation	*Methodology depends on degree of trust between nodes. Where there is no basis for trust, may be achieved through proof of work, which requires the algorithmic solving of a cryptographic hash.*	
Consensus Mechanism	*Mechanism depends on degree of trust between nodes. Where there is no centralized authority, consensus may be determined algorithmically.*	

- Blockchain comprised of;
  - Transactions
  - Immutable ledgers
  - Decentralized peers
  - Encryption processes
  - Consensus mechanisms
  - Optional Smart Contracts

Transactions

- As with enterprise transactions today, Blockchain is a historical archive of decisions and actions taken
- Proof of history, provides provenance

Notable transaction use cases
Land registration – Replacing requirements for research of Deeds (Sweden Land Registration)
Personal Identification – Replacement of Birth/Death certificates, Driver's Licenses, Social Security Cards (Estonia)
Transportation – Bills of Lading, tracking, Certificates of Origin, International Forms (Maersk/IBM)
Banking – Document storage, increased back office efficiencies (UBS, Russia's Sberbank)
Manufacturing – Cradle to grave documentation for any assembly or sub assembly
Food distribution – Providing location, lot, harvest date Supermarkets can pin point problematic food (Walmart)
Audits – Due to the decentralized and immutable nature of Blockchain, audits will fundamentally change.

Demo - https://anders.com/blockchain/blockchain.html

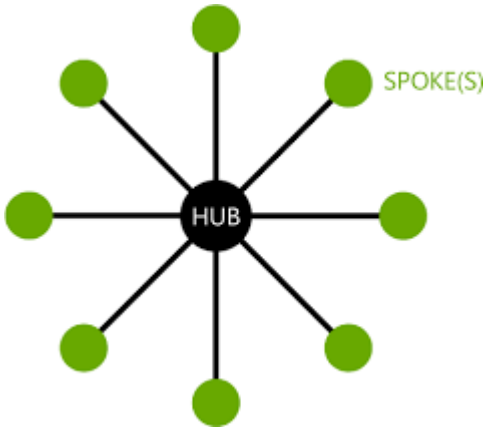
Immutable

- As with existing databases, Blockchain retains data via transactions
- The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.
- The transaction is, immutable, or indelible
- In DBA terms, Blockchains are Write and Read only
- Like a ledger written in ink, an error would be be resolved with another entry

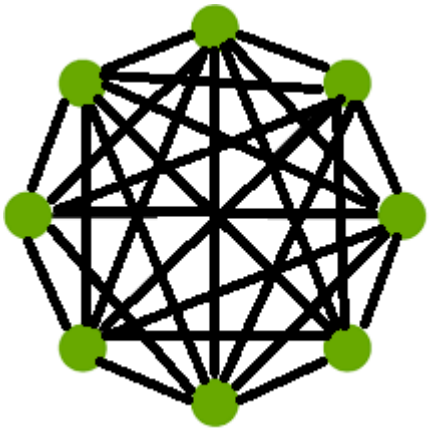
Decentralized Peers

- Rather than the centralized “Hub and Spoke” type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

Legacy Network
Centralized DB



Blockchain Network
Distributed Ledgers



Encryption

- Standard encryption practices
- Some Blockchains allow for “BYOE” (Bring Your Own Encryption)
- Only as good as the next hardware innovation
- All blocks are encrypted
- Some Blockchains are public, some are private
  - Public Blockchains are still encrypted, but are viewable to the public, e.g. https://www.blocktrail.com/BTC
  - Private Blockchains employ user rights for visibility, e.g.
    - Customer – Writes and views all data
    - Auditors – View all transactions
    - Supplier A – Writes and views Partner A data
    - Supplier B – Writes and views Partner B data

Consensus

- Ensures that the next block in a blockchain is the one and only version of the truth
- Keeps powerful adversaries from derailing the system and successfully forking the chain
- Many Consensus mechanisms, each with pros and cons

Consensus Mechanism
Proof of Work
Proof of State
Proof of Elapsed Time
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others….

Smart Contracts

- Computer code
- Provides business logic layer prior to block submission

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

Cutting the Middleman

- Blockchain technology makes middlemen (so-called trusted third parties) obsolete in many applications.
- Bitcoin can serve as an example here. Bitcoins are not routed via a central instance, e.g. a bank, but can be transferred directly between the parties.

Building Consensus

- Blockchain technology has a wide range of applications for consensus building. In a finite timeframe, all participants of the blockchain agree on a proposal, which was worked out by a benign participant.
- At Bitcoin, for example, all participants agree on who owns how many bitcoins. But many applications are also conceivable in industry.

Creating Witnesses

- Finally, a public blockchain can also be used for the automated creation of witnesses. If something is published on a public blockchain, all participants become witnesses.
- This is used, for example, by OriginStamp to create a secure timestamp for documents.

Key Features

A public blockchain has some characteristic features:

- Write-only, immutable, transparent data storage.
- Decentralized, no need for intermediaries.
- Consistent state across all participants.
- Resistant against malicious participants.
- Open to everyone.

Strength

- Tamper resistance and trust-facilitation
- Openness
- Security
- Fault Tolerance

Weaknesses

- Scalability and latency
- Storage requirements
- Privacy
- Inflexibility and complex governance
- Unpredictability of consensus mechanisms

Challenges

Although Blockchain technology has a strong disruptive power and can change many areas of our daily lives, there are still some challenges that need to be addressed.

- The high energy consumption - Bitcoin uses a lot of energy.
- The scalablity issue - Bitcoin supports far less transactions per second than e.g. VISA.
- It opens up possibilities for money laundering - Some blockchains as Monero are anonymous.

KADRENCHE

Presentation on Blockchain Technology by
Sonam Jamtsho, 25th Nov,2019