Professional Blockchain Course

What is Blockchain?

“Blockchain is the tech. Bitcoin is merely the first mainstream manifestation of its potential.”

What is Blockchain?

- Blockchain is a digitized, distributed ledger for all the records.
- A distributed database recording transaction in chronological order.
- Devised initially to power Bitcoin.

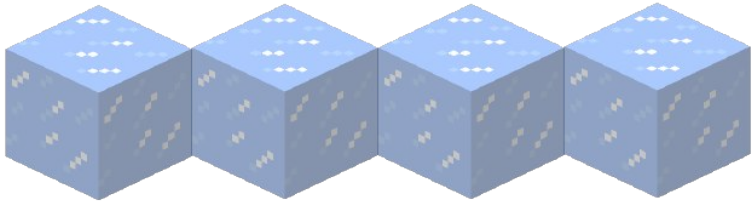
Blockchains are built from 3 technologies		
1. Private Key Cryptography	2. P2P Network	3. Program (the Blockchain protocol)
ECC	Torrent Networks	Hashing Algorithms
RSA	System of Records	Handshake Algorithms

Blockchain Analogies to Real World

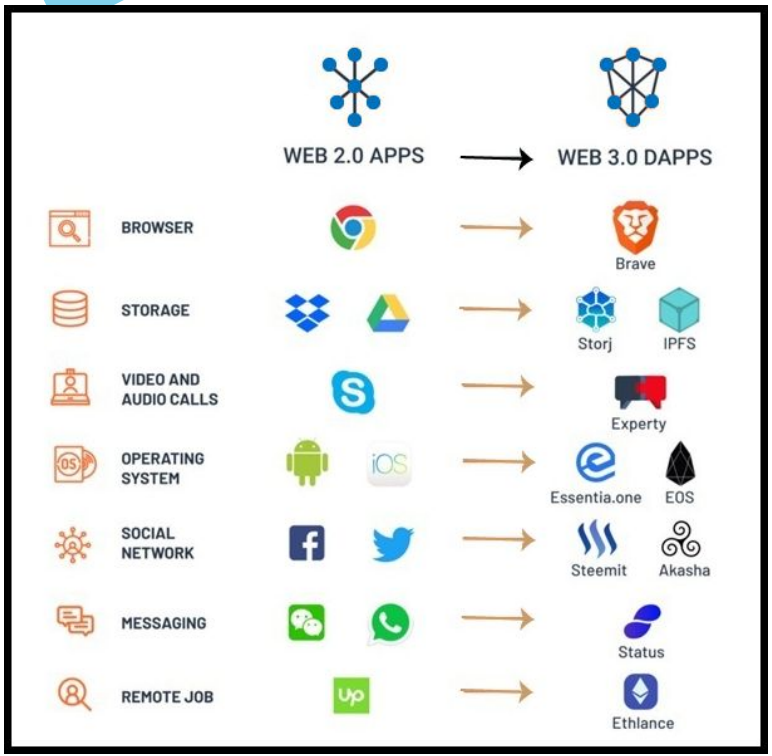
- Transparent Bank Vaults.
- Bank account statements.
- A spreadsheet which is duplicated hundreds of times across the network of computers.
- A large size notebook distributed across all the readers.
- A google doc shared between multiple parties.
- A street soccer game.

Blockchain Analogy

- Imagine a massive vault system from a bank.
- The vault is filled with rows of deposit boxes.
- Each deposit box is made up of glass, allowing everyone to visualize the contents of the deposit box, but only have access to their vault.
- When a person opens a new deposit box, he/she get a key that is unique to that box.
- This is the fundamental concept of cryptocurrencies based on Blockchain. Anyone can see the contents of all other addresses.

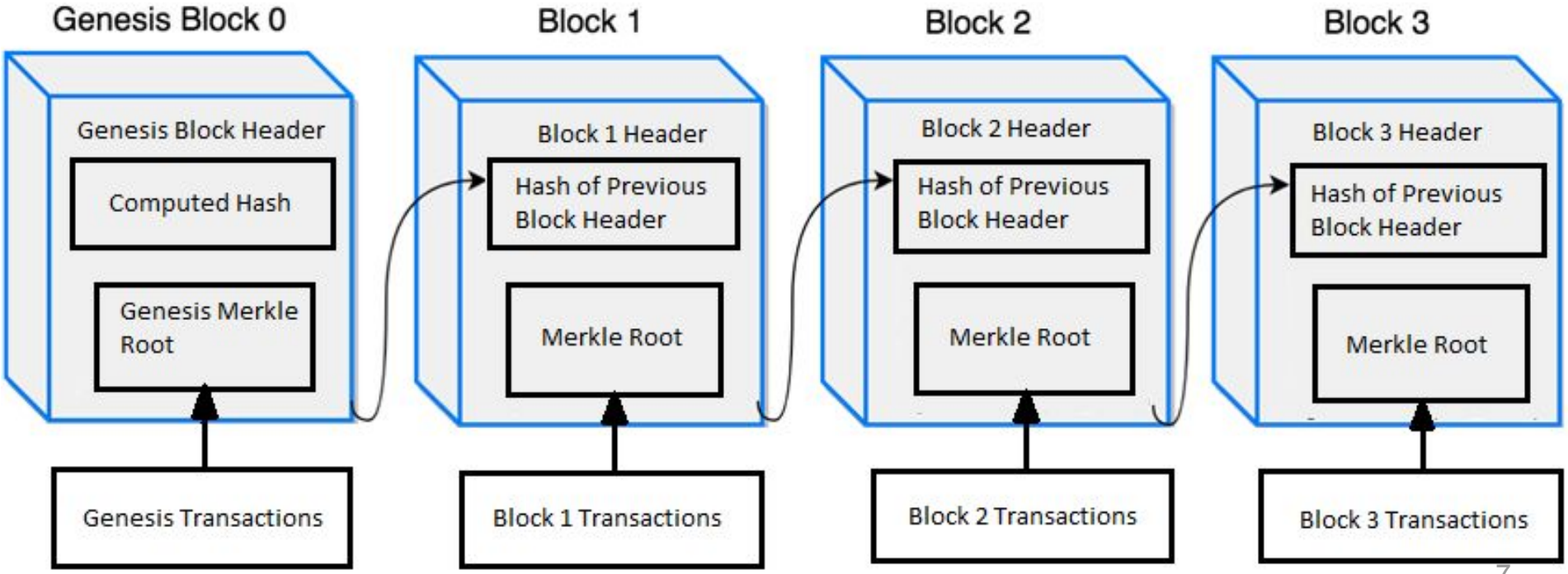


Why Blockchain is Web 3.0?



- No Central point of control.
- Ownership of Data.
- Reduction in Hacks and Data Breaches.
- Uninterrupted Service

Peek Inside Blockchain



Blockchain Characteristics

- Each block is built on top of the previous block and uses the block's hash to form a chain.
- Validating and confirming blocks over the chain is handled by miners.
- Blocks created are cryptographically sealed over the Blockchain, which means that it is nearly impossible to delete and modify data over the Blockchain.
- Consensus algorithms make sure that all the transactions are validated and only added once over the Blockchain.
- Miner receives a reward for running the consensus algorithms; the current reward is 12.5 BTC in case of Bitcoin Blockchain and 2 ETH in case of Ethereum Blockchain.
- All the Blocks added are in chronological order and time-stamped.

Summarising Blockchain

- It’s a digitized store for information in the form of transactions.
- It is distributed. Thus, nobody controls it.
- Consensus algorithms make sure of the security and immutability.
- When a new block is added to a blockchain, it is linked to the previous block using a cryptographic hash.
- Data gets recorded in chronological order.
- Everyone present over the network can view the transactions.

Blockchain Definition:
“A blockchain is a digitized, distributed, consensus-based secure storage of information protected from revision and tampering over the peer-to-peer network.”

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

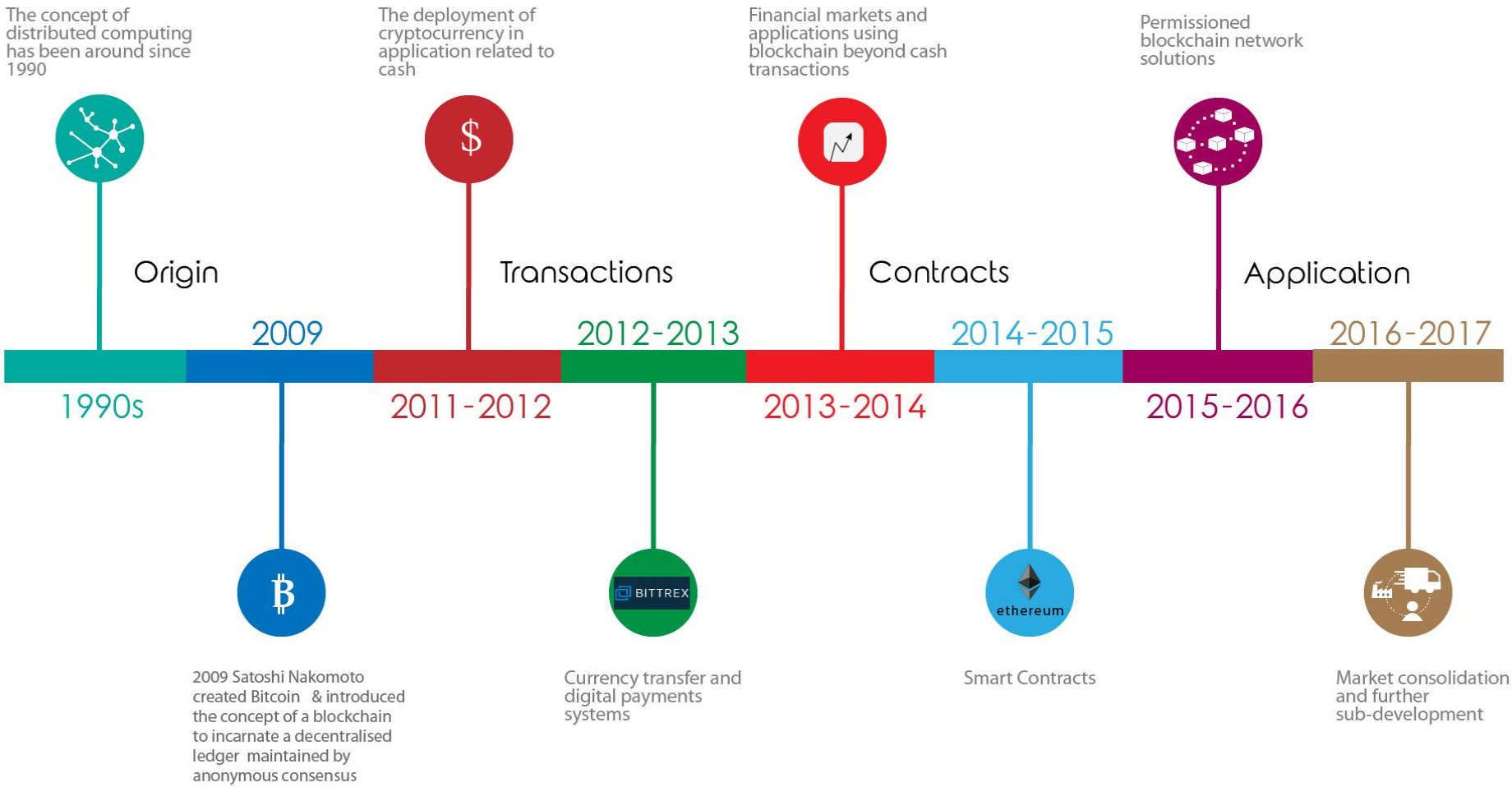
History of Blockchain

Bitcoin Beginnings

- The Blockchain technique was initially described in 1991 with the intent to timestamp digital documents to avoid tampering. It was adapted by Satoshi Nakamoto in 2008 to create the digital cryptocurrency called Bitcoin
- The concept of the Blockchain technology was introduced ten years back.
- The first use case of Blockchain technology was Bitcoin.
- In 2008, Satoshi published the white paper of bitcoin entitled “Bitcoin: A peer to peer Electronic cash system.” It stated that the transaction could take place without involving any third party. This lead to the introduction of the Blockchain technology.
- A few months later a new protocol was released that began the concept of genesis block with 50 coins. It was an open source program and later became a part of the Bitcoin peer-to-peer network.

Rise of Smart Contracts

- Vitalik Buterin, an initial contributor to the Bitcoin codebase, became frustrated around 2013 with the programming limitations of Bitcoin and set out to build the second public blockchain called Ethereum.
- Ethereum can record assets such as funds, boats, cars, or contracts, not just currency.
- Ethereum was launched in 2015 with the functionality of Smart Contracts that can automatically perform logical operations based on a set of criteria established in the blockchain.
- For example, a smart contract can be created to make a bet on tomorrow's weather. You and opposition would upload the contract to the Ethereum blockchain and then send some digital currency, which the software would permanently hold. The next day, the smart contract would check the weather and then post the earnings to the winner.


The concept of distributed computing has been around since 1990
The deployment of cryptocurrency in application related to cash
Financial markets and applications using blockchain beyond cash transactions
Permissioned blockchain network solutions
Origin
Transactions
Contracts
Application
1990s
2009
2011-2012
2012-2013
2013-2014
2014-2015
2015-2016
2016-2017
BITTREX
ethereum
2009 Satoshi Nakomoto created Bitcoin & introduced the concept of a blockchain to incarnate a decentralised ledger maintained by anonymous consensus
Currency transfer and digital payments systems
Smart Contracts
Market consolidation and further sub-development

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

How Blockchain works?

How Blockchain Works?

- Let's imagine that ten people in one room decided to make their currency. They need to know the flow of the funds. One person – let's call him Dave– chose to keep a list of all actions in a diary:

1. Alice gave 3 coins to Carol
2. Carol gave 5 coins to Chuck
3. Chuck gave 3 coins to Eve
4. Eve gave 1 coin to Bob
5. .....

How Blockchain Works?

- One man – let's call him Chuck – decided to steal money. To hide this, he changed the entries present in the diary:

1. Alice gave 10 coins to Carol
2. Carol gave 5 coins to Chuck
3. ~~Chuck~~ Carol gave 3 coins to Eve
4. Eve gave 1 coin to Bob
5. .....

How Blockchain Works?

- Dave noticed that someone had interfered with his diary. He decided to stop this from happening. He created a program called a Hash function that turns text into a set of numbers and letters as in the table below:

Attack	4CD548F3CC29CF9C99A0134A971B1BE03C8F6BF80BA8F03E174E030B0D292396
Can't Attack	88F5E3FED928950C36A67A11CA068F38CCB2E7DA01421C087BC11C842C869282
Can Attack	4AB7698451F8A85580ABED2E2BC94F6CCF05B6B95A587C2BFD771CCDCB4E450D

How Blockchain Works?

A hash is a fixed string of alphanumeric characters, created by a hash function. A hash function is a mathematical function that takes a variable number of string characters and converts them into a fixed number of alphanumeric characters. Even a small change in a line creates an entirely new hash.

- After each record, he inserted a hash. The new diary was as follows:

6. Alice gave 10 coins to Carol

7C9A5C77D3D2FD537469685A3530A6EC07C
E0F6E69C29BDB7C66D14C8448C44F

7. Carol gave 5 coins to Chuck

F71E69770F15BE2831F345B9C25B294C7CEA
8A85C9B7B237773949702F8EE88F

How Blockchain Works?

- Chuck decided to manipulate entries again. He got to the diary at night, changed the record and generated a new hash.

6. Alice gave 10 coins to Carol

7C9A5C77D3D2FD537469685A3530A6EC07C
E0F6E69C29BDB7C66D14C8448C44F

7. Carol gave ~~5~~ 8 coins to Chuck

~~**F71E69770F15BE2831F345B9C25B294C7CEA**~~
~~**8A85C9B7B23777394702F8EE88F**~~

787CCB59661D1D0A7F79C0EE5C2467810941
6F510A2DFB3FD4A9D368EFD2D851

How Blockchain Works?

- Dave noticed that somebody had sifted through the diary again. He decided to complicate the record of each transaction. After each record, he inserted a hash generated from the record+last hash. So each entry depends on the previous.
- If Attacker tries to change the record, he will have to change the hash in all previous entries.

How Blockchain Works?

Input	Hash
Alice gave 10 coins to Carol	7C9A5C77D3D2FD537469685A3530A6EC 07CE0F6E69C29BDB7C66D14C8448C44F
Carol gave 5 coins to Chuck 7C9A5C77D3D2FD537469685A3530A6EC 07CE0F6E69C29BDB7C66D14C8448C44F	F71E69770F15BE2831F345B9C25B294C7 CEA8A85C9B7B237773949702F8EE88F
Carol gave 3 coins to Eve F71E69770F15BE2831F345B9C25B294C7 CEA8A85C9B7B237773949702F8EE88F	5C19F496C977AA7798EFF57C939B3AE5E FB442B69D63CAFE8D41203884C5BAC1
Eve gave 1 coin to Bob 5C19F496C977AA7798EFF57C939B3AE5E FB442B69D63CAFE8D41203884C5BAC1	C4BDA779BE74375BC6FF1FFE6DC158EDB D645E8BAB0F1334AEA39EA061D853D0

How Blockchain Works?

- Chuck wanted more money, and he spent the whole night counting all the hashes.
- Finally changing all the hash entries accordingly. He replaced all the hashes with the corresponding cheat hashes.

How Blockchain Works?

- Dave did not want to give up. He decided to add a random number after each record. This number is called “Nonce.” Nonce should be chosen so that the generated hash ends in two zeros.

Input	Hash
Alice gave 10 coins to Carol 247	2B9E9A4B5D5ED6150F4AF78A09331C0A90748D839B3FA87560A1FDCDE408E200
Carol gave 5 coins to Chuck 511 2B9E9A4B5D5ED6150F4AF78A09331C0A90748D839B3FA87560A1FDCDE408E200	3B2DA269E0194EDCE20949F17A4253E8239403693D19E58EF3F80BEE97C40A00
Carol gave 3 coins to Eve 146 3B2DA269E0194EDCE20949F17A4253E8239403693D19E58EF3F80BEE97C40A00	22779476E592C8437CCD03B4D06E2CA851F673AE4A1741300FF75A6749BCA500
Eve gave 1 coin to Bob 171 22779476E592C8437CCD03B4D06E2CA851F673AE4A1741300FF75A6749BCA500	360FF6414D739B9DCB38164C8FE46372F2ACA9E1640D29B5DEC2824733EA1B00

How Blockchain Works?

- Now, to forge transactions, Chuck would need to spend hours choosing Nonce for each line.
- More importantly, its very hard for even the computers to figure out the nonce quickly.
- Sometime after, Dave realized that there were too many transaction records and that he couldn't keep the diary like this forever. After reaching 10,000 transactions, he converted them to a one-page spreadsheet. Carol checked that all transactions are right.
- Dave spread his spreadsheet diary over 10,000 computers located globally.
- These computers are called nodes. Every time a new transaction occurs, it has to be validated by the nodes.
- Once every node has received/checked a transaction there is a sort of electronic vote, as some nodes may think the transaction is valid and others believe it is a fraud.
- Now, if Chuck changes one entry, all the other computers will have the original entries. They would not allow fraud entries to occur.

Summarising

- This spreadsheet created in the example is called a block.
- The whole chain of blocks is collectively called as Blockchain. Every node holds a copy of the Blockchain. Once a block reaches a certain number of approved transactions, then a new block is formed.
- The Bitcoin Blockchain updates itself every ten minutes.
- As soon as the spreadsheet or ledger or registry is updated, it can no longer be changed. Thus, it’s impossible to forge it.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Wallet, Digital Signatures, Protocols

Wallets

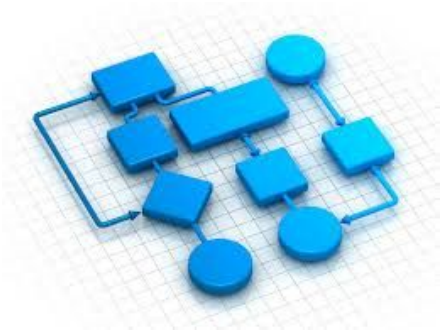
- A blockchain wallet is similar to a digital wallet that allows participants to manage their cryptocurrencies.
- A wallet lets the users generate the private key and public address.
- The private key is used to send the transaction, and public address is used to receive the transaction.
- No visible records of identity about who did what transaction with whom, only the address of a wallet is visible in the transactions.
- Types of Blockchain wallets are:
  - Paper wallets
  - Web wallets
  - Mobile wallets
  - Desktop wallets
  - Hardware wallets
  - Physical wallets

Digital Signatures

- Digital signatures similar to real signatures are a way to prove that somebody is who they say they are.
- Digital signatures use cryptography which is more secure than handwritten signatures.
- The private key is used to sign messages digitally.
- The recipient can verify using the sender's public key.
- Every transaction that is executed on the blockchain is digitally signed by the sender using their private key.
- SSL is an example of a digital signature.

Protocols

- Every Blockchain consists of behavior specifications that are programmed into it.
- Protocols define the Blockchain
- The private key is used to send the transaction, and public address is used to receive the transaction.
- Some examples of protocols:
  - Input information for every hash number has to include the previous block's hash number.
  - The reward for successfully mining a block decreases by half after every 210,000 blocks are sealed-off.
  - To keep the amount of time needed to mine one block at approximately 10 minutes, mining difficulty is adjusted every 2,016 blocks.



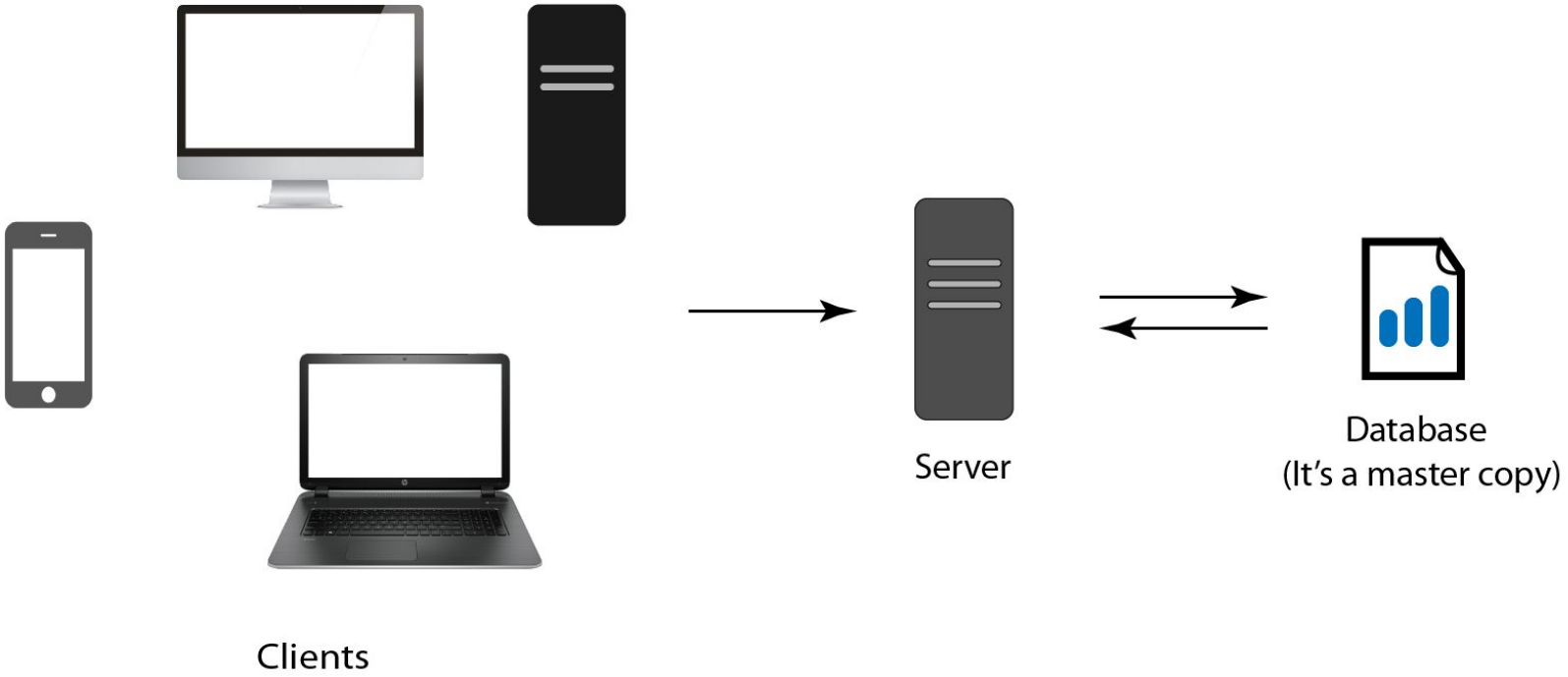
THANK YOU

For more information contact
info@we2blocks.com

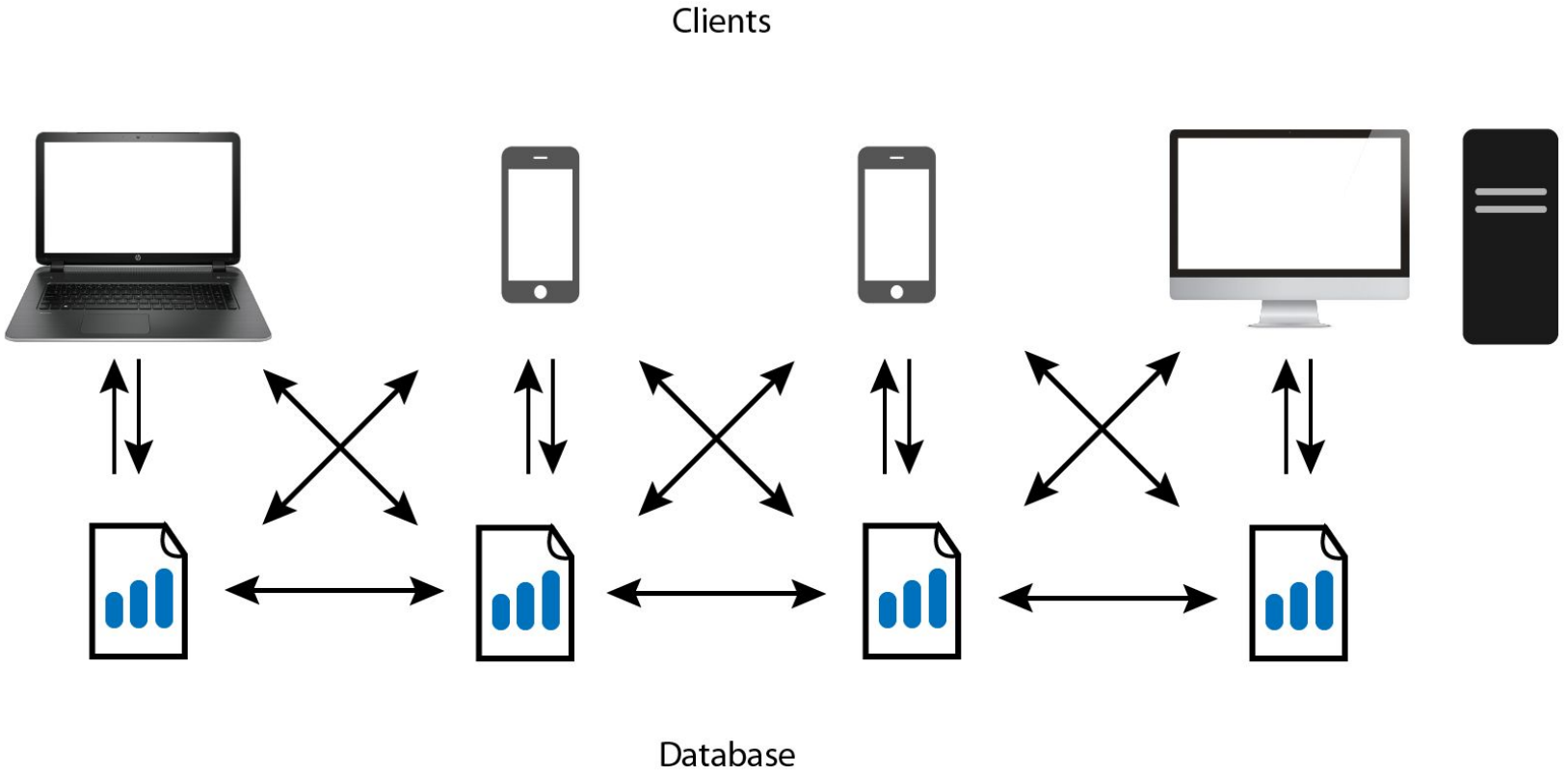
Professional Blockchain Course

Benefits over Traditional Technologies

Traditional Technology



Blockchain Technology



Decentralized Control

- Blockchains allow multiple parties that do not trust each other to share information without requiring a central control.
- It eliminates the risks of centralized control. With a centralized database, anybody with sufficient access to the system can destroy or corrupt the data within.
- Cost savings are also provided; usually billions of dollars are spent on safeguarding central repositories from hackers.
- Blockchain provides a same shared system of record simultaneously for everyone who is connected to the network.
- The trust is established by the Cryptographic protocols running behind the Blockchain technology.
- All the parties must agree to make a change in Blockchain which is nearly impossible.

Integrity and Transparency

- Blockchain technology distinguishes it from traditional database technology as it is publicly verifiable, which is enabled by integrity and transparency.
- Every user can be sure that the data they are retrieving is uncorrupted and unaltered since the moment it was recorded.
- Every user can verify data appended over the blockchain.
- Blockchain grows like ever-expanding archives of their history while also providing a real-time portrait.
- Merkle tree ensures the integrity of the data by hashing the transactions to a single root.

Confidentiality

- The blockchain is an openly distributed ledger, yet a private system can be established to maintain confidentiality.
- Data confidentiality in blockchains ensure that individuals or organizations who are prevented from accessing data are not authorized to access it.
- Permissioned blockchains have emerged as an alternative to public ones to address enterprise needs for having known and identifiable participants.
- Solutions like Hyperledger Fabric Blockchain and Block Stream offers rich sets of permissions to maintain confidentiality in the system.

Enhanced Security

- Transactions are encrypted and linked to the previous transaction.
- Information is stored across a network of computers instead of on a single server.
- Blockchain prevents fraud and unauthorized activity.
- Cryptography protocols make sure that the data is thoroughly secure.
- Safeguard from DOS attacks as the data is present on all the nodes connected to the network.
- Cryptographic fingerprint(hash of the block) is unique for each block.

Faster Processing

- Traditional banking process takes days to settle, but the Blockchain has reduced that time nearly to minutes or even seconds.
- Everyone has access to the same information, and it becomes easier to trust each other without the need for numerous intermediaries.
- Moreover, tracking of products could also be made efficient by uploading the data on Blockchain.
- Digital assets and the trustless system makes sure that the data is protected and transacted efficiently.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

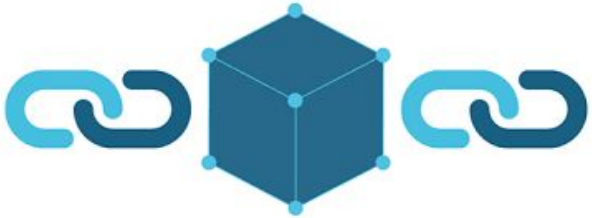
Bitcoin vs Blockchain

Bitcoin

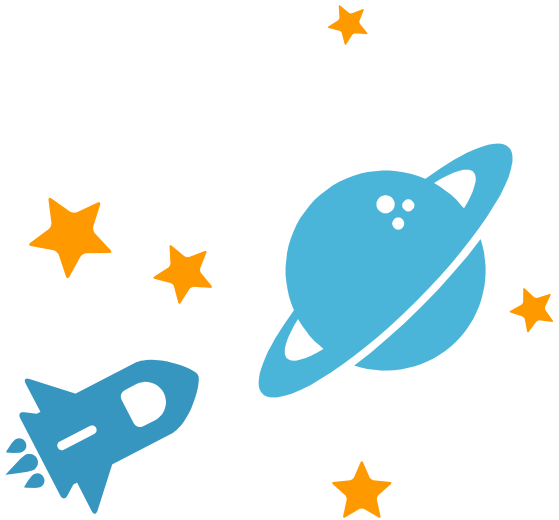
- Bitcoin is a cryptocurrency, created and held digitally on your PC or in a virtual wallet.
- It is decentralized, so no person, institution or bank controls the currency.
- An implementation of Blockchain.
- It was started in 2009 to get rid of third-party payment processing intermediaries.
- The blockchain is the underpinning technology that maintains the Bitcoin transaction ledger.
- In simple words “It’s gold for nerds.”

Blockchain

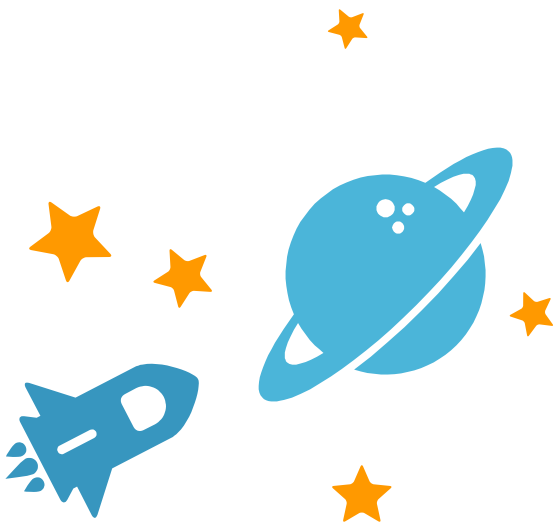
- A blockchain in the core is a distributed database of records.
- Each transaction in the public ledger is verified by consensus.
- Transactions are encrypted and cannot be replicated or altered.
- Currently, the most famous blockchain application is the Bitcoin blockchain.
- Blockchain can easily transfer everything from property rights to stocks and currencies without having to go through an intermediary.
- In simple words “Blockchain is the tech. and Bitcoin is merely the first mainstream manifestation of its potential.”



BITCOIN IS A MIRAGE



BLOCKCHAIN HOLDS PROMISE



THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Key Concepts

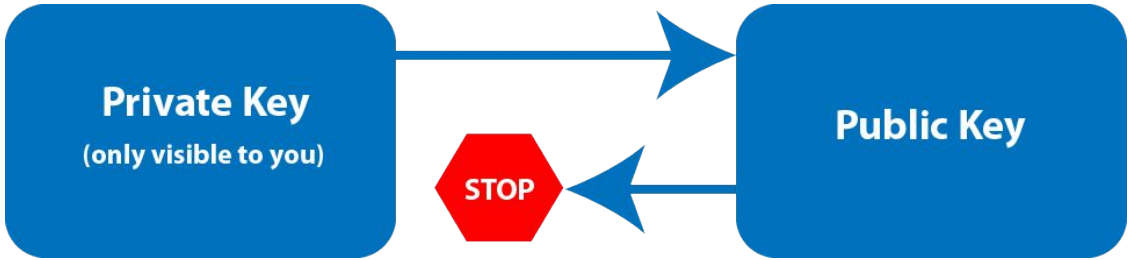
Keys

Private Keys

- Private Key is used to generate a signature for each transaction over the blockchain.
- The generated signature is used to confirm that the transaction has come from a specific user, and also prevents the transaction from being altered by any malign entity.
- In simple words - “Private Keys are used to sign the cryptocurrencies you send to others.”
- If someone obtains your private key, they would be able to send your cryptocurrencies to themselves, which has happened in most of the hacks around the world.
- Example: **L34EXrFCuxQCorfE66sxQe8Tyh71SyU8cc9z7HnbEWwW8YsgbvTw**

Public Keys

- The Private Key is used to derive the Public Key mathematically.
- Public Keys are practically irreversible, i.e., you can easily derive public key from the private key, but it would take millions of years to do the vice versa.
- Public Keys can be distributed to everyone.
- Example:
  0237F49F4CCF760BF5FA993616E63B7B2A8611AB71AE7630386738B3BC4D1B84FD



Addresses

- A cryptocurrency address in a core is a representation of the public key.
- One-way cryptographic hash functions are used to derive address from the public key.
- For example in Bitcoin, the algorithms that are being used to generate a bitcoin address from the public key are the Secure Hash Algorithm 256 (SHA-256) and the RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160)
- The address appears typically in a transaction between two parties, with the address signifying the recipient of the funds.
- Example: **1JPgMJuAvYJU6mxxbJdmf1XBd7bBPdPV3a**

Private Key

Large, randomly generated number

Public Key

Generated from Private key

Address

Generated from Public key

Transactions

- Transactions are records of data in chronological order
- Transactions are stored in a Merkle tree inside the Block.
- The transactions, when submitted, are picked up by the blockchain network and is inserted into a ‘pool of unconfirmed transactions.’ The transaction pool is a collection of all the transactions on that network that have not been confirmed yet.
- Miners on the network select transactions from this pool and add them to their ‘block.’
- Transactions also contain metadata information which can be utilized to store data over the Blockchain.

What are Blocks?

- A Block is a container data structure which contains a set of confirmed transactions.
- A block could contain different information, and a chain of these blocks evolves into a blockchain as long as it links one and the other.
- The blocks are stored on the hard drives of many miners spread across the globe on a peer to peer network.
- In the Bitcoin algorithm, a block is created every 10 minutes. All the transactions happening over the network within 10 minutes interval are crunched into that block and added to the chain.

Structure of Blocks

All blocks in the Blockchain are composed of a header, identifiers and a long list of transactions. The structure of a block is as follows:

- Block Header
- Block identifiers
- Merkle Trees

Structure of Blocks

An Example of Bitcoin Blockchain

Field	Description	Size
Magic No	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction Counter	positive integer VI = VarInt	1 - 9 bytes
Transactions	The (non empty) list of transactions	Transaction counter-many transactions

Block Header

The header contains metadata about a block. There are three different sets of metadata:

- The previous block hash. In a blockchain, every block is inherited from the last block because we use the previous block's hash to create the new block's hash.
- Mining competition for the network. For every block to be part of the blockchain, it needs to be given a valid hash. This contains the values for the timestamp, the nonce, and the difficulty.
- Merkle tree root. This is a data structure to summarise the transactions inside the block.

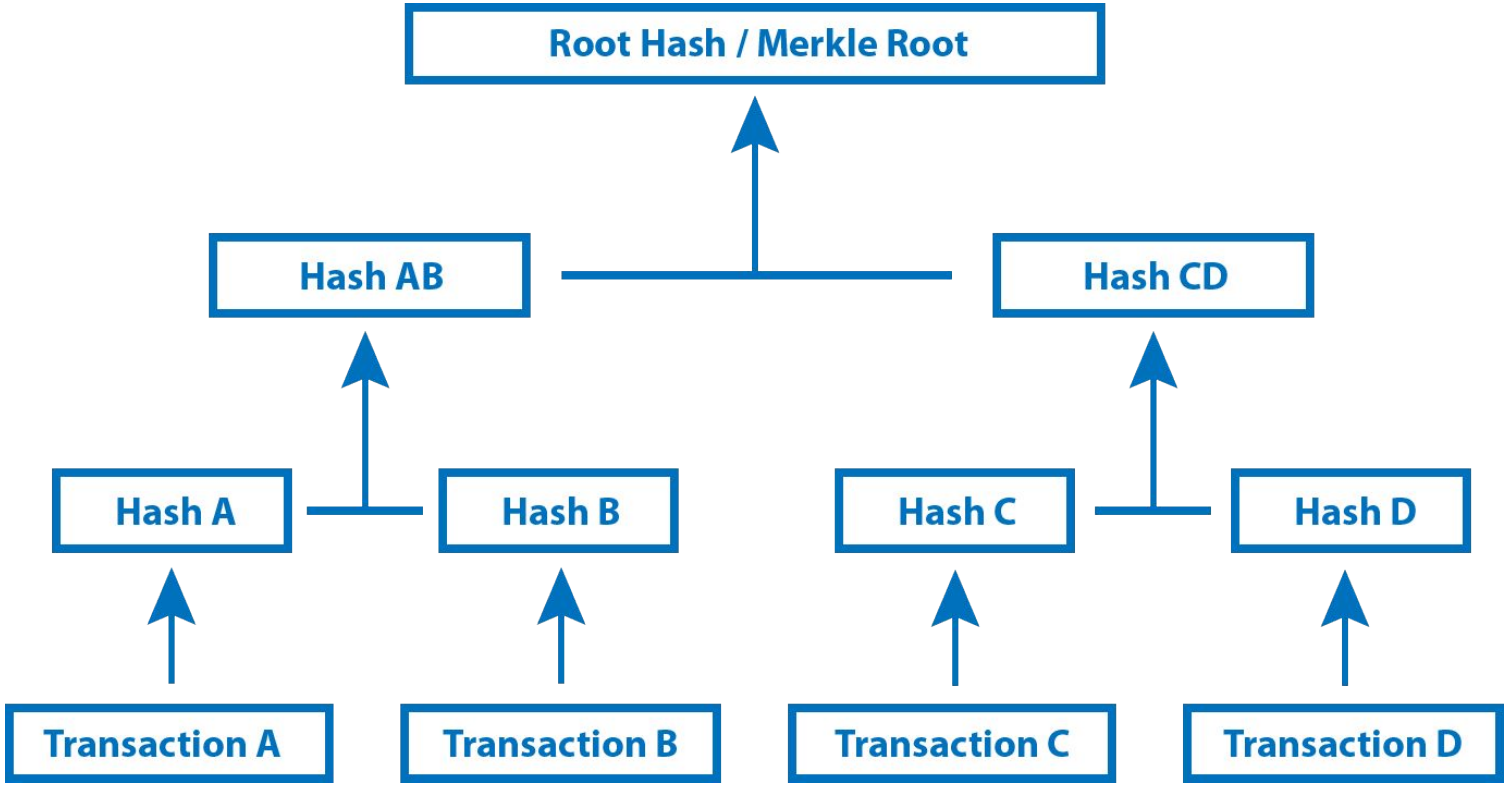
Block Identifier

- To identify a block, we need to have a cryptographic hash, a digital signature. This is created by hashing the block header twice with the SHA256 algorithm in case of Bitcoin Blockchain. You can use different hash functions for your Blockchain.
- Every block uses the last block's hash to construct its hash.
- Another way to identify a specific block is the block height. This is the position of the block in the blockchain.
- For example, if we say the block is in the 7312 position. This means that there are 7311 blocks before this one.

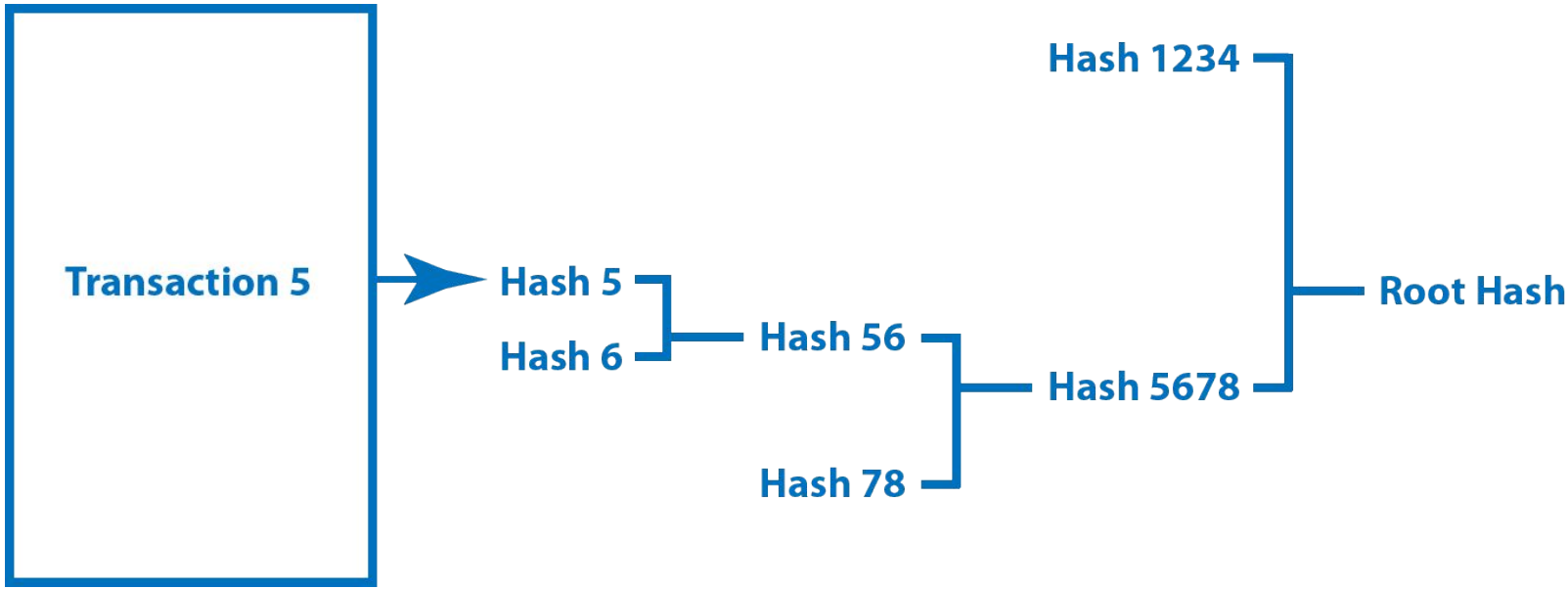
Merkle Tree

- A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions.
- The user can verify whether or not a transaction is included in a block.
- Merkle trees are created by repeatedly hashing pairs of nodes until there is only one hash left which is called the root hash.
- Each leaf node is a hash of transactional data, and each non-leaf node is a hash of its previous hashes.
- Merkle trees are binary and therefore require an even number of leaf nodes.
- If a single detail in any of the transactions or the order of the transaction's changes, so does the Merkle Root.

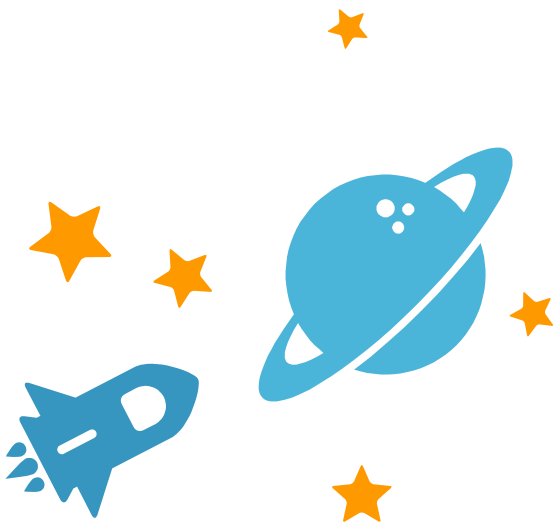
Merkle Tree



Merkle Tree



ADDITIONAL CONCEPTS



HD Private Key

- Hierarchical deterministic is a type of deterministic cryptocurrency wallet derived from a known seed, which allows for the generation of child keys from the parent key.
- The child key is generated from a known seed. There is a relationship between the child and parent keys that is invisible to anyone without that seed.
- The BIP 32 protocol can generate a nearly infinite number of child keys from a deterministically-generate seed from its parent.
- You can recreate those same child keys as long as you have the seed.
- The child key can operate independently, and the parent key can monitor and control each child key.

Mnemonics Seed

- A mnemonic seed is used to substitute either a 12, 18 or 24-word phrase for the private keys which can easily be memorized by human mind compared to hex encoded format.
- Mnemonic word phases are tied with the private keys and support wallet restoration.
- This provides additional security for the user, as well as a convenient solution to recover a wallet.
- BIP 39 introduced the mnemonic wallet implementation.
- The English wordlist for BIP 39 contains 2048 words, so to crack a 12-word phrase, it would require figuring out 2048^12 = 2^132 possible combinations under a shield of 128-bit security.

Smart Contracts

- Smart Contracts are the digital contracts signed between two parties and stored over the immutable ledger.
- Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.
- Contracts can be encoded on any blockchain, but Ethereum is mostly used since it gives unlimited processing capability.
- Hyperledger is also providing chain codes which are very similar to Smart Contracts.
- Example: Renting an apartment.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

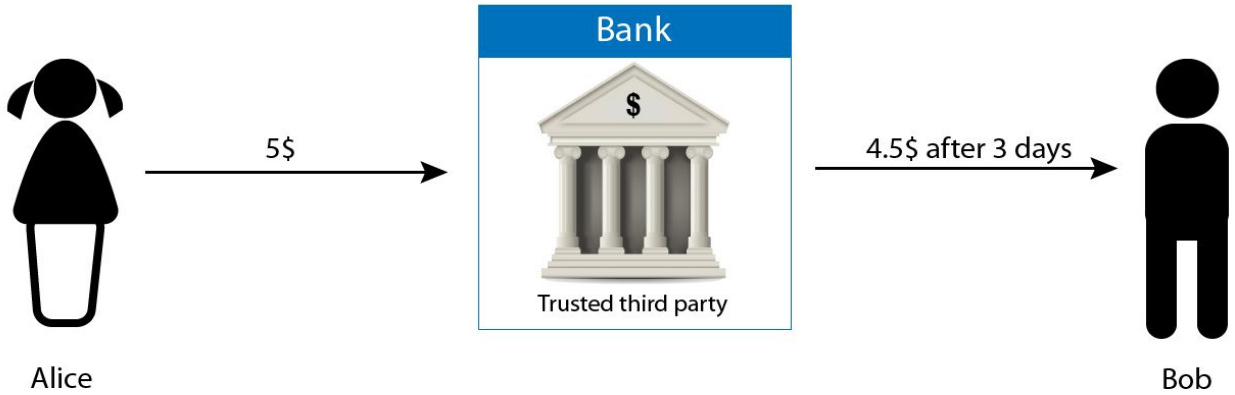
How Blockchain transaction works?

Present Solution with Example

- Alice in the US wants to send $5 to Bob in Australia
- She will make use of net banking or any other payment services like PayPal.
- The 3rd party services will take 3-4 days for cross-border transaction and charges a cut let’s say $0.5.
- Moreover, Alice cannot see the whole process of her transaction execution.

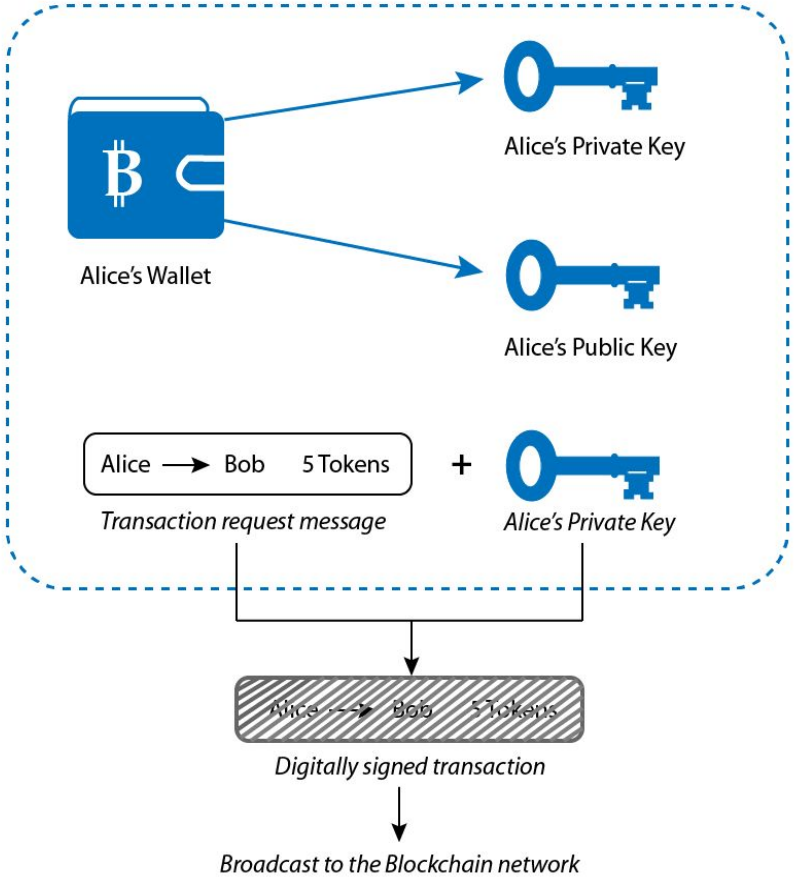
Problems with Present Solution

- The transaction costs are high with 3rd parties involved.
- The time taken for the process is also slow.
- Imagine a scenario where Alice needs to transfer a large sum of money for some medical operations. This will take time and charge massive cost over the transaction.
- Can we do the same things removing the present problems?

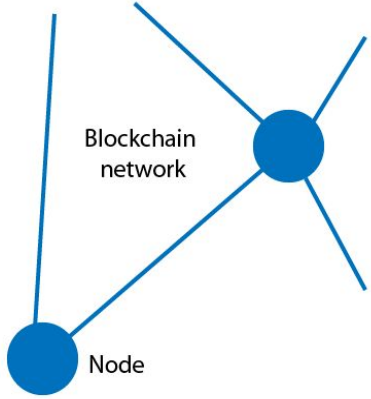


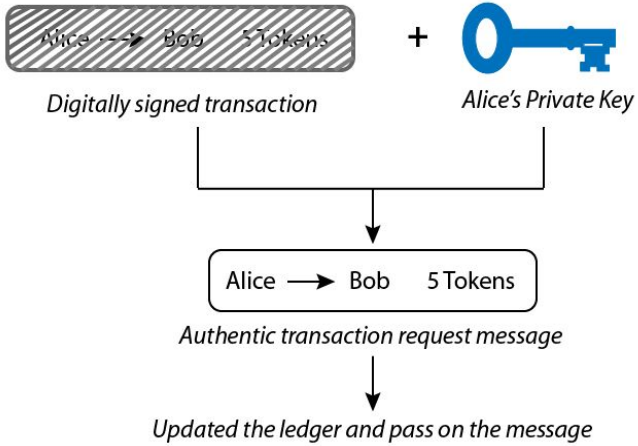
Blockchain for the save

- Blockchain uses a ledger, a digital file/database that keeps track of all transactions.
- Ledger file is not stored over a central server. It is distributed globally via a network of private computers that are both storing data and executing computations.
- If Alice wants to send money to Bob, she broadcasts a message to the network that says the amount of Cryptocurrency in her account should go down by 5 Tokens/5 $, and the amount of Bob's account should go up by the same quantity.
- Each node connected in the network will receive the message and apply the requested transaction to their copy of the ledger, thus updating the account balances.



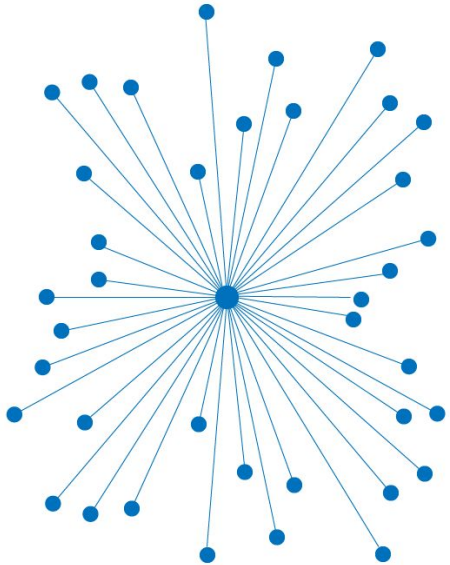
Private area:
The information which can be seen on the blockchain are the digital signature, transaction and Alice's public key.



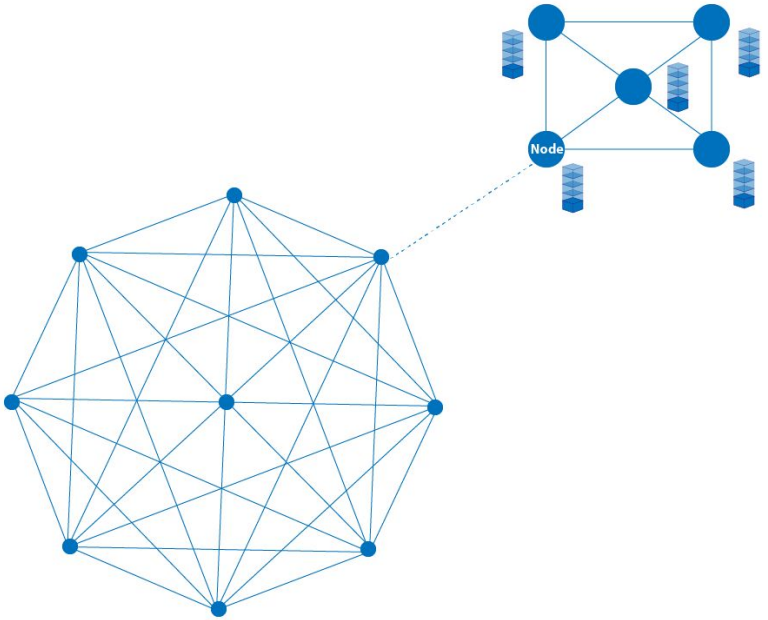


Transaction Distribution

All transactions are distributed in blocks and all nodes hold all transactions



Centralized



Distributed Ledger
Shared Ledger

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Consensus Mechanisms

What is Consensus?

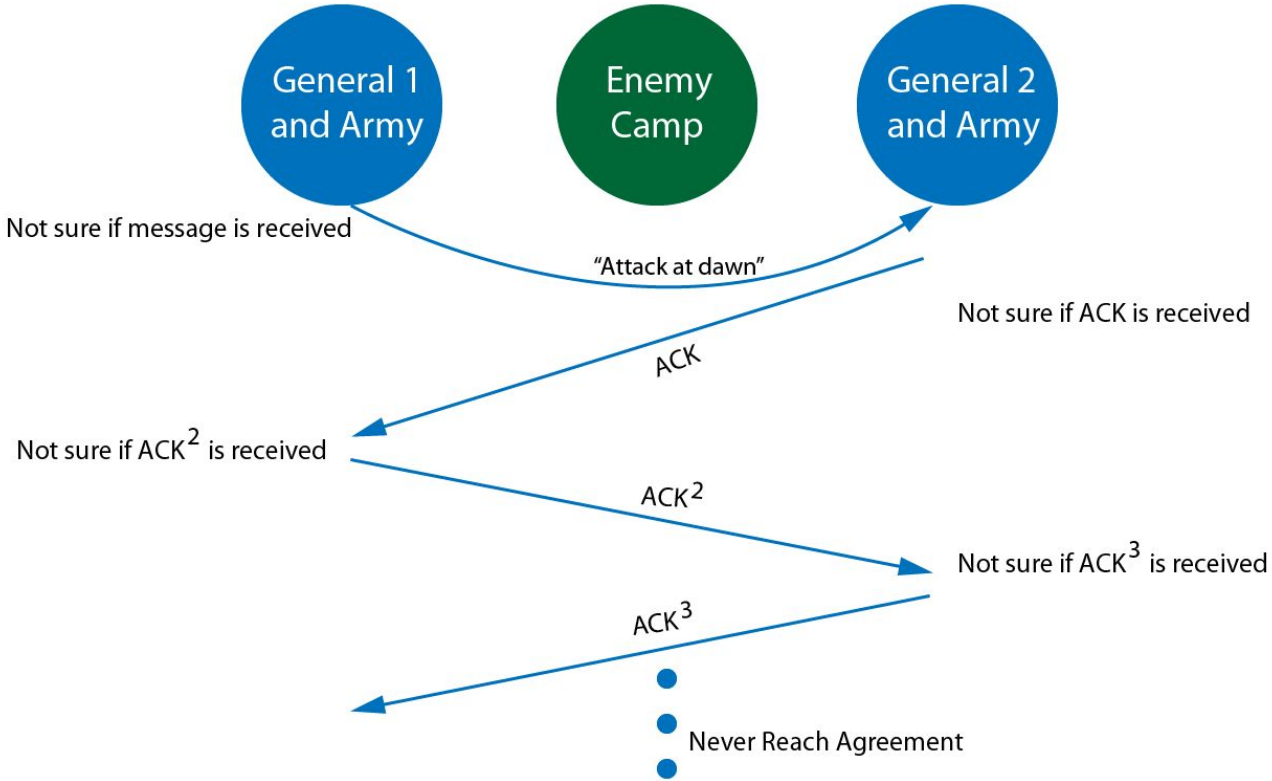
- Blockchains are decentralized systems which consist of different participants who act depending on incentives they receive and the information that is available to them.
- When a new transaction gets broadcasted on the network, nodes connected to the network have the option to either include that transaction to their copy of ledger or to ignore it. When the majority of the nodes which comprise the network decide on a single state, the **consensus** is achieved.

Let’s dive into 2 Generals Problem and understand the consensus better.

Two Generals Problem

- This problem describes a scheme where two generals are attacking a prevalent enemy. General 1 is considered the leader and the other general is regarded as the follower.
- Each general's army on its own does not have the strength to defeat the enemy army; thus they need to collaborate and attack at the same time.
- For them to collaborate and agree on a time, General 1 needs to send a messenger across the enemy's territory that will provide the time of the attack to the other General. However, there is a probability that the messenger will get captured by the enemies, and thus the message won't be delivered. This will result in General 1 attacking while General 2 and his army hold their ground.
- Even if the first transmission goes through, General 2 has to acknowledge that he has received the news, so he sends a messenger back, thus repeating the previous scenario where the messenger can get caught. This extends to infinite message exchange, and therefore, the generals are unable to reach an agreement.

Two Generals Problem



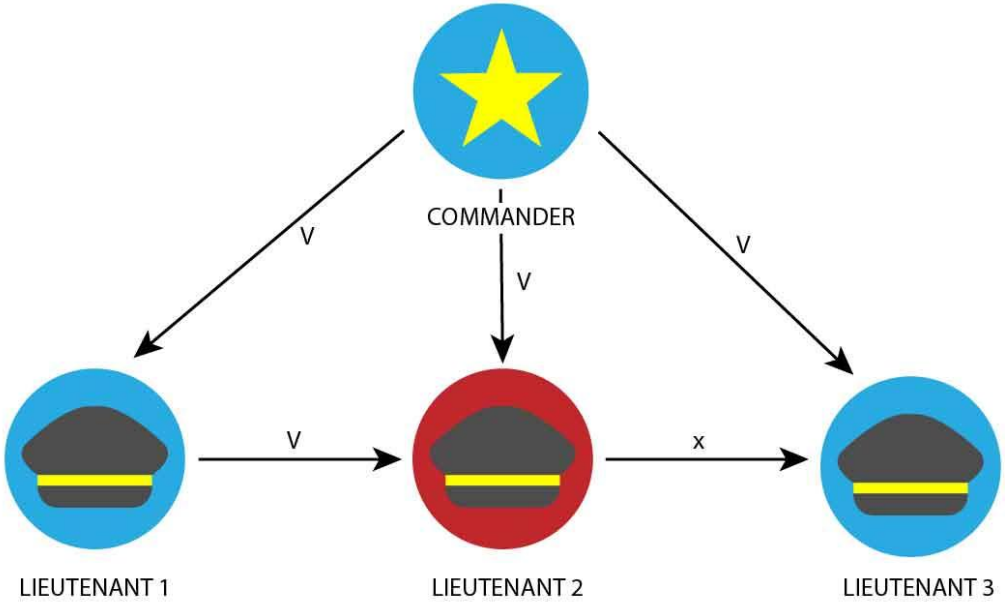
Byzantine Generals Problem

- A more generalized version of the Two Generals Problem describes more than two generals agreeing on the time of the attack. Additionally, one or more generals can be the traitors, meaning that they can lie about their attack choice (e.g., they say that they agree to attack at 5 am, but instead they do not attack).
- To reach a consensus here, the commander and all the lieutenants must agree on the same decision.
- Let's change the scenario to a Commanding General and Lieutenants based approach. So when General issues an order, every loyal Lieutenant will follow the same to attack.
- If the commander is a traitor, the consensus is still achieved. As a result, all lieutenants take the majority vote over the Default value.
- This implies that the algorithm can reach a consensus as long as 2/3 of the actors are honest. If the traitors are more than 1/3, the consensus is not reached, the armies do not coordinate their attack, and the enemy wins.

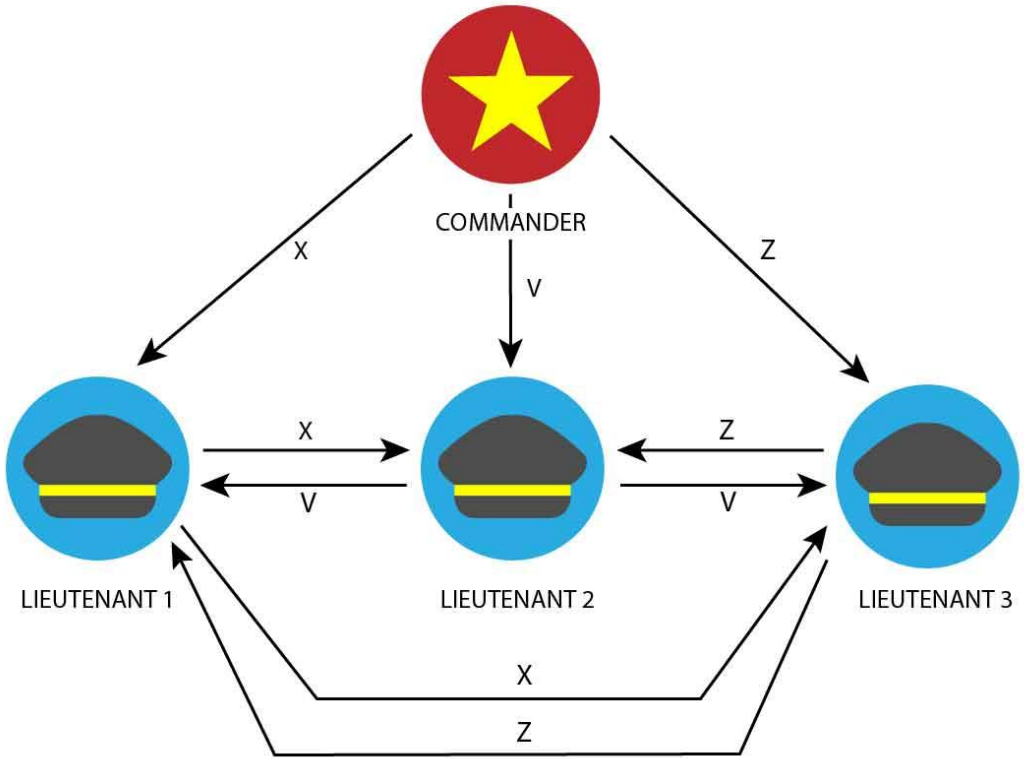
Explanation with Example

- Take an example; every Lieutenant needs to convey orders within 10 minutes. In other words, 10 minutes are required for communicating a message for an attack.
- Moreover, the passing of messages is related to appending the message and then sending them to the next Lieutenant.
- Example:
- General - Attack at 3 am
- Lieutenant 1 - Attack at 3 am, Attack at 3 am
- Lieutenant 2 - Attack at 3 am, Attack at 3 am, Attack at 5 am
- As you can see if the Lieutenant 2 is a traitor, then the 3rd Lieutenant can verify that the incoming message is not in synchronization.
- Moreover, if Lieutenant 2 decides to change all the previous messages too, then each message would take 10 minutes thus Lieutenant 2 will be working for 30 mins.
- But Lieutenant 3 expects the message to come in 10 minutes, thus again giving in that Lieutenant 2 is a traitor.
- If the commander is a traitor, then he might send different orders to different Lieutenants, which will come into consensus but since the messages don't follow the structure of providing in the same attack time, the default option of retreat will come to action.

When Lieutenant is a Traitor



When Commander is a Traitor



How does it relate to Blockchain?

- Blockchains are decentralized ledgers which are not controlled by a central authority. Due to the value stored in these ledgers, bad actors have substantial economic incentives to try and cause faults.
- Proof-of-Work is a probabilistic solution to the Byzantine Generals Problem as described in depth by Satoshi Nakamoto.
- It follows the longest chain rule where miners shift to the chain which is being more worked upon.
- When a miner solves the puzzle and confirms the block, all the nodes in the network will verify if the block is valid and add it to their copy of the chain. The nodes first need to reach a consensus on the validity, only then the network will synchronize, and the state of the blockchain will update.

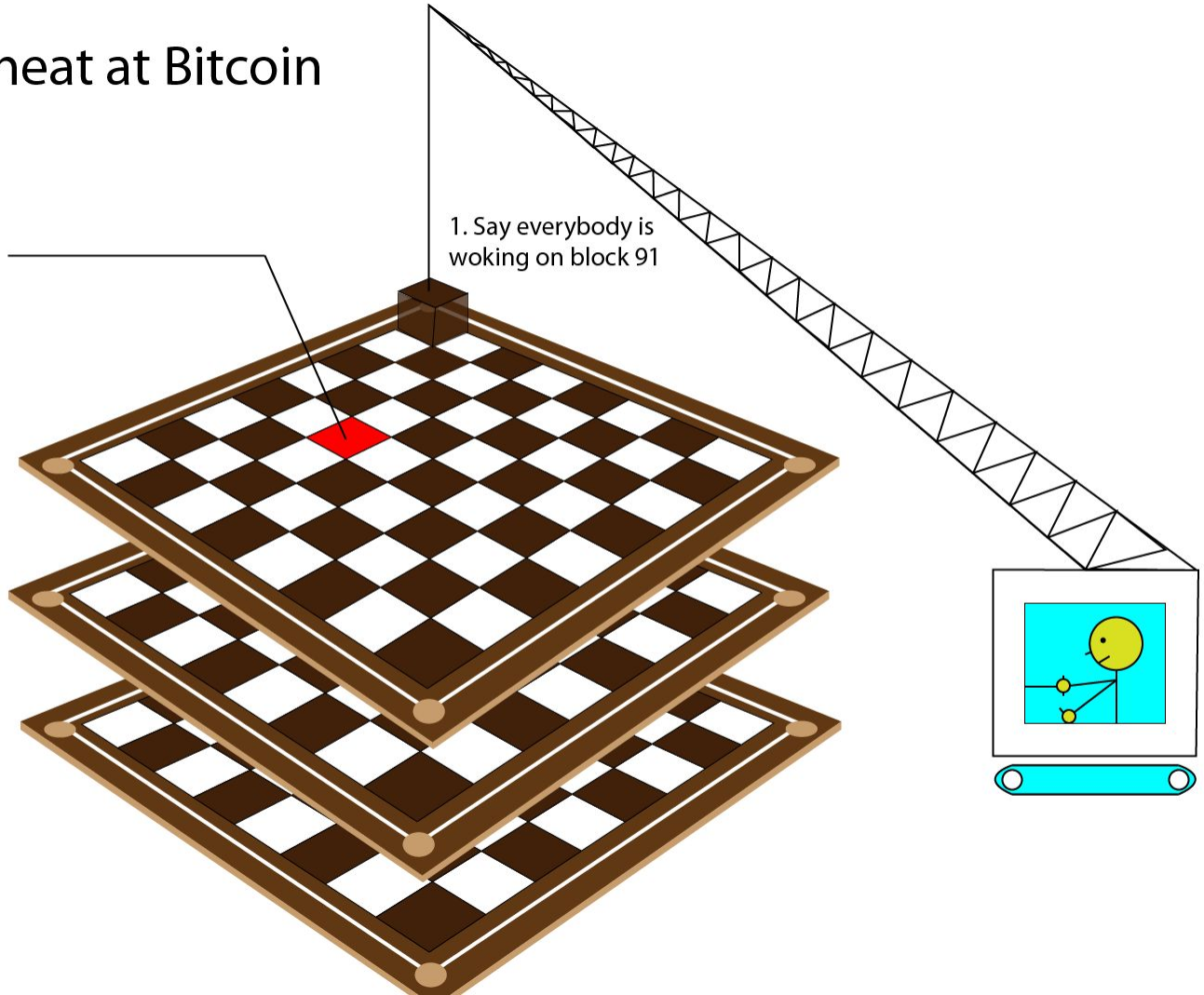
Why you can't cheat at Bitcoin

1. Say everybody is woking on block 91

2. But one miner wants to alter a transaction in block 74

3. He'd have to make his changes and redo all the computations for blocks 74-90 and do block 91. That's 18 blocks of expensive computing

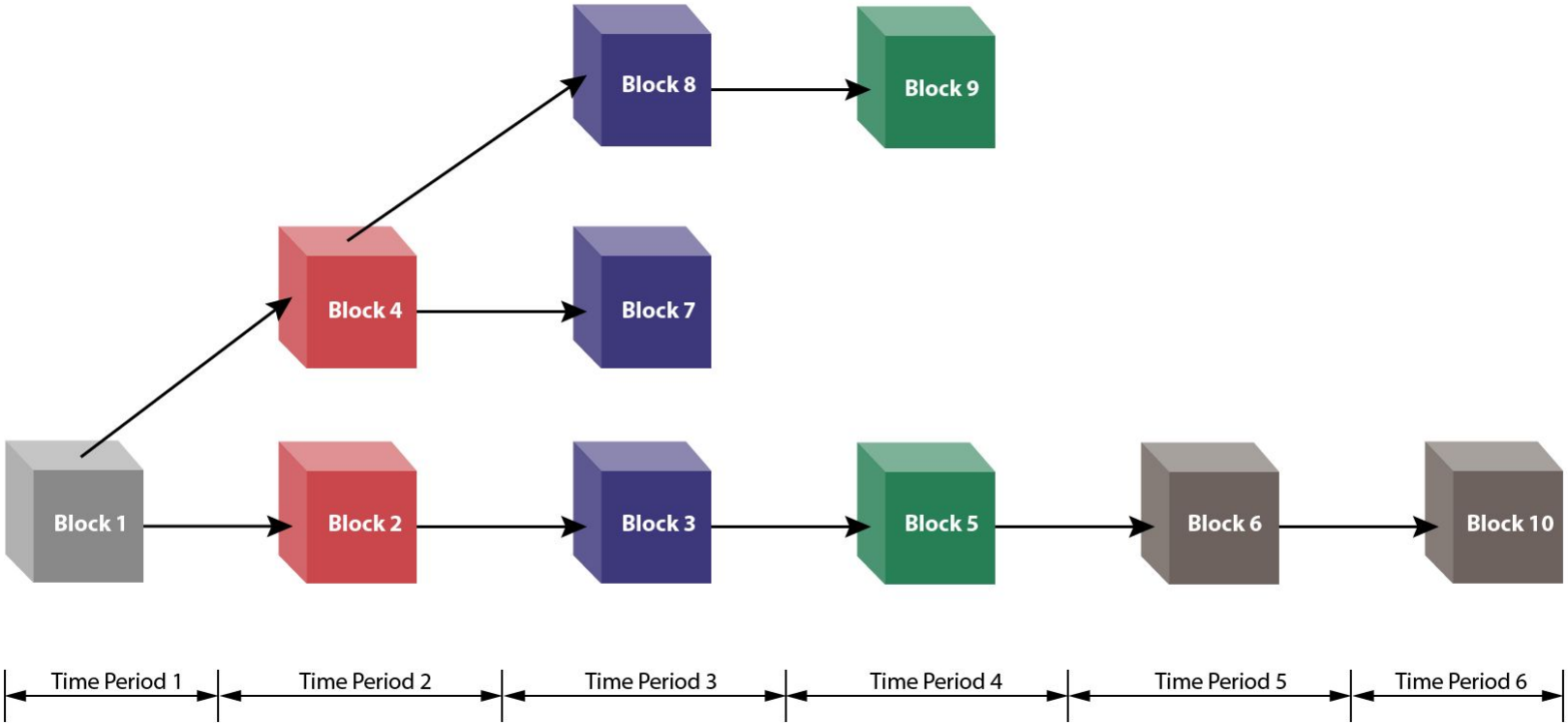
4. What's worse, he'd have to do it all before everybody else in the Bitcoin network finished just the one block (number 91) that they're working on



Conflict Example in Mining

- Multiple miners work on mining the Blocks.
- Suppose two miners can confirm a block within a fraction of seconds
- Other miners start working in for the next blocks.
- Bitcoin and Ethereum identify the longest chain based on total work is done/difficulty.
- Node prefers the first-seen valid chain with the most work measured in terms equivalent to the sum of the difficulty of all the blocks.

Conflict Example in Mining



Longest Chain Rule

- In Public Blockchains like Bitcoin, conflicts are being resolved by the longest chain rule.
- Let’s say a miner received the first Block 4 then he will start building the next Block on top of that Block 4.
- Now, in a few seconds that miners see another Block 2, so that miner will keep an eye on that new Block.
- If the next Block 3 is being detected from other nodes in Blockchain then that miner will disregard the 4 and will accept the new longest chain which is 1-> 3-> 5 and so on.
- Conventional wisdom states that it is therefore wise to wait for six blocks to confirm a transaction.

THANK YOU

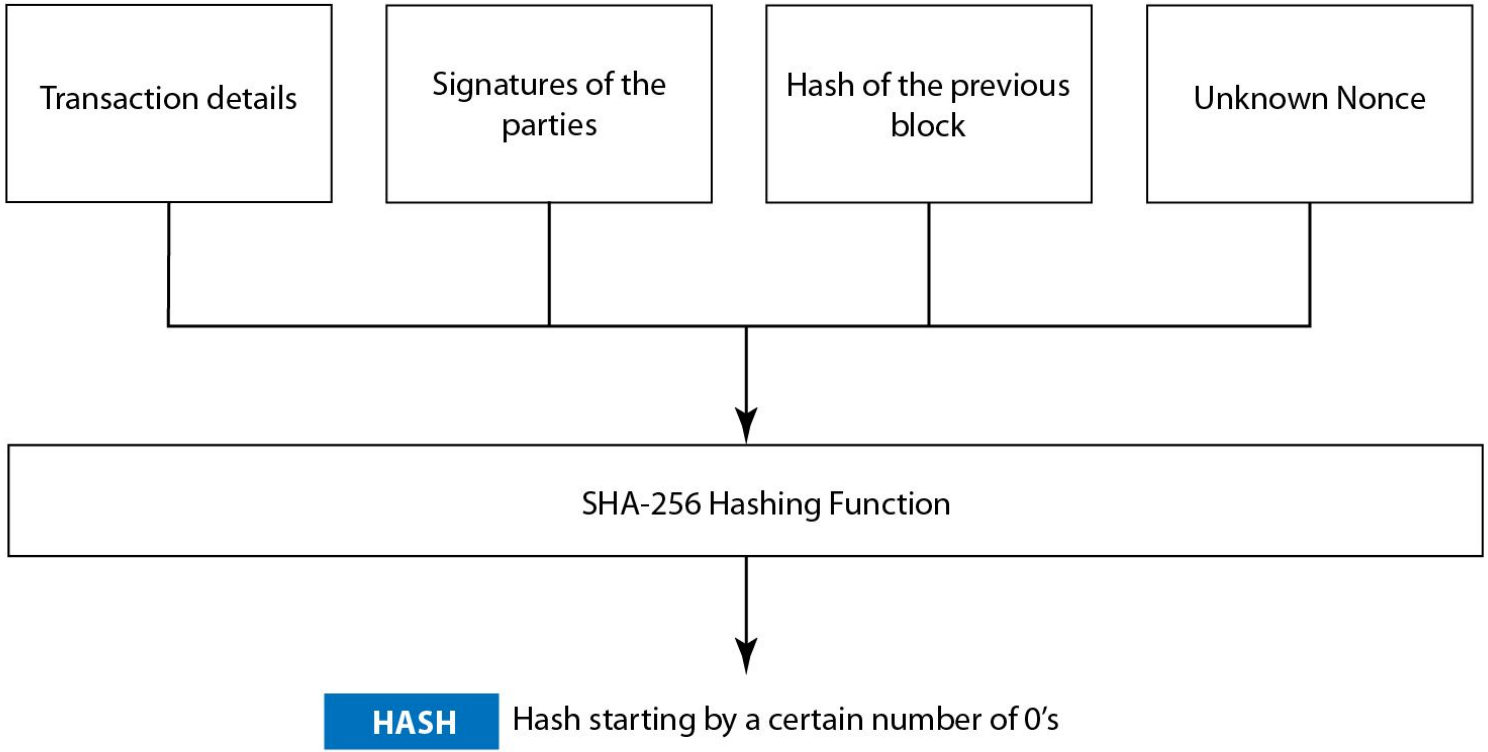
For more information contact
info@we2blocks.com

Professional Blockchain Course

Top 5 Consensus Mechanisms

Proof of Work

- Proof of Work is the consensus algorithm where miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm. This proof proves that a miner spends a lot of time and resources to solve the problem. When a block is 'solved,' the transactions contained are considered confirmed.
- By Mathematical problem we mean:
  - Hash function - how to find the input knowing the output.
  - Integer factorization - how to present a number as a multiplication of two other numbers.
  - Guided tour puzzle protocol - If the server suspects a DoS attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it’s a ‘how to find a chain of hash function values’ problem.
- Miners receive a reward when they solve the complex mathematical problem.
- For example in Bitcoin miners receive 12.5 bitcoins for solving the puzzle.
- Miners can also receive transaction fees in addition to rewards.


Transaction details
Signatures of the parties
Hash of the previous block
Unknown Nonce
SHA-256 Hashing Function
HASH
Hash starting by a certain number of 0's

Proof of Work Example

Example Bitcoin:

In Bitcoin, a block is being mined every 10 minutes. The difficulty is adjusted such that it never deviates much from this limit. If the difficulty stays the same, while the computer power increases gradually, it will take less and less time to mine a block.

To make sure this doesn't happen over blockchain, the Proof of Work target is a dynamic parameter. In the Bitcoin blockchain, the target gets adjusted every 2016 blocks. Computing the amount of time it took to mine 2016 blocks. It should take 20160 minutes (2016 * 10 minutes = 14 days). The difficulty is adjusted depending on the time it took to mine those blocks.

Proof of Stake

- Proof-of-Stake is a different algorithm to validate transactions and achieve the distributed consensus.
- Proof-of-Work algorithm rewards miners who solve complex mathematical problems with the end goal of validating transactions and creating new blocks. On the other hand, in the Proof-of-Stake algorithm, the creator of a new block is chosen in a deterministic way, depending on its wealth/stake in the blockchain.
- No block reward
- All the digital currencies are created at the start of the chain, and their number never changes. Miners only take the transaction fees. That is why in the PoS system miners are also called forgers.

1 Anyone who holds the native currency can become a validator.

2 The chance of mining and earning rewards are based on how much of the stake they have in the blockchain.

3 The chosen validator is rewarded by a part or the whole of the transaction fee.

Proof of Stake Example

Example Neo:

NEO is a smart contract development platform often referred to as “China’s Ethereum.” The network aims to be the center of a creative economy where digital assets can be securely traded with little overhead.

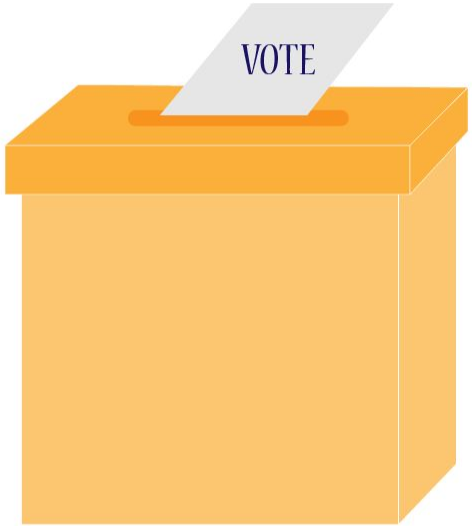
Staking NEO lets, you generate GAS, the platform’s internal currency. The more NEO you have staked, the more GAS you’ll earn with each payment. NEO rewards stakeholders with an annual return of 4-6%.

Delegated Proof of Stake

- People in a particular blockchain ecosystem vote for Witnesses to safeguard their computer network.
- Let's imagine a reward system where only the top 100 Witnesses are paid for their service, and only top 20 earn a regular salary. As it creates a healthy competition, many wants become a Witness thus providing hundreds of backup Witnesses.
- The vote strength of a person is determined by how many tokens they hold. People who have more tokens will influence the network more than people who have less tokens.
- If a Witness starts acting like a schmuck or stops doing a quality work in securing the network, people in the blockchain community can remove their votes, essentially firing the lousy actor. Voting is always ongoing.
- Delegates are elected as witnesses. A delegate becomes a co-signer on an individual account that has the privilege of proposing certain changes to the network parameters. This account is known as the Genesis account. These parameters include everything from transaction fees to block sizes, witness pay and block intervals.

1 Anyone who holds the blockchain base currency can vote for a validator.

2 The validator with the most votes gets to become a delegate, validating transactions and collecting the rewards for doing so



Delegated Proof of Stake Example

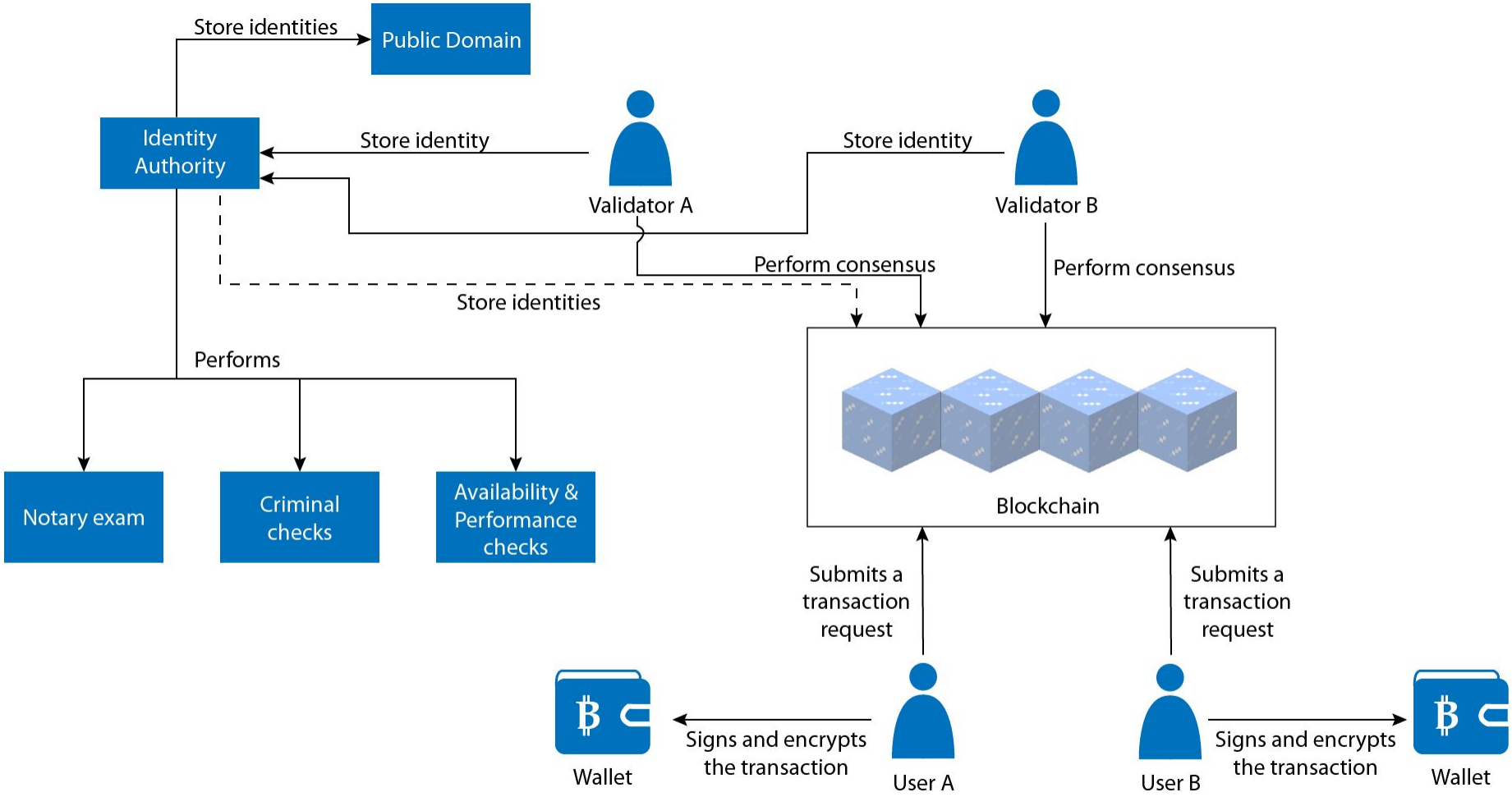
Example Lisk:

Lisk is a decentralized network similar to Bitcoin, Ethereum, or BitShares. Lisk uses a simplified implementation of the Delegated Proof of Stake consensus algorithm.

Lisk token holders can vote for mainchain delegates who secure the network. There is a maximum of 101 active mainchain delegates whosoever got the most votes on the whole network, and they can earn block generation rewards. Every other delegate is on standby waiting to be elected, or securing a Lisk sidechain.

Proof of Authority

- The proof-of-authority consensus is essentially an optimized Proof of Stake model that leverages identity as the form of stake rather than staking tokens.
- The group of validators is usually supposed to remain relatively small (~25 or less) to ensure efficiency and manageable security of the network.
- Individuals under PoA earns the right to become a validator, that's why there is no incentive to retain the position that they hold.
- Validators are required to formally verify identity either on the chain or some public domain.
- The eligibility to become a validator is difficult to obtain, and the individuals need to go through many steps to become a validator.


Store identities
Public Domain
Identity Authority
Store identity
Validator A
Store identity
Validator B
Perform consensus
Perform consensus
Store identities
Performs
Notary exam
Criminal checks
Availability & Performance checks
Blockchain
Submits a transaction request
Submits a transaction request
Wallet
Signs and encrypts the transaction
User A
User B
Signs and encrypts the transaction
Wallet

Proof of Authority Example

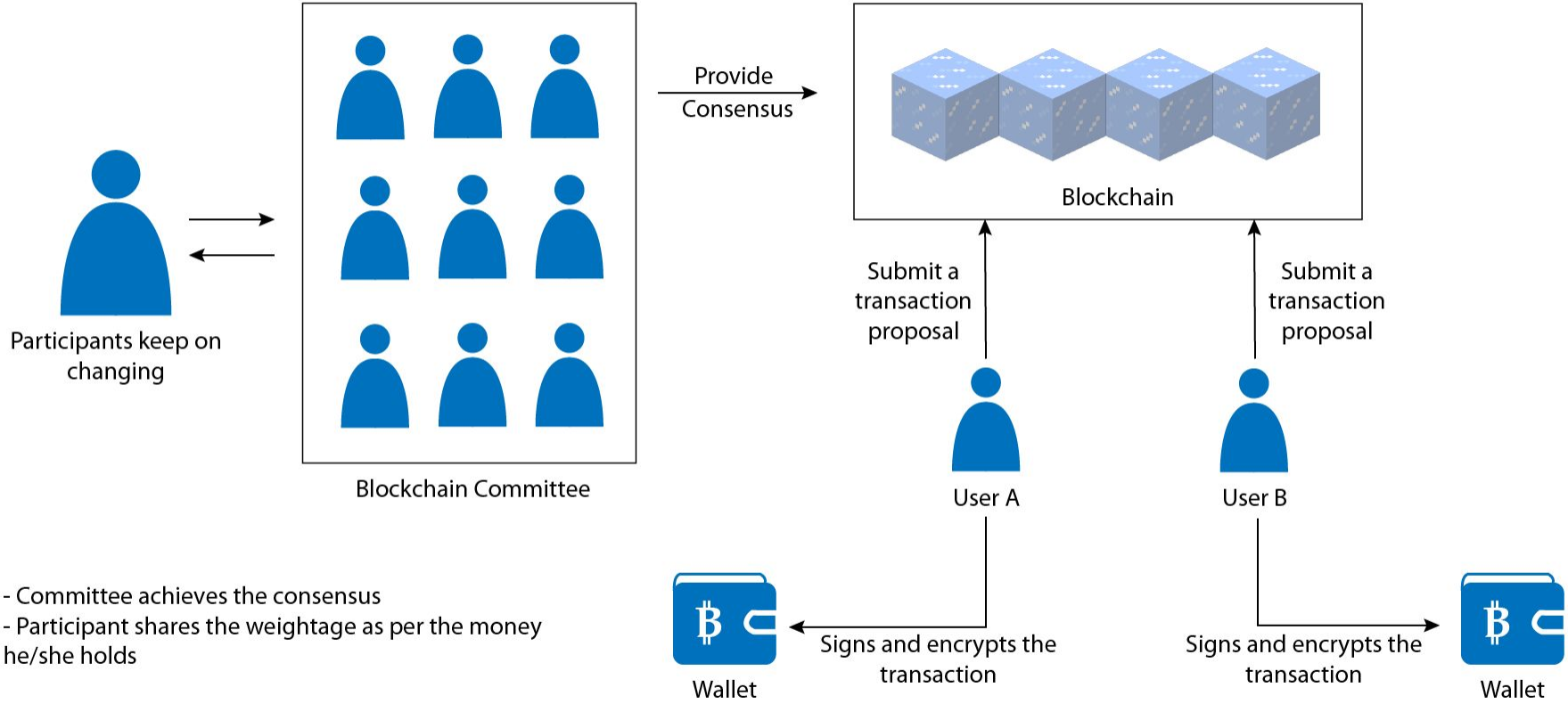
Example POA Network:

Proof of Authority Network (POA Network) is a blockchain platform founded on the core principle of implementing PoA consensus in their blockchain. POA Network is a public platform for smart contracts that exists as an Ethereum sidechain with their nodes consisting of independent validators.

To make eligibility for staking identity its very hard to obtain, candidates for validators have to overcome the hurdle of passing notary exams. Not only do the exams attest to no criminal records and good moral standing of a candidate, but they also filter out those who are not committed.

Proof of Weight

- Proof-of-Weight is a broad consensus classification based on the algorand algorithm which in turn specifies a new protocol known as Byzantine Agreement.
- BA* protocol is highly scalable and secure.
- PoW consensus model runs a committee where participants keep on changing, and the committee achieves the consensus for the network.
- Every user over the network has a weight attached to them which is determined by the money they hold in their account.



- Committee achieves the consensus
- Participant shares the weightage as per the money he/she holds

Proof of Weight Example

Example Filecoin:

Filecoin is using Proof-of-Spacetime as a weighted consensus on how much IPFS data you're storing. The weight is based on different parameters. If the overall weight fraction of honest users is higher than two-thirds of the total weight than the network will remain secure. This method also helps in protecting the network from double-spend attacks.

It is based on Algorand. While some may see similarities between Algorand and Proof-of-stake, they are not the same. In a PoS environment, the number of tokens held at any given time determines the amount of additional rewards users earn. Proof-of-weight uses an entirely different weighted value.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Types of Blockchain

Public Blockchain

- A public blockchain as its name suggests is the blockchain which is available to all, in other words it is a kind of blockchain which is-‘ for the people, by the people, and of the people.’
- No one is in charge of the network, and anyone can participate in reading/writing/auditing the blockchain.
- More complex rules are present for safeguarding it from malicious actors.
- All the decisions are made using the complex consensus algorithm
- Computationally these blockchains expensive to mine & commit a Block over the network.
- Example: Bitcoin Blockchain, Ethereum Blockchain, etc

Private Blockchain

- An individual or an organization privately operate private blockchain as its name suggests.
- Unlike public blockchain in private blockchains, there is an administrator/anchor who looks after essential things such as permissions and identities.
- The consensus is achieved on the whims of the central in-charge who can provide mining rights to anyone or not give at all.
- Compared to public blockchain it is much faster and cheaper because one doesn't have to spend an enormous amount of energy, time and money to reach a consensus.
- It is less secure compared to the Public Blockchain.
- Examples: Bankchain, Medichain, etc.

Consortium Blockchain

- This type of blockchain removes the individual autonomy which gets vested in just one entity by using private blockchains.
- Here instead of one in charge, we have more than one in charge. A group of companies or representatives coming together can make decisions for the benefit of the whole network.
- As a way of achieving things much faster and also have more than one single point of failures which protects the whole ecosystem.
- In simple words, it’s the best of both Private and Public Blockchains.
- Gives options for rights and access management while leveraging the same blockchain technology and reaping its benefits.
- Examples: R3, EWF, etc.

Difference

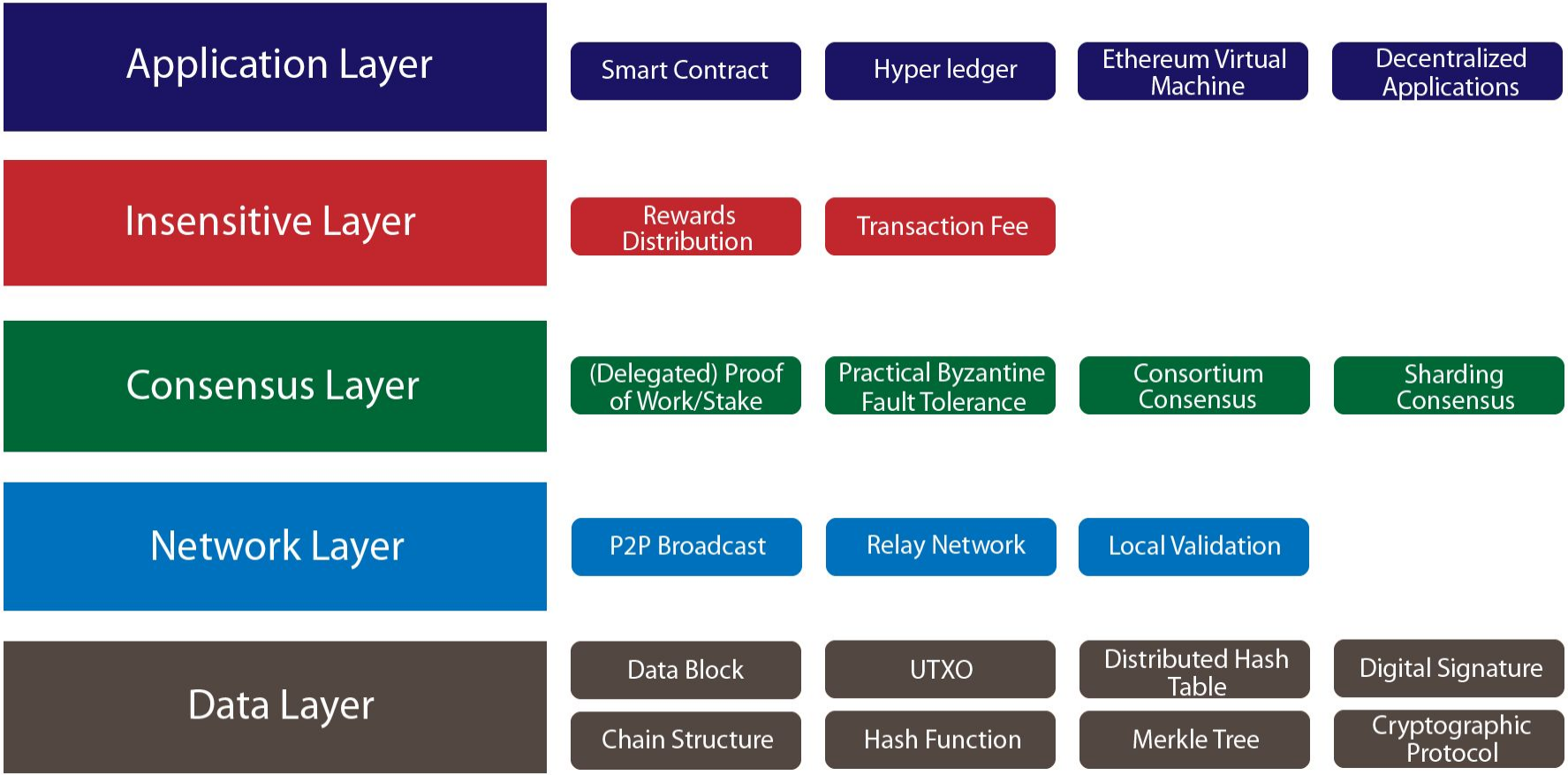
Property	Public	Consortium	Private
Consensus Determination	All miners	Selected few miners	Organisations participating.
Permissions	Read permissions to all	Could be restricted	Could be restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Centralised	No	Partial	Yes
Efficiency	Low	High	High
Consensus providers	Permissionless	Permissioned	Permissioned

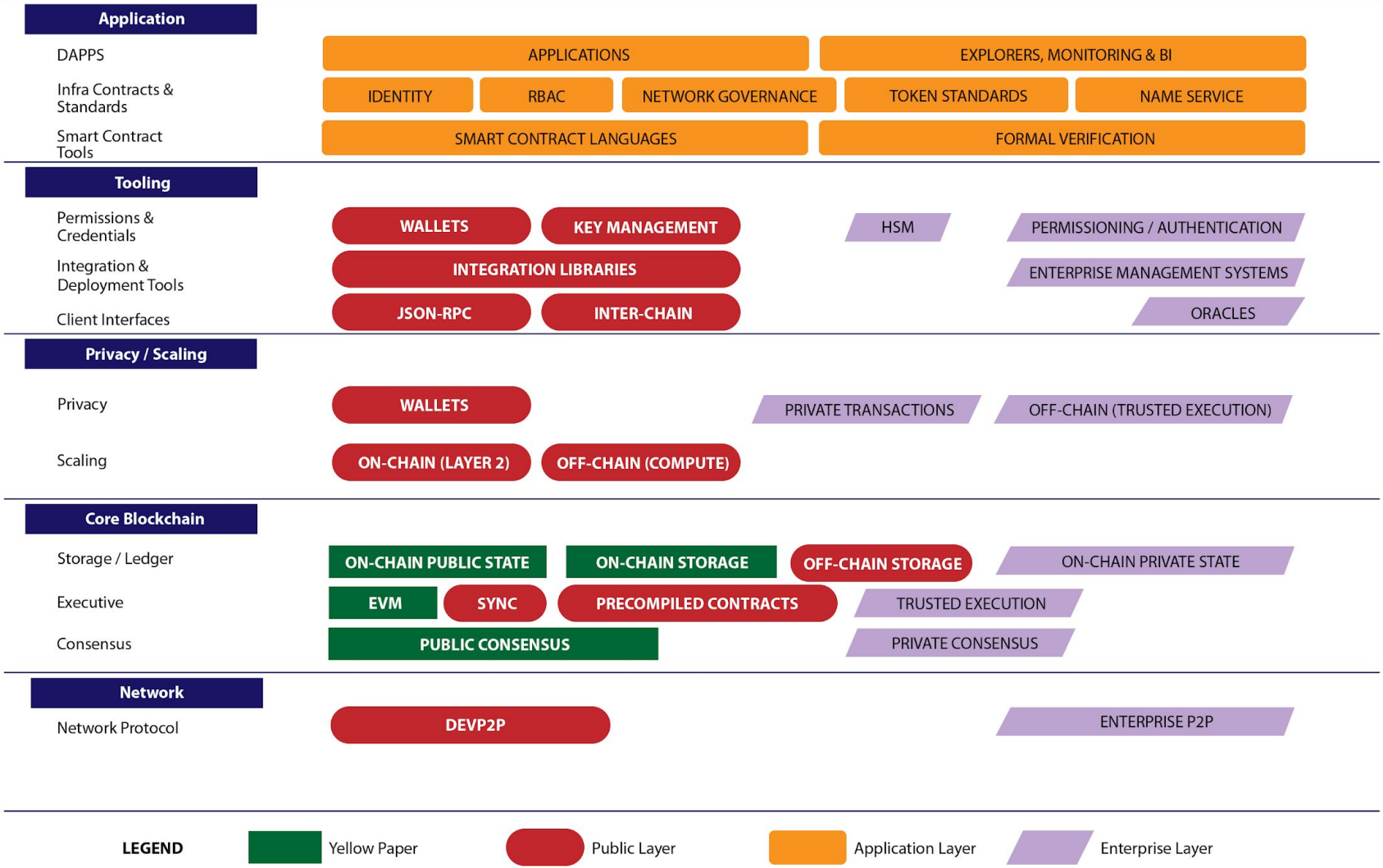
THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Blockchain Architecture


Application Layer
Smart Contract
Hyper ledger
Ethereum Virtual Machine
Decentralized Applications
Insensitive Layer
Rewards Distribution
Transaction Fee
Consensus Layer
(Delegated) Proof of Work/Stake
Practical Byzantine Fault Tolerance
Consortium Consensus
Sharding Consensus
Network Layer
P2P Broadcast
Relay Network
Local Validation
Data Layer
Data Block
UTXO
Distributed Hash Table
Digital Signature
Chain Structure
Hash Function
Merkle Tree
Cryptographic Protocol


Application
DAPPS
APPLICATIONS
EXPLORERS, MONITORING & BI
Infra Contracts & Standards
IDENTITY
RBAC
NETWORK GOVERNANCE
TOKEN STANDARDS
NAME SERVICE
Smart Contract Tools
SMART CONTRACT LANGUAGES
FORMAL VERIFICATION
Tooling
Permissions & Credentials
WALLETS
KEY MANAGEMENT
HSM
PERMISSIONING / AUTHENTICATION
Integration & Deployment Tools
INTEGRATION LIBRARIES
ENTERPRISE MANAGEMENT SYSTEMS
Client Interfaces
JSON-RPC
INTER-CHAIN
ORACLES
Privacy / Scaling
Privacy
WALLETS
PRIVATE TRANSACTIONS
OFF-CHAIN (TRUSTED EXECUTION)
Scaling
ON-CHAIN (LAYER 2)
OFF-CHAIN (COMPUTE)
Core Blockchain
Storage / Ledger
ON-CHAIN PUBLIC STATE
ON-CHAIN STORAGE
OFF-CHAIN STORAGE
ON-CHAIN PRIVATE STATE
Executive
EVM
SYNC
PRECOMPILED CONTRACTS
TRUSTED EXECUTION
Consensus
PUBLIC CONSENSUS
PRIVATE CONSENSUS
Network
Network Protocol
DEVP2P
ENTERPRISE P2P
LEGEND
Yellow Paper
Public Layer
Application Layer
Enterprise Layer

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Forming your own Blockchain Solutions

Identify the Use Case

- The blockchain is not a solution for all the problems.
- There is a lot of hype, but you need to map the hype with the use.
- Having a concrete use case is essential to weave the solution around.
- Some of the widespread use cases are:
  - Payments
  - KYC
  - Smart asset
  - Land Records

Design a Workflow for Blockchain Integration

- Analyze whether you need a blockchain as a solution or there are other ways to solve the existing problem.
- Don’t start churning up detailed technical specification without any validation.
- Blockchain should solve a problem for existing centralized systems, e.g., expensiveness, transparency, and reliability.
- Have a feasible layout on integrating the technology into your development strategy.

Identify the Consensus Mechanism

- Depending on your use case choose the Consensus Mechanism.
- Choose the mechanism which is apt for the Use Case.
- For example, A private Blockchain solution may not require expensive POW consensus.
- Some of the popular Consensus Mechanisms are:
  - Proof-of-Work
  - Proof-of-Stake
  - Delegated-Proof-of-Stake
  - Proof-of-Authority
  - Proof-of-Weight

Identify the Platform

- Depending on the consensus mechanism of your choice, choose the platform which fits your needs and plans.
- Blockchain started as open source, and there are many platforms available free to use.
- Some of the major platforms are:
  - Bitcoin
  - Ethereum
  - Multichain
  - Hyperledger
  - Corda
  - Quorum
  - BigChainDB
  - Stellar

Design the Architecture

- The architecture includes elements such as the infrastructure, software, and hardware configuration.
- The solution may be architectured on the cloud, on-premises, or a hybrid model depending on the organization’s need.
- Further architecture can be design according to permission-less, permissioned, public, private, or hybrid.

Design the Blockchain Instance

- You need to plan your instance carefully.
- In specific platforms, it's difficult to configure some parameters once set.
- Things needed under configuration can be as following:
  - Permissions
  - Asset Issuance/ Reissuance
  - Atomic Exchanges
  - Key Management
  - Multi-Signature
  - Block Parameters
  - Limits
  - Network Protocols/ Handshaking
  - Key and Address Formats
  - Native Assets

Build the APIs for your Blockchain

- APIs are required by the developers and applications to interact with your Blockchain.
- Usually, platforms come with APIs, and if you are building from scratch, you need to look into design and schemas for your APIs carefully.
- As per your requirements you need to see which APIs to expose for your Blockchain.
- Some of the APIs that you might need:
  - Generating Key Pairs
  - Asset Issuance
  - Data Authentication
  - Checking Blockchain Parameters
  - Create and Read operations
  - Smart Contracts
  - Address Specifications

Designing the Front End

- You require a Front End for your users and administrators.
- Most platforms work on JSON format which can be collaborated with major programming languages.
- Some of the platforms offer SDKs to integrate existing front-end applications with Blockchain.
- You can use languages like HTML5, CSS, PHP, C#, Java, Javascript, Python, Ruby, Golang, Solidity, AngularJS Nodejs.
- Moreover, you can also use external storages like Cloud Storage, NoSQL, RDBMS, etc.

Future Prospects

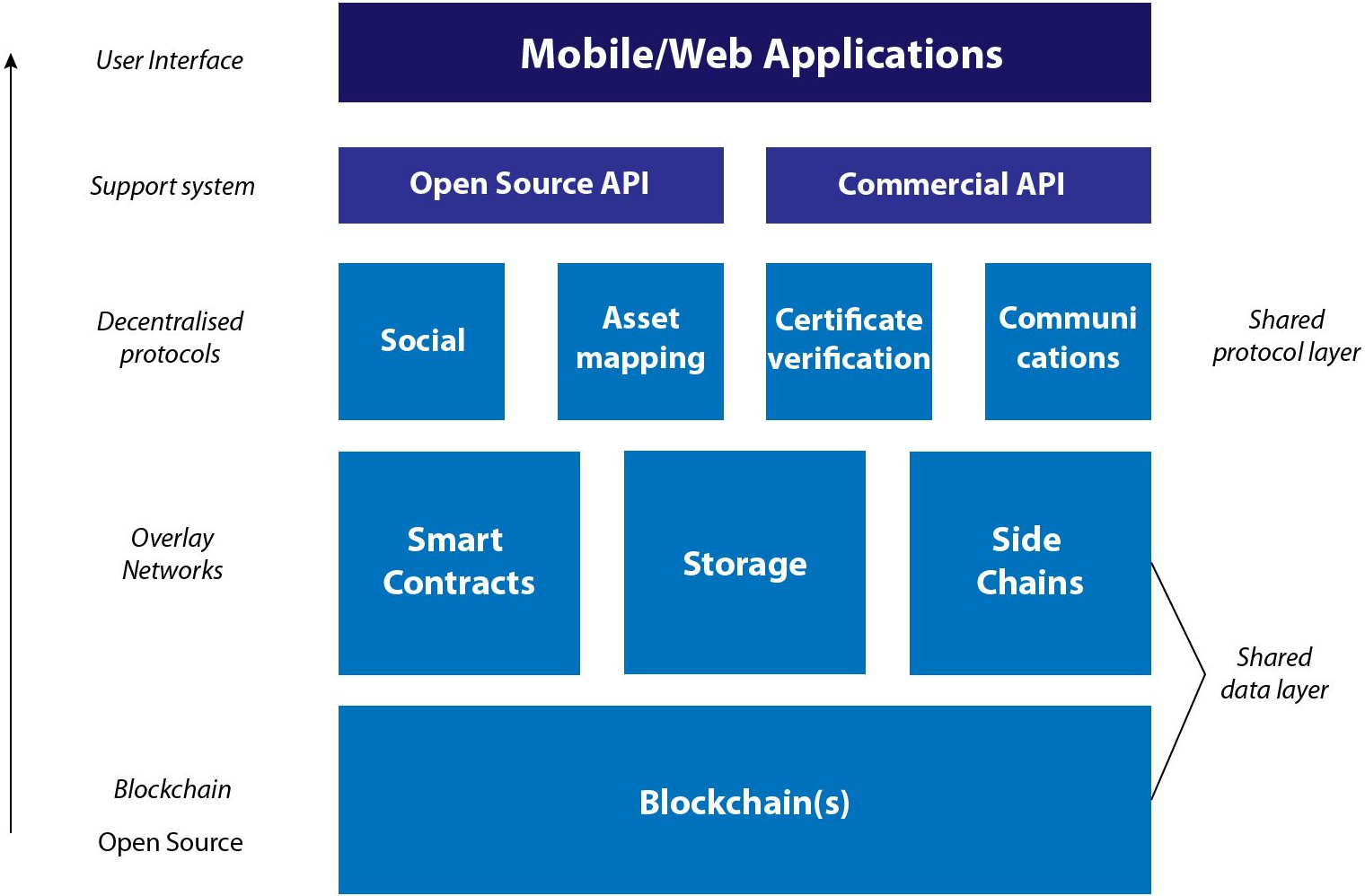
- Once you have the stable application up and running, you can look into future integrations with other technologies.
- You can enhance the power of your Blockchain solution by integrating Artificial Intelligence, Biometrics, Internet of Things, Bots, Cloud, Cognitive services, Containers, Data Analytics, and Machine Learning.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Blockchain Technology Stack


User Interface
Mobile/Web Applications
Support system
Open Source API
Commercial API
Decentralised protocols
Social
Asset mapping
Certificate verification
Communi cations
Shared protocol layer
Overlay Networks
Smart Contracts
Storage
Side Chains
Shared data layer
Blockchain
Blockchain(s)
Open Source

Blockchain

- This is the base of all Blockchain based applications.
- It is a network of nodes spread across the world which run algorithms to verify and commit transaction over the Blockchain.
- This is a decentralized network and mostly based open source cryptography algorithms.
- This can be created as public, private or consortium.
- This can also include Certificate Authorities and Membership services for government and enterprises.

Overlay Networks

- This is a network that achieves additional functionality without bootstrapping the original protocols.
- They benefit from the network effects and build on top of that.
- Some of the additional functionalities you achieve are:
  - Smart Contracts - crypto agreements between two parties
  - Storage - renting network
  - Sidechains - transfer tokens from one Blockchain to a different Blockchain.

Decentralised Protocols

- This is the essential part of the Blockchain Technology stack as it makes sure the Blockchain layer and overlay networks do not depend on a single entity for validation and transactions.
- It helps to create decentralized peer-to-peer datasets.
- Decentralized Protocols can be based on asset mapping, social identities, verification algorithms or communication channels.

Support System

- For building Blockchain applications, you require APIs to interact with the underneath technology.
- You can directly build a solution using the existing APIs, without depending and working on your ledger.
- Most APIs respond to JSON format, thus can be easily integrated with existing Front End Technologies.
- You can use the open source APIs like Bitcoin and Ethereum, or you can choose from commercial APIs like block.io or blockcypher for more boxed up functionalities.

User Interface

- Finally, a user interface is required for your users to connect to your Blockchain.
- User Interface can be built with existing frontend mechanisms and can easily employ the power of Blockchain by using APIs.
- Some platforms like Hyperledger also provide generators to produce a box user interface for the applications built open them.
- Most Blockchain platforms also provide with connecting services to link Applications to Blockchain.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Blockchain Ecosystem

Blockchain Projects

The Blockchain ecosystem is currently running with some major projects and more are under pipeline. Some of the major projects on Blockchain are:

- **Bitcoin** - This project introduced the world to Blockchain.
- **Ethereum** - This project came with concept of Smart Contracts where two parties adhere to certain rules and create a trust. This opens the world for more decentralized applications.
- **Neo** - This project positioned itself as the “Chinese Ethereum” but it bought the Python as the main language for the creation of Applications.
- **Stellar** - This project is trying to make cross border transactions simpler. Stellar comes with extensive APIs which helps the developers build applications fast, thus reducing the time to market for the applications.

Blockchain Users

- Blockchain users are normal people like you and me, who make use of the blockchain or cryptocurrency to achieve some results. They can also be investors who buy cryptocurrencies to sell at a later date.
- For creating a Blockchain user base the technology or cryptocurrency should have some utility related to the problem being tackled.

For Example:

- Bitcoin serves the major utility of payment for goods and services. Currently there are over 50,000 merchants registered with Bitcoin including - Microsoft, PayPal and Subway.
- Bitcoin was the first mover in Blockchain and it's high utility as payment system made sure that a large part of its ecosystem is based upon users.

Blockchain Exchanges

- Every Blockchain project has a robust ecosystem working under it, and it always include a decentralized exchange. These are developed by the Blockchain team or the community of other developers.
- A typical exchange is designed to find the cheapest rates of exchange between any two cryptocurrencies, making it more affordable to trade tokens/cryptocurrencies.
- Exchanges used for trading also might integrate with hardware wallets, or users can create their own wallet on the exchange website.

Blockchain Miners

- To function a blockchain and maintain its integrity, it needs a large network of independent nodes around the world to maintain it continuously. In private blockchains, a central organisation has the authority over every node on the network. In the case of public blockchains, on the other hand, anyone can set up their computer to act as a node. The owners of these computers are called miners.
- Since the integrity of the blockchain is directly related to the number of independent nodes on the network, there also needs to be some incentive to mining. Different blockchains utilize different mining systems however most of them contain some form of:
  - An incentive system
  - A consensus algorithm

Blockchain Developers

- Blockchain technology is built by the potential of developers working behind it. A strong team of developers can lead to a successful Blockchain project. Currently there are two types of developers in the blockchain ecosystem:
  a. Blockchain developers
  b. dApp developers

- Blockchain developers build new blockchains with different levels of functionalities and Consensus Algorithms.
- dApp developers work with decentralized applications that can run on blockchains thus providing a similar functionality like Google Play Store over the Blockchain Technology.
- The development of Smart Contracts over the Blockchain has open possibility for the developers to create extensive applications and use cases for the industries.

Blockchain Applications

Apart from exchanges, platforms and users, another important aspect of the Blockchain ecosystem is the applications that industries, developers and communities build to serve a specific purpose.

There are various examples of Applications being build upon Blockchain, some of the major working applications are:

- **CryptPad** - A decentralized document creation application.
- **Humaniq** - A fintech startup which connects unbanked people with global economy.
- **Augur** - A peer to peer oracle and prediction market place.
- **Filament** - Building the IoT applications over the Blockchain.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Comparison of top Blockchain Solutions

Bitcoin

- It is a globally known cryptocurrency and digital payment system.
- First Decentralized Digital Currency whose ledger is maintained by Blockchain openly and gave us the taste of the blockchain.
- It was founded by an unknown person or group of people and released as open-source software in 2009.
- Peer-to-peer.
- Transactions take place between users directly, without an intermediary.
- Network nodes verify these transactions and record them in a public distributed ledger called Blockchain.

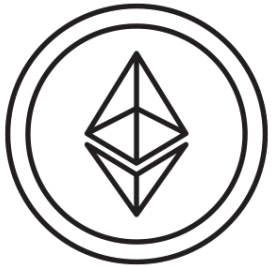
Bitcoin

Features that differentiate Bitcoin from fiat currencies:

- Decentralized System: The control of Bitcoin is not centralized. The nodes/computers work together to mine the currency and process transactions which form the network, without any need of a central authority.
- Simple Setup Process: Regular banks make you go through a lot of processes to open an account. However, the configuration process of Cryptocurrency is straightforward and free.
- Anonymous and Transparent Usage: Users can have many Bitcoin addresses without a link to any personal identifying information. However, it records every transaction in a giant ledger called Blockchain.
- Meager Transaction Fee: Bitcoin charges a minimal fee for international transfers.
- Fast Network Process: The payment process is quick on the Bitcoin network.
- Non-Refundable: Once sent, Bitcoins cannot be refunded.

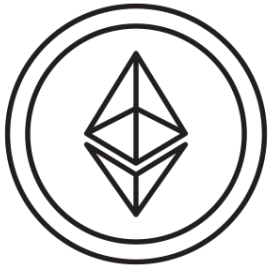
Ethereum

- Ethereum is an open source software platform which is based on Blockchain technology that enables developers to build and deploy decentralized applications like smart contracts.
- It offers a Decentralized Virtual Machine aka Ethereum Virtual Machine which can execute scripts using a globally distributed network of public nodes.
- Launched by Vitalik Buterin in late 2013.
- The development for ethereum was funded by an online public crowdsale during July–August 2014, by buying the Ethereum token (Ether).



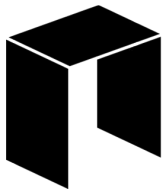
Ethereum

- The first public beta pre-releases network known as "Olympic.” The Olympic network provides users with a bug bounty of 25,000 Ethers for stress testing the limits of the Ethereum Blockchain.
- Ethereum's live Blockchain named “Frontier” was launched on 30 July 2015.
- The current milestone is named "Homestead" and is considered stable. As it has led to various improvements such as transaction processing, gas pricing, and security.
- There are at least two other protocol upgrades planned for the future, i.e., Metropolis and Serenity (Proof-of-stake).



NEO

- NEO is a smart economy for the distributed network.
- NEO was chosen as the name because “NEO” in Greek means, “newness, novelty, and youth.”
- NEO was initially called AntShares (ANS) which was launched in 2014, founded by Da Hongfei and Erik Zhang.
- Antshares announced on June 22, 2017, that it planned to rebrand itself as NEO.
- The first ICO on the NEO blockchain, Red Pulse Token (RPX) was announced soon after the rebranding finished.
- Apart from the NEO cryptocurrency itself, the NEO platform has another crypto-token called “GAS” which was formerly called as “ANC-Antcoins.”



Hyperledger

- Hyperledger is an open source created to advance cross-industry blockchain technologies.
- It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing, and technology.
- Hyperledger acts as an operating system for marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities. It has the potential to vastly lessen the expense and complications in getting things done in the real world.

HYPERLEDGER

EOS

- EOS is an operating system for marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities. It has the potential to vastly lessen the expense and complications in getting things done in the real world.
- EOS Blockchain aims to become a decentralized operating system which can support industrial-scale decentralized applications.
- EOS is planning to delete transaction fees. EOS claims to have the ability to conduct millions of transactions per second.
- EOS runs on DPOS consensus algorithm.

Corda

- Corda is an open source blockchain aiming to meet requirements for use of blockchain in businesses.
- Corda offers a solution where a shared ledger can be intiated between parties under the contract.
- Corda’s communications are point-to-point, meaning only participants of a transaction can see it.
- With Corda's point-to-point architecture participants only have copies of the transactions they are participants to or observers of. This means that every node in a Corda network is likely to have a unique ledger. This is called as multilateral ledger.

Quorum

- Quorum is the brainchild of J.P. Morgan bringing in enterprise focused version of Ethereum.
- Quorum provides private smart contract execution and enterprise grade performance.
- Quorum uses zk-Snarks cryptography which allows verification of the computation correctness without even learning what was executed.
- Quorum uses a hybrid privacy design.

Multichain

- Multichain was created by Gideon to make available a blockchain solution for organizations to build and develop fast.
- Multichain is built upon Bitcoin Blockchain but offers the functionality of Permissions, Streams, and Assets
- Multichain also provides other tools like explorers to interact with underline Blockchain seamlessly.
- Bankchain is using Multichain as it’s base.

THANK YOU

For more information contact
info@we2blocks.com

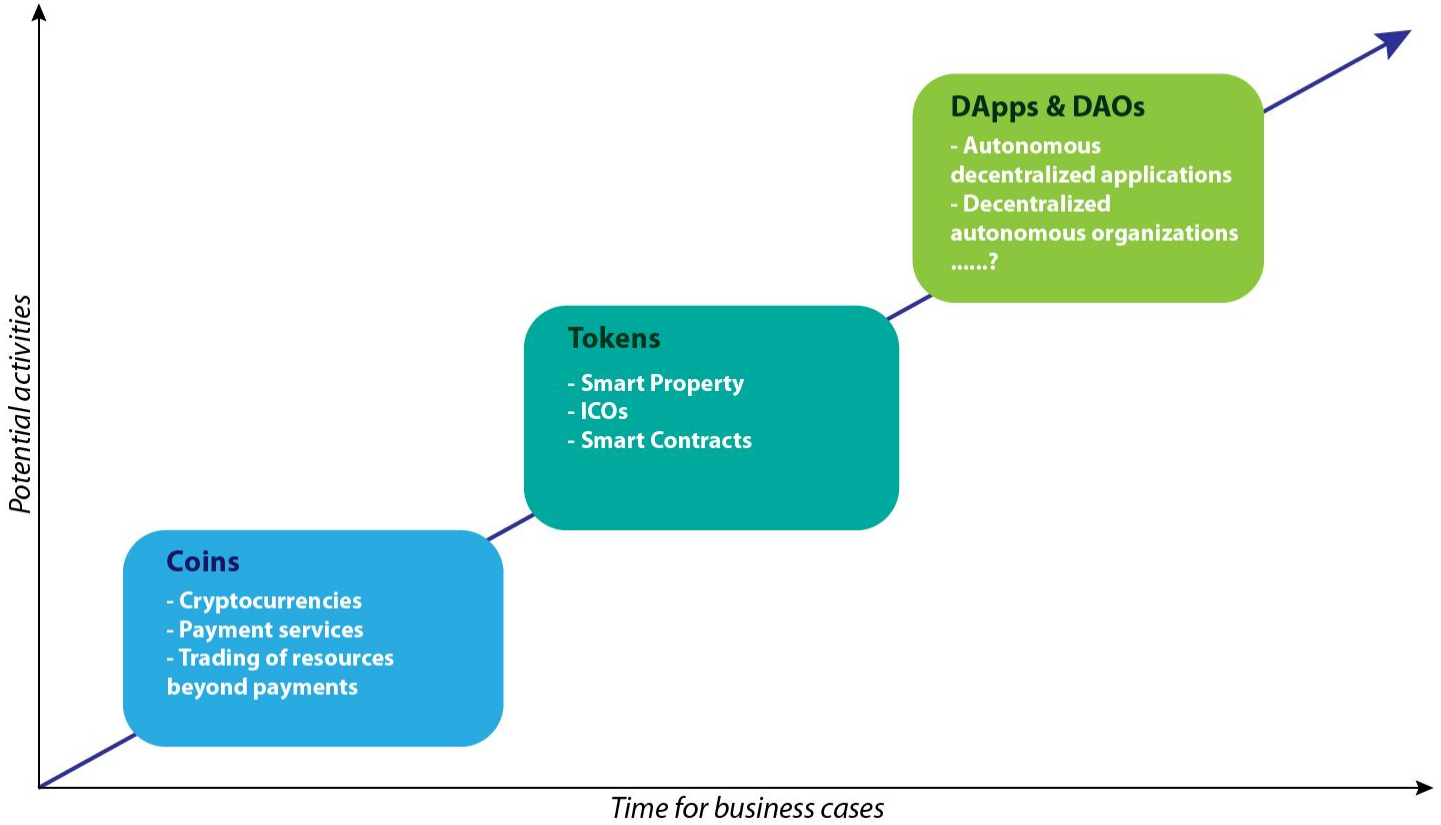
Professional Blockchain Course

Why do industries need to adopt Blockchain?

Current Industries using Blockchain

- **Pharmaceuticals** - DHL worked with Accenture to establish a blockchain-based track-and-trace system in six areas worldwide. Currently, the system has 7 billion unique pharmaceutical serial numbers and handling more than 1,500 transactions per second.
- **Fashion** - CGS has developed a system for tracking garments and compliances on raw materials for many apparels and fashion clients.
- **Cross-Border Payments** - IBM has developed a new blockchain banking solution that allows financial institutions to move quickly and cost-effectively process payments globally.
- **Food Safety** - IBM has partnered up with Dole, Nestlé, and Walmart to set up a blockchain for better regulation of food.
- **United Nations** - United Nations is currently using Blockchain for 16 agencies including Human Trafficking and World Food Program.
- **Jewelry** - Brilliant Earth has partnered up with Everledger to use blockchain in tracking and tracing the provenance of diamonds and other gemstones. This will also ensure that they are conflict-free.

Blockchain Revolution



Exciting Disruptions Coming Soon

- **Entertainment Industry** - Movie Braid was the first movie to be produced by doing an ICO.
- **Property Rental** - Rentberry aims to address the common pitfalls and headaches of the traditional rental model.
- **Politics** - Sierra Leone carried out their elections on Blockchain.
- **Education** - Socrates Coin is making big moves to change the traditional approach to a “3DInternet”.
- **Digital Advertising** - Basic Attention Token is taking a crack to solve the problems with Digital Advertisements.
- **Internet of Things** - Waltonchain, an award-winning Chinese project that seeks to integrate IoT and blockchain technology on an unprecedented scale.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Industry Challenges with Blockchain

Energy Consumption

- Some major public Blockchains use Proof-of-Work algorithms.
- PoW involves the use of the computational power of a machine to solve a complex mathematical puzzle to verify a transaction and add it to a block.
- Current Bitcoin energy consumption is almost equal to the consumption by Ireland.
- By 2020 it’s estimated that Bitcoin will utilize more energy consumption than the entire world currently uses.
- A probable solution for this has emerged in the form of different consensus mechanisms like Proof-of-Stake, Delegated-Proof-of-Stake, etc.

Scalability

- Scalability has appeared as a significant issue for the Blockchain networks like Bitcoin and Ethereum.
- Blockchains are having trouble effectively supporting a large number of users on the network.
- Moreover, the size of public blockchains keeps on increasing. Currently, Bitcoin ledger size is above 100 GB.
- One possible solution which has emerged is storing a hash of data over the network.

Public Perception

- Presently, blockchain technology is almost synonymous with Bitcoin.
- The majority of the public is still oblivious to the existence and potential uses of Blockchain technology.
- As Bitcoin is anonymous and is used for shadowy dealings of money laundering, black market trade, and other illegal activities. The blockchain is also getting a bad reputation due to the same.
- Mainstream adoption is needed to remove the sometimes-negative undertones of Bitcoin.

Blockchain Standards and Regulations

- Blockchains are continuously evolving, but still, countries are skeptic about it as there is no proper definition for standards and regulations.
- Enterprises and Governments require regulations to protect their customers.
- To tackle this problem, certain countries are trying to launch their regulations over the technology.
- Mass adoption might also standardize the Blockchain.

THANK YOU

For more information contact
info@we2blocks.com

Blockchain Professional Course

Attacks over Blockchain

51% Attack

- It states that group of miners controlling more than 50% of the network's mining hashrate, or computing power can take over the network.
- It is a speculative attack described over Bitcoin blockchain.
- Bitcoin Gold, at the time one of the top 30 cryptocurrencies, suffered a 51% attack and lost $18 million.
- Potential damage could be
    - The attackers would be able to prevent new transactions gaining confirmations, allowing them to halt payments between users.
    - Attackers would also be able to reverse the transactions that were confirmed while they were in control of the blockchain network, meaning they could double-spend coins.
- The mining pool ghash.io was briefly exceeding 50% of the bitcoin network computing power in July 2014, leading the pool to commit to reducing its share of the network voluntarily.

Eclipse Attack

- This attack is based on Distributed application architecture that partitions tasks or workloads among peers without the need for a central coordinating server or stable hosts.
- Cripple a node in such a way that it can not talk to other nodes in the network.
- This attack is possible due to design strategy flaws in the Blockchain such Peer's identity and Peer Selection Strategy.
- Currently, Bitcoin has eight outgoing connections, and Ethereum has 13 which implies one node in Bitcoin only has a view for eight nodes connected to it.
- So one node in Bitcoin has to depend on the other 8 for the complete view of the network which can be taken advantage by the hacker.
- Potential damage could be:
  - Double spending;
  - Attacks against second layer protocols, e.g., an attacker can obtain the products/services without paying by tricking his victims into thinking that the payment channel is still open while the non-eclipsed part of the network sees that payment channel is closed.
  - Smart contracts also may be attackable if users see inconsistent views of the blockchain.

Sybil Attack

- In a Sybil attack, the attacker attempts to fill the network with clients nodes that they control, if this happens then you would be most likely to connect with attacker nodes.
- Bitcoin never keeps a count of nodes for anything, If the attacker completely isolates a node from the honest network than it can help the attacker in the execution of other attacks.
- Potential damage could be:
  - Attacker refuse the relay blocks
  - Attacker only relay blocks which he creates.

Timejacking Attack

- Timejacking attack is an extension of the Sybil attack.
- Each node internally maintains a network time counter.
- The counter is based on the median time of a node's peers which is sent in the version message when peers connect.
- The network time counter reverts to the system time if the median time differs by more than 70 minutes from the system time.
- Potential Damage could be:
    - An attacker could potentially slow down or speed up a node's network time counter by connecting multiple peers and reporting inaccurate timestamps.
    - Since the time value can be distorted by at most 70 minutes, the difference between the nodes would be 140 minutes.

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

How Blockchain is taking over the world?

World Domination

- The blockchain is already deployed in wild and continuously growing.
- The ‘World Economic Forum’ anticipates that 10% of global GDP will be stored on the blockchain by 2025.
- The real power of Blockchain is yet to be unleashed.


Real World Examples
Railways
Russian rail operator Novotrans is storing inventory data on a blockchain pertaining to repair requests and rolling stock
Supply Chains
IBM & Walmart have partnered in China to create a blockchain project that will monitor food safety
Identification
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by Uport
Diamonds
The De Beers Group is using blockchain to track the importation and sale of diamonds
Real Estate
Blockchain is now being being used to complete real estate deals, the first of which was conducted in Kiev by Propy
Advertising
New York Interactive Advertising Exchange has been experimenting with blockchain as a means of providing an ads marketplace for publishers

In China, a tax based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**

Arbit is a blockchain based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts

In a bid to boost its tourism economy, **Hawaii** is examining ways in which bloackchain- based cryptocurrencies can be adopted throughout the US state

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Use Cases: Finance

Blockchain in Loans and Mortgages

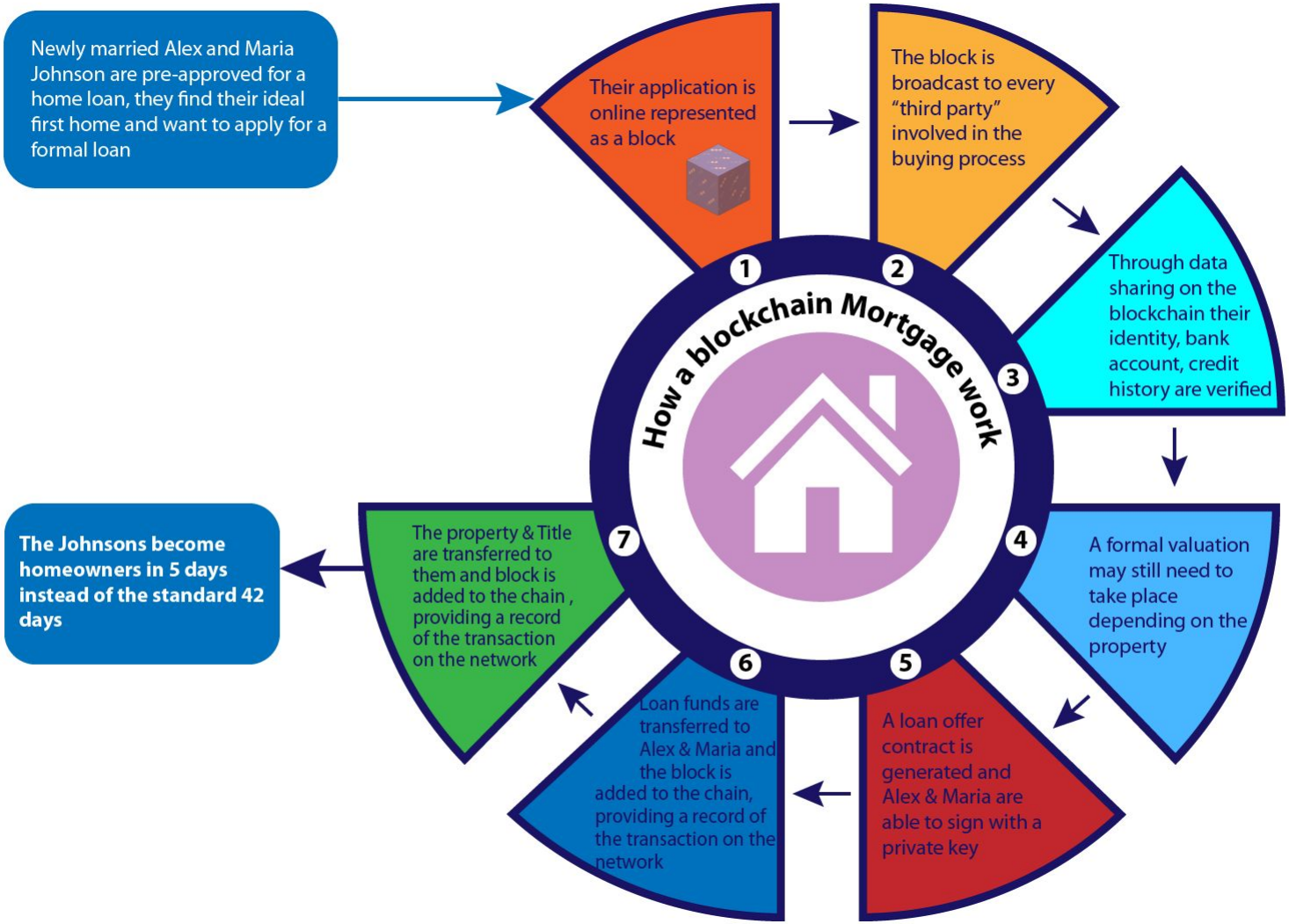
PROBLEM: Lot of intermediaries and Bank walls. Adding to that complexity of the loan process is high.

SOLUTION: A Blockchain based peer to peer mortgage lending platform.

- Initiating a smart contract between borrowers and lenders.
- Token-based loan issuance
- Real-time reporting through Blockchain.

BENEFITS:

- Cost effective and free from the middleman.
- Increasing transaction performance and reducing the time taken for transactions.
- Provide transparency for borrowers and lenders.
- Streamlined and efficient processing of mortgages, thus reducing process time.


Newly married Alex and Maria Johnson are pre-approved for a home loan, they find their ideal first home and want to apply for a formal loan
How a blockchain Mortgage work
1
Their application is online represented as a block
2
The block is broadcast to every "third party" involved in the buying process
3
Through data sharing on the blockchain their identity, bank account, credit history are verified
4
A formal valuation may still need to take place depending on the property
5
A loan offer contract is generated and Alex & Maria are able to sign with a private key
6
Loan funds are transferred to Alex & Maria and the block is added to the chain, providing a record of the transaction on the network
7
The property & Title are transferred to them and block is added to the chain , providing a record of the transaction on the network
The Johnsons become homeowners in 5 days instead of the standard 42 days

Blockchain in Cross-Border Payments

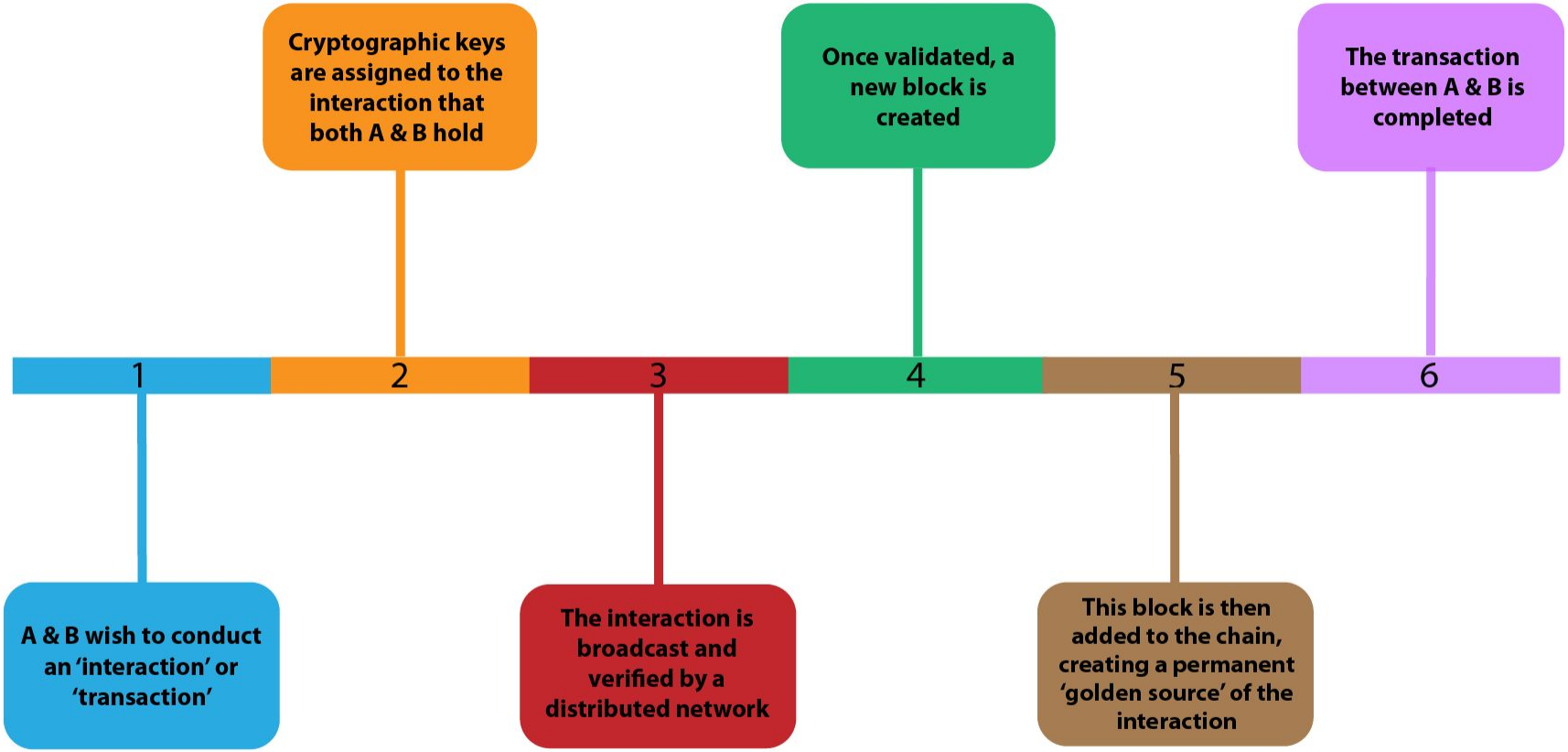
PROBLEM: Opaque process, cost and time for the transactions are high.

SOLUTION: A Blockchain based solution with Digital assets and Smart Contracts.

- Digital assets will cut the operational as well as capital compliance cost.
- Smart Contracts help parties to engage in financial agreements.
- Multiple currencies can be exchanged between Banks.

BENEFITS:

- Greater speed and affordability.
- Transparency and security.
- Reduce economic risks.
- Digital currencies will also solve the cross-border liquidity issues.


1
2
3
4
5
6
A & B wish to conduct an 'interaction' or 'transaction'
Cryptographic keys are assigned to the interaction that both A & B hold
The interaction is broadcast and verified by a distributed network
Once validated, a new block is created
This block is then added to the chain, creating a permanent 'golden source' of the interaction
The transaction between A & B is completed

Blockchain in Stock Trading

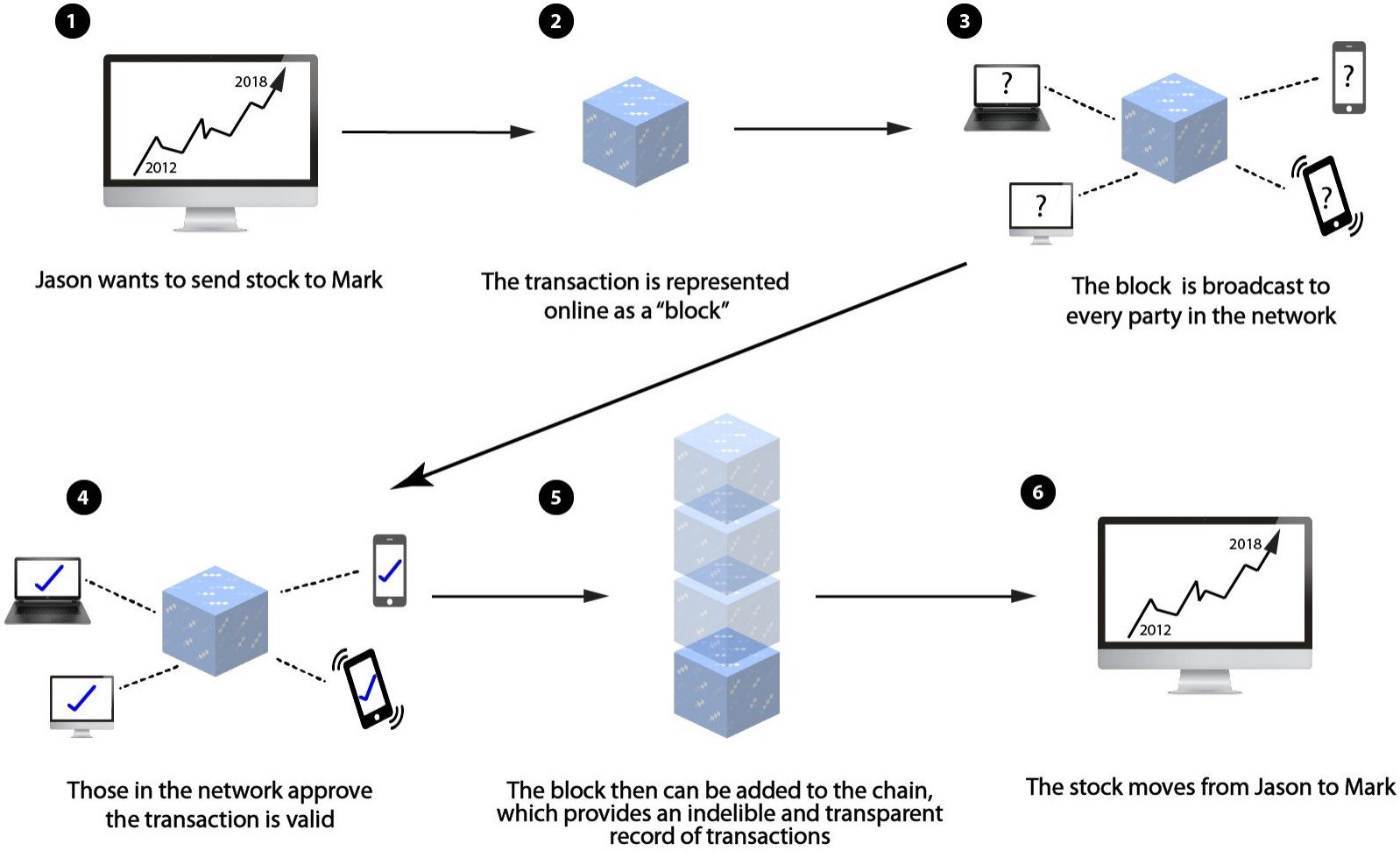
PROBLEM: The current functioning of stock exchanges involves complex procedures that can be time-consuming, cost inefficient, cumbersome, and prone to risks.

SOLUTION: A Blockchain private trading platform that would allow private companies to represent their share ownership digitally.

- Complete and record private-securities transactions for a private investor over the Blockchain.
- Smart Contracts can be initiated to agree on the validity of a specific stock movement.
- Settlement of securities can be based on digital tokens.

BENEFITS:

- Traceability of stock provenance.
- Eliminating 3rd parties.
- Faster Settlements.


1
2018
2012
Jason wants to send stock to Mark
2
The transaction is represented online as a "block"
3
?
?
?
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
2018
2012
The stock moves from Jason to Mark

Blockchain in Online Identities

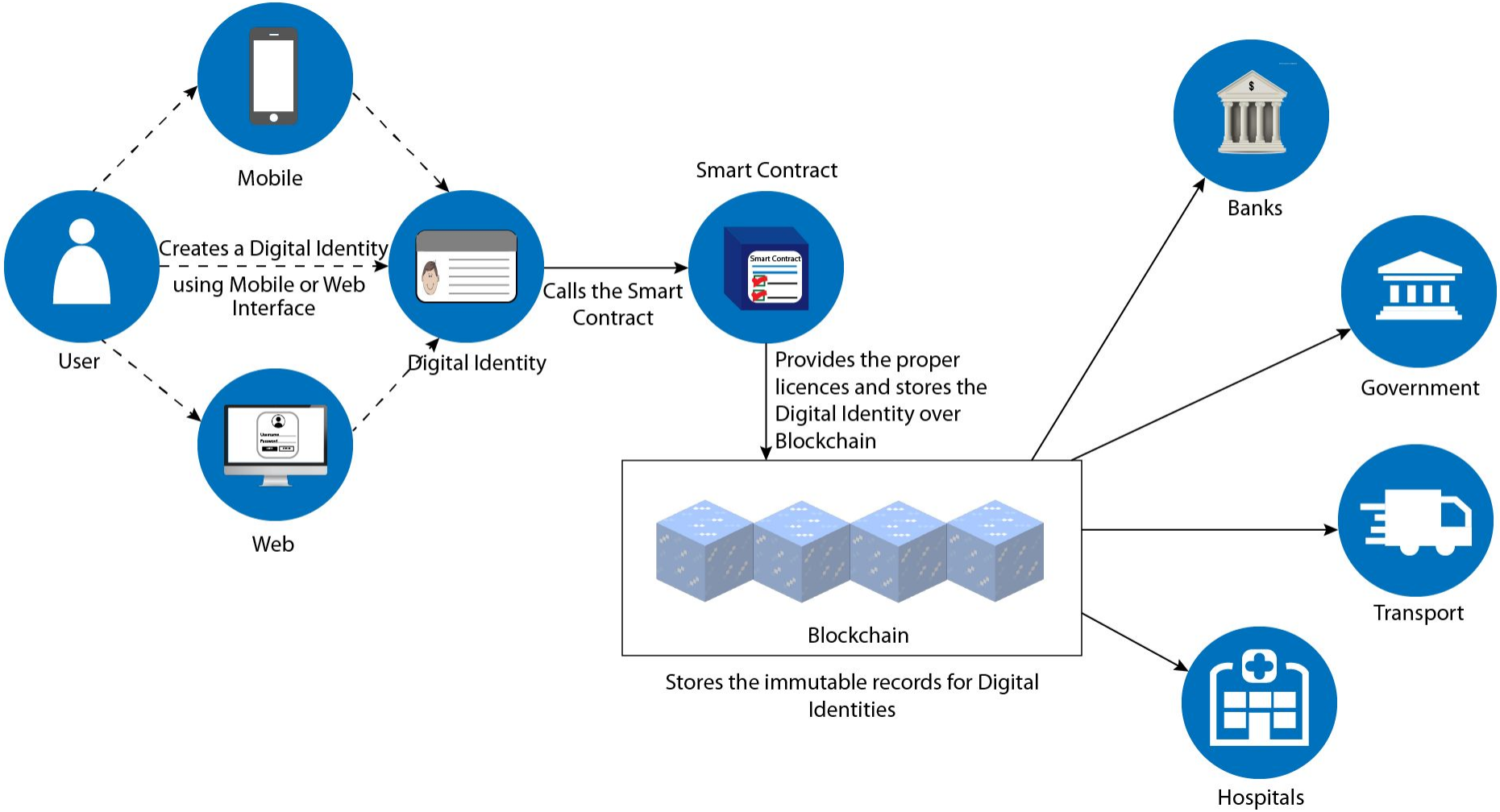
PROBLEM: Online identity management is a time-consuming and costly process.

SOLUTION: A permission based Blockchain solution to store digital identities.

- Immutable storing of user identities, which would provide a tamper-proof solution.
- Users can choose how they identify themselves and with whom their identity is shared.
- Sharing of ledger between banks to maintain a single source of identity.

BENEFITS:

- Remove the middlemen and provide every party access to the same source of truth.
- Real-time information.
- Authentication and Authorization.


Mobile
User
Creates a Digital Identity
using Mobile or Web
Interface
Digital Identity
Web
Smart Contract
Calls the Smart
Contract
Provides the proper
licences and stores the
Digital Identity over
Blockchain
Blockchain
Stores the immutable records for Digital
Identities
Banks
Government
Transport
Hospitals

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Use Cases: Healthcare

Blockchain in Public Health Security

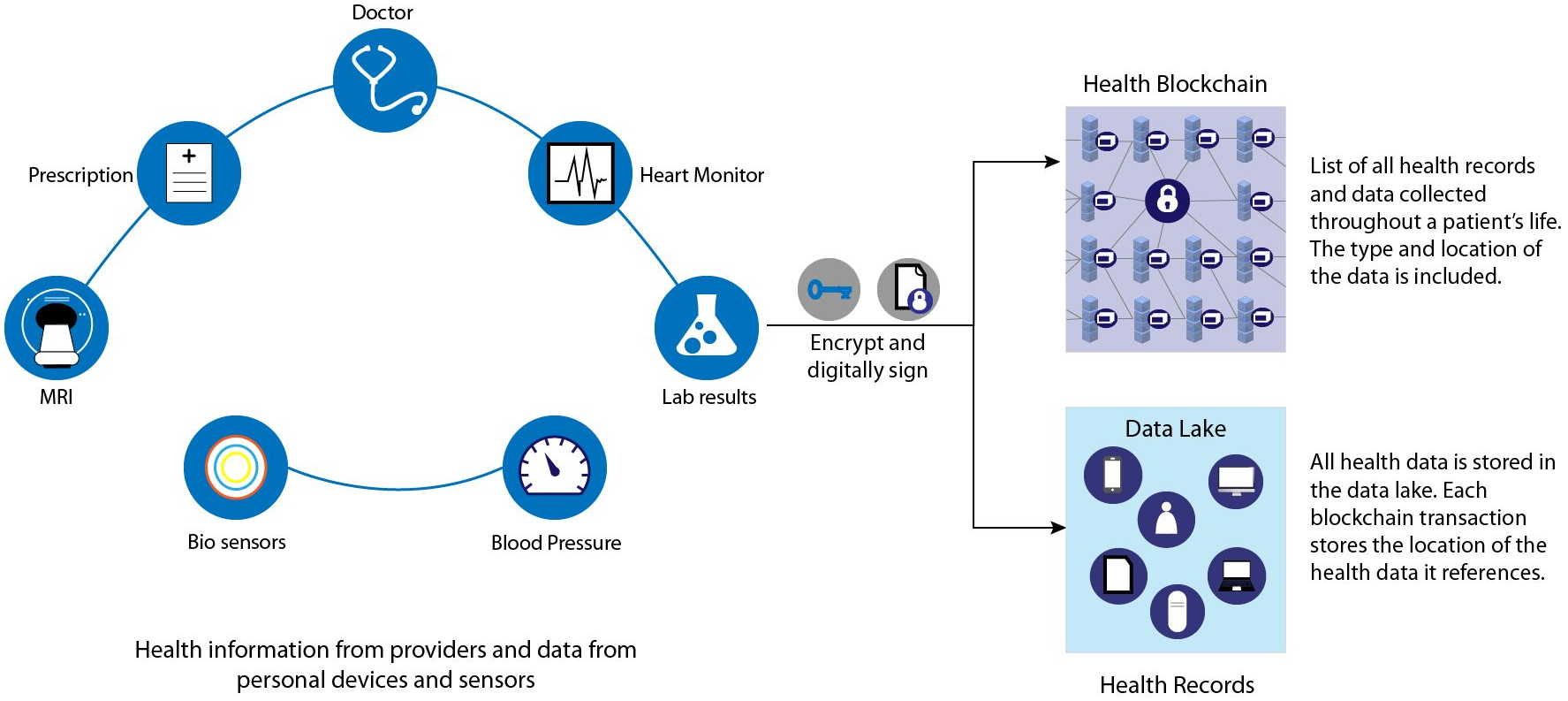
PROBLEM: How to maintain and share public health records?.

SOLUTION: A public blockchain between healthcare providers, pharmacies, and patients.

- All the health records are maintained using the public ledger.
- An encrypted link to the patient's record is created for the doctor and patient access only.
- IoT device can be integrated to record data directly over the blockchain.
- Smart Contracts can be initiated between entities to share medical data.

BENEFITS:

- Data security is maintained as the hackers would need to breach every participant in the network simultaneously.
- Data privacy can be maintained by using proper permissions.
- Reduce barriers involved in complex data sharing agreements.


Doctor
Prescription
Heart Monitor
MRI
Lab results
Bio sensors
Blood Pressure
Health information from providers and data from personal devices and sensors
Encrypt and digitally sign
Health Blockchain
List of all health records and data collected throughout a patient's life. The type and location of the data is included.
Data Lake
All health data is stored in the data lake. Each blockchain transaction stores the location of the health data it references.
Health Records

Blockchain in Drug Traceability

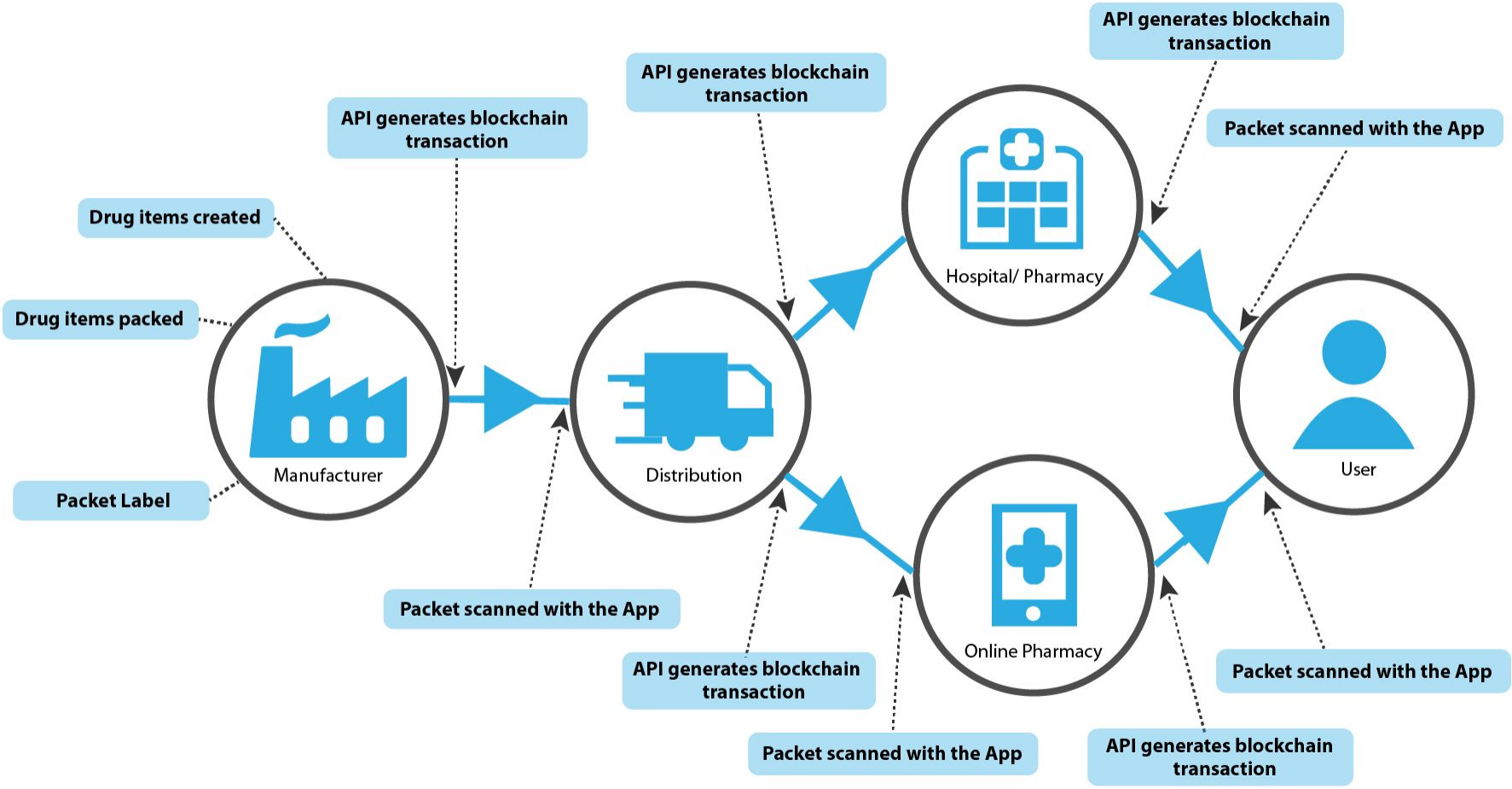
PROBLEM: A lot of counterfeit drugs on the market which even lead to loss of lives.

SOLUTION: A blockchain based solution for drug supply chain integrity.

- Unique ID based solution for tracking the drugs.
- A separate ledger can be initiated for government-approved drug suppliers.
- Patents for the drugs can also be recorded over the blockchain for verification.
- Smart Contracts can be initiated between suppliers and distributors.

BENEFITS:

- Provide visibility needed to make critical decisions.
- Reduce costs lost due to counterfeit.
- Protect consumers and brand through reduction of fake pharmaceuticals companies.


Drug items created
Drug items packed
Packet Label
Manufacturer
API generates blockchain transaction
Packet scanned with the App
Distribution
API generates blockchain transaction
API generates blockchain transaction
Hospital/ Pharmacy
Packet scanned with the App
User
API generates blockchain transaction
Packet scanned with the App
Online Pharmacy
Packet scanned with the App
API generates blockchain transaction

Blockchain in Clinical Trials

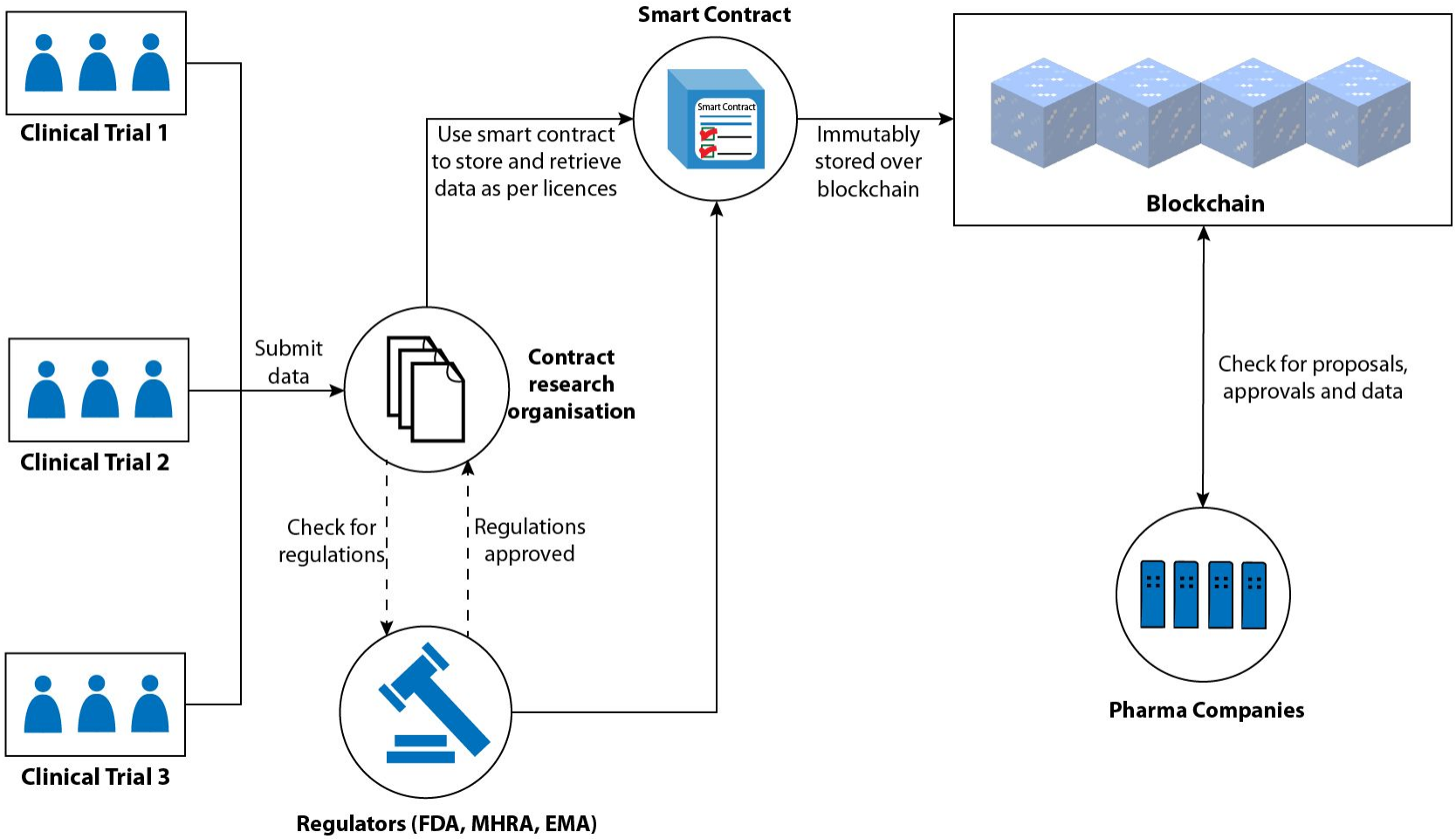
PROBLEM: Over half of the clinical trials report misconducted research.

SOLUTION: A blockchain based solution for providing secure and synchronised data submission.

- Patients can control their own data and contribute to decisions related to their preferred treatment choices
- Intercommunication can be established using smart contracts.
- Authorisation can be maintained for different parties involved.

BENEFITS:

- Increase access to urgent information.
- Increase inter-operations between multiple hospitals.
- Insight into multiple data sources, resulting in new treatment plans.


Smart Contract
Clinical Trial 1
Use smart contract to store and retrieve data as per licences
Immutably stored over blockchain
Blockchain
Clinical Trial 2
Submit data
Contract research organisation
Check for proposals, approvals and data
Check for regulations
Regulations approved
Pharma Companies
Clinical Trial 3
Regulators (FDA, MHRA, EMA)

Blockchain in Health Care Billing

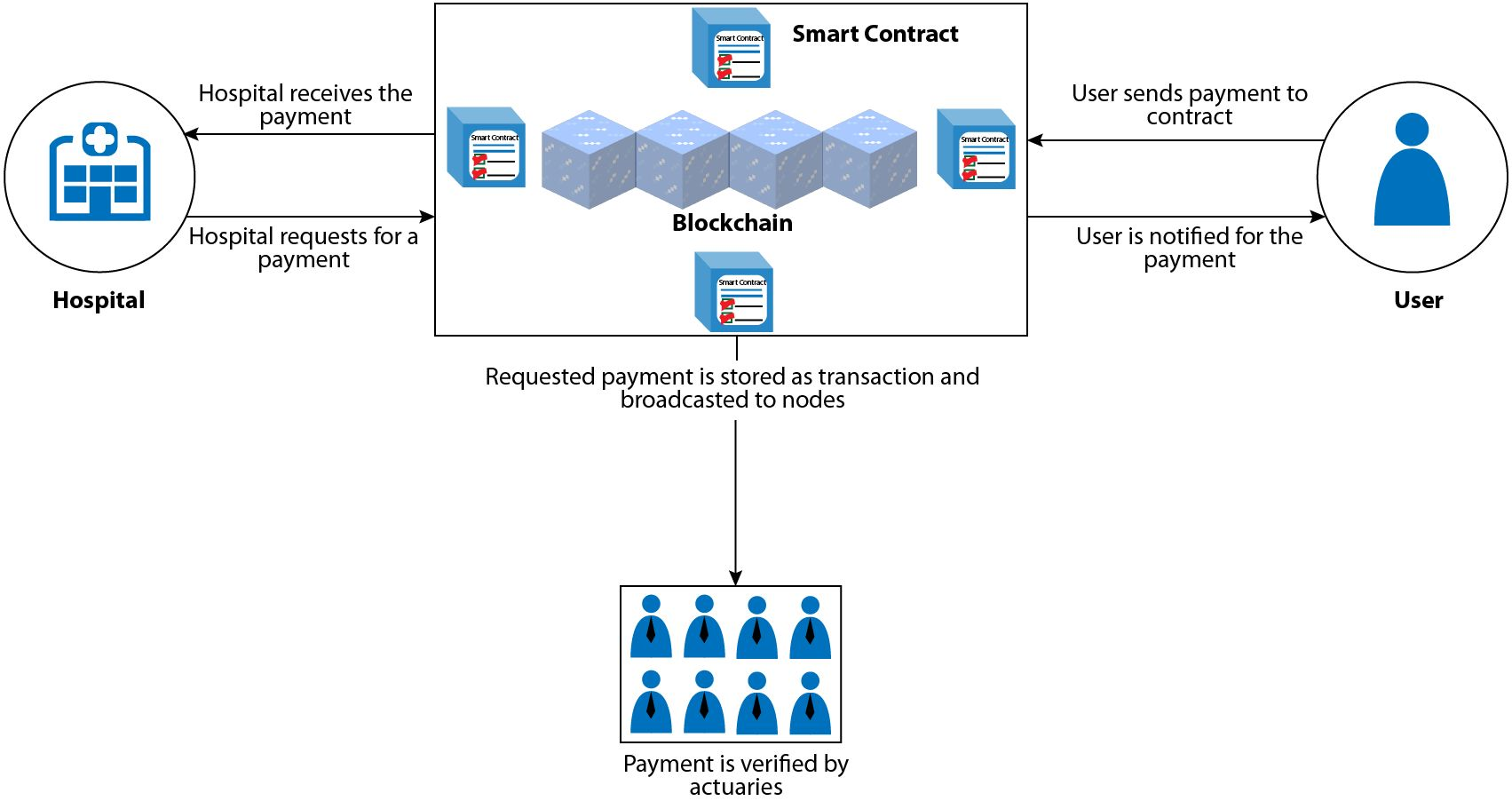
PROBLEM: Healthcare billing faces several challenges including unintentional billing inaccuracies, fraud and time taken to process the transactions.

SOLUTION: A blockchain based solution for proper payment processing.

- Blockchain will provide audit and transparency for the all the payments processed.
- Smart Contracts can be initiated for automatic payment processing as per the services received.
- Smart Contracts can also be initiated for providing insurance to the patients.

BENEFITS:

- By storing billing information inside blockchain, a reliable source of information for claims adjudication will be kept..
- Reduce costs and save time for funds transfer.
- Billing frauds will be reduced as everything is immutable.


Smart Contract
Hospital receives the payment
Hospital requests for a payment
Hospital
Blockchain
User sends payment to contract
User is notified for the payment
User
Requested payment is stored as transaction and broadcasted to nodes
Payment is verified by actuaries

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Use Cases: Media and Entertainment

Blockchain in Piracy

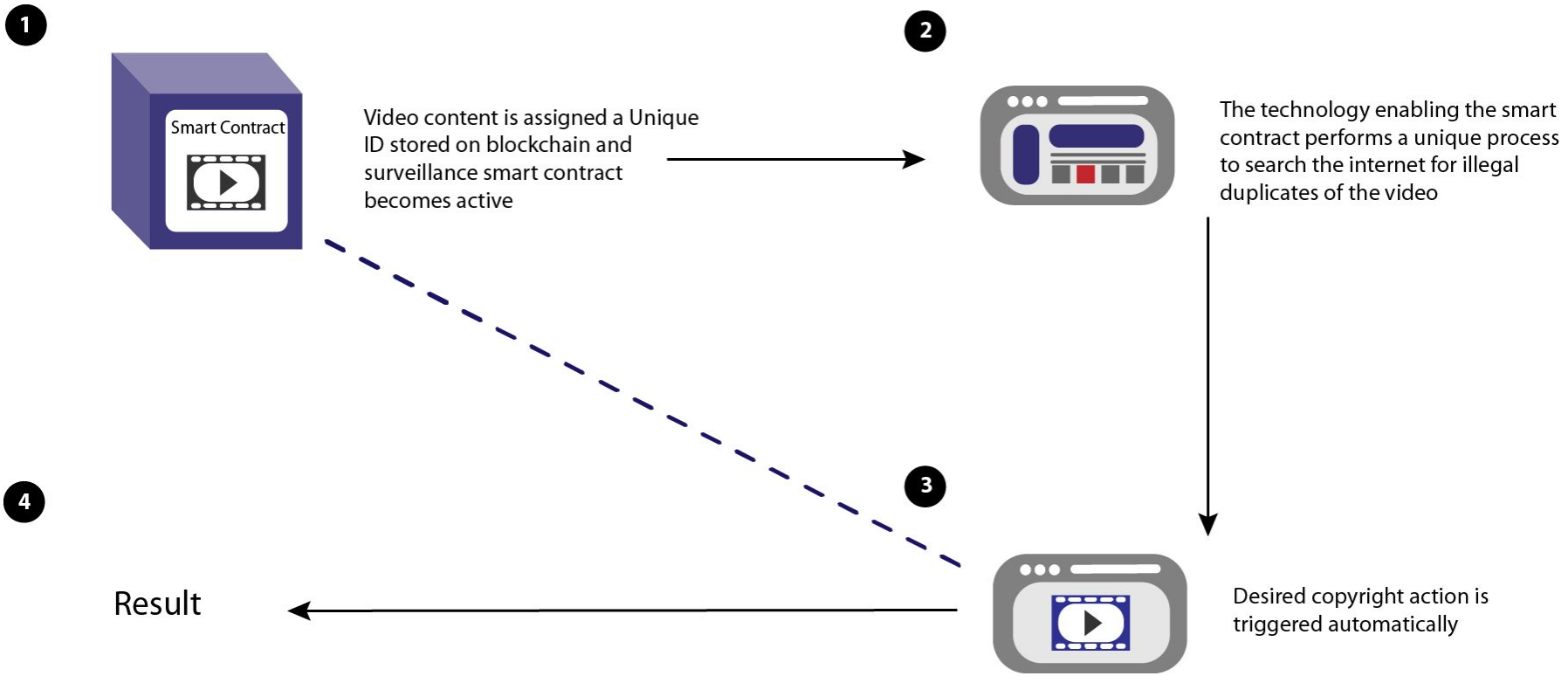
PROBLEM: Digital media created for human consumption can be captured and duplicated. This causes monetary loss to the content creators.

SOLUTION: A blockchain based media tracking technology.

- Video content is assigned a unique id and stored on the Blockchain.
- Content can be consumed using the tokens.
- A Smart Contract can be triggered for surveillance of the copyrights.
- Smart Contract can trigger copyrights action automatically on finding the duplicate content.

BENEFITS:

- This will enable tracking the life cycle of any content.
- Piracy can be tracked instantly.
- Micro consumption of content can be achieved by using such technology.


1
Smart Contract
Video content is assigned a Unique ID stored on blockchain and surveillance smart contract becomes active
2
The technology enabling the smart contract performs a unique process to search the internet for illegal duplicates of the video
3
Desired copyright action is triggered automatically
4
Result

Blockchain in Content Crowdfunding

PROBLEM: Many independent movie makers are not able to raise the money for their niche projects.

SOLUTION: A Blockchain based crowdfunding solution with the use of tokens.

- A Blockchain based crowdfunding solution with the use of tokens.
- The public can invest into projects using the Smart Contracts.
- The public would be able to earn from content market capture.
- Tokens and returns can be made available in the form of percentages.
- Additionally, KYC can be enabled to track the investments.

BENEFITS:

- Blockchain-powered crowdfunding offers tons of advantages, including privacy and transparency.
- There would be no need to source out and implement any external payment or verification solutions.

Concept for the media/movie is created

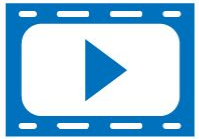
Concept is finalized into a presentable form

Smart Contract is initiated for funding

Smart Contract is immutably stored over the blockchain and agreed by the people participating in the funding

People/Investors provide funding for the concept by depositing in Smart Contract and in return getting some tokens

Smart Contract for crowdfunding ends on a specific date and funds are accumulated in fiat currency



Media/Movie is produced using the funds accumulated

Media/Movie is released for the public consumption

People earn through Smart Contract on the basis of performance of the media/movie by the percentage of tokens they are holding

Blockchain in Digital Advertisements

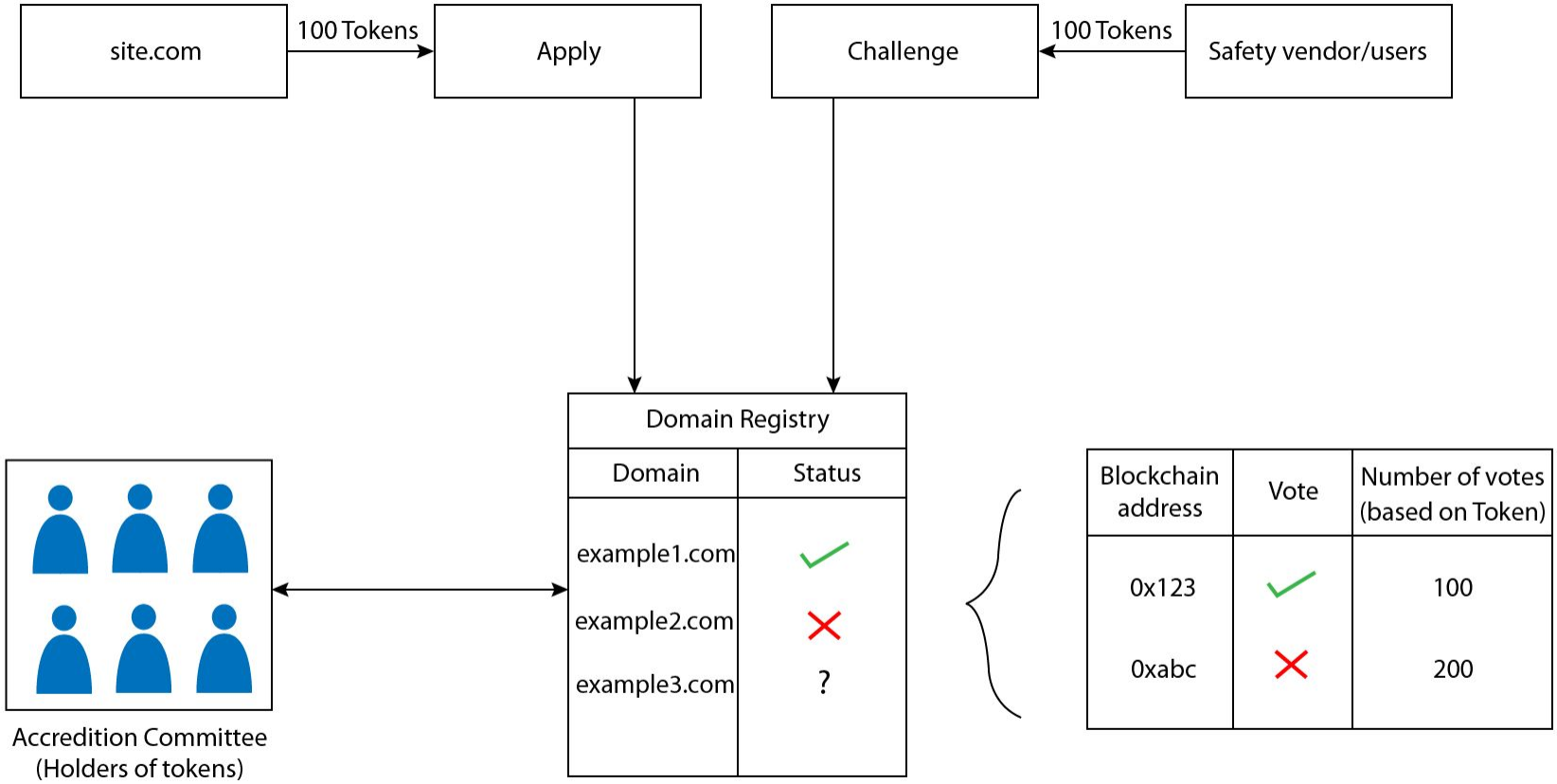
PROBLEM: Ad fraud is a multibillion-dollar problem concerning the practice of fraudulently representing online advertisement impressions, clicks, conversion or data events to generate revenue.

SOLUTION: A set of interoperable open protocols built on the public blockchain.

- A smart contract can be initiated on the blockchain that maintains and stores a record of publisher domain names accredited as non-fraudulent.
- Holders of tokens over the Blockchain can perform the accreditation.
- Moreover, the ledger can be challenged and updated if a fraudulent entry has been made and still maintain the history of all the entries.

BENEFITS:

- It will provide transparency for the advertisers.
- The incentives for artificially inflating supply volume for advertisements will be reduced.


site.com
100 Tokens
Apply
Challenge
100 Tokens
Safety vendor/users
Domain Registry
Domain
Status
example1.com
example2.com
example3.com
?
Accredition Committee
(Holders of tokens)
Blockchain address
Vote
Number of votes (based on Token)
0x123
100
0xabc
200

Blockchain in Royalty Payments

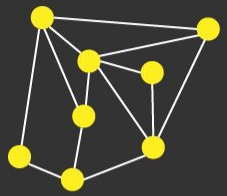
PROBLEM: It is challenging to pay fairly for creative work in a digital world where it is easy to share and distribute copies.

SOLUTION: A transparent blockchain-based ledger as a foundation technology that contains media assets and their rights holders.

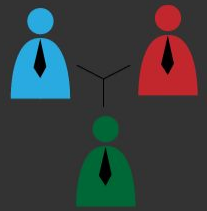
- A ledger for supporting media and copyrights permissions can be initiated.
- The owner of the media can distribute rights through the initiation of Smart Contracts.
- Smart contracts can automate royalty payments based on a song's consumption, including streaming.

BENEFITS:

- It will provide transparency for the content developers on the consumption and payments.
- The payments can be made instantly as per the usage of the media.



Entertainment publishers and distributors in music, gaming, television or cinema connect to the blockchain platform



Business terms and conditions are agreed upon by the group

Terms and conditions are coded, reviewed and approved by the group

Consumers buy content online or from retail stores and generate millions of transactions daily

Distributors and publishers review information, have better visibility to financial positions and in the future, may more quickly make royalty payments to downstream participants like entertainers, graphic designers, game developers

Distributors and publishers get instant access to applicable information and review data

Royalty transactions are recorded on blockchain as per the terms and conditions

	Debit	Credit
Distributor	5.00	5.00
Publisher	15.00	15.00
Developer	3.00	3.00

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Use Cases: Real Estate

Blockchain in Rental

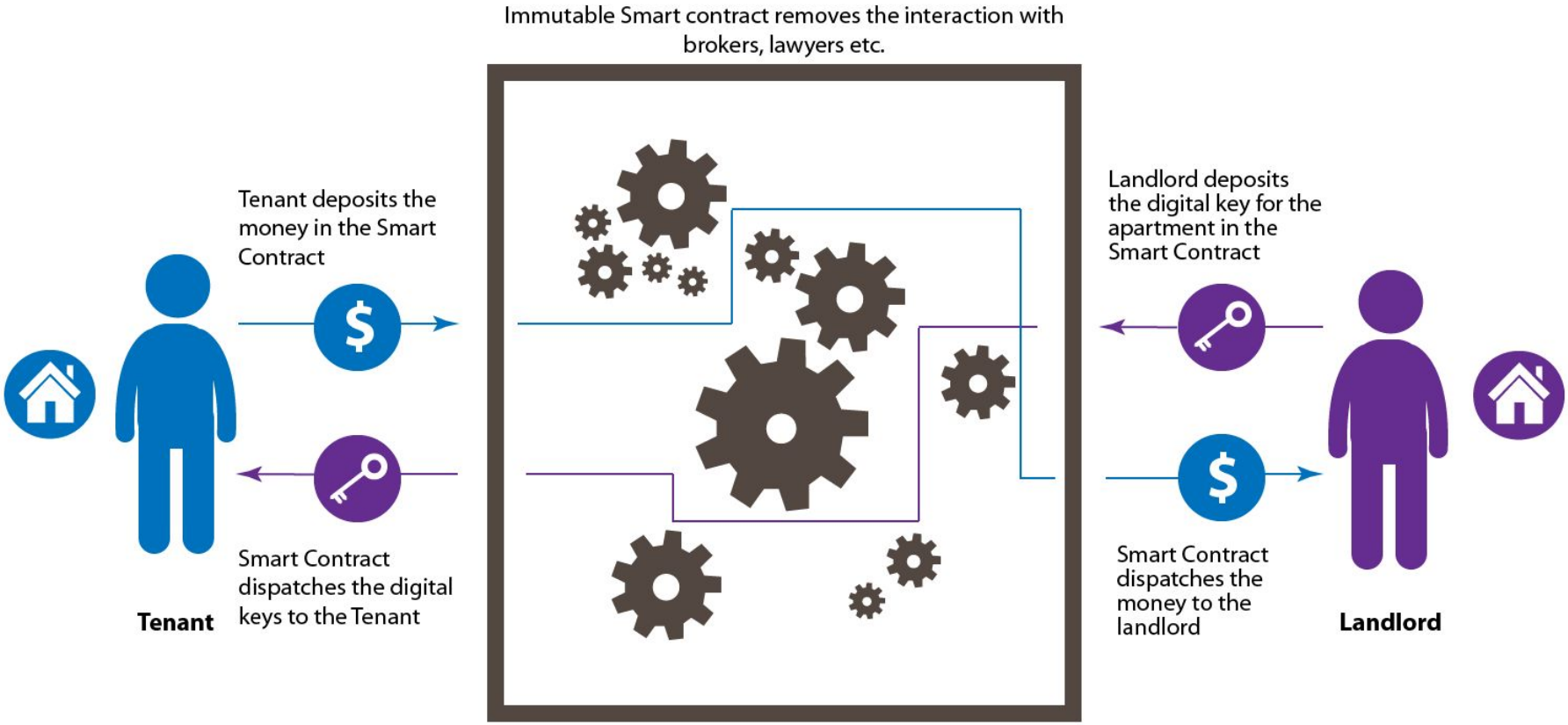
PROBLEM: Multiple listing services providing incomplete lists. Moreover, releasing apartment ownership or documents are not adequately defined.

SOLUTION: A public blockchain for listing and storing the rental documents and servicing payments.

- All the rental records will be available in one place.
- All transactions and listings can be independently verified and automatically reconciled.
- The rental process will be the implemented with the help of self-executing smart contracts. Automated transactions between the tenant and the landlord eliminate the need for a real estate agent altogether.

BENEFITS:

- Negates the risk of double spending, fraud, abuse and the manipulation of transactions.
- Reduce barriers involved in complex data sharing agreements saving both the property owners and renters.


Immutable Smart contract removes the interaction with brokers, lawyers etc.
Tenant deposits the money in the Smart Contract
Smart Contract dispatches the digital keys to the Tenant
Tenant
Landlord deposits the digital key for the apartment in the Smart Contract
Smart Contract dispatches the money to the landlord
Landlord

Blockchain in Title Records

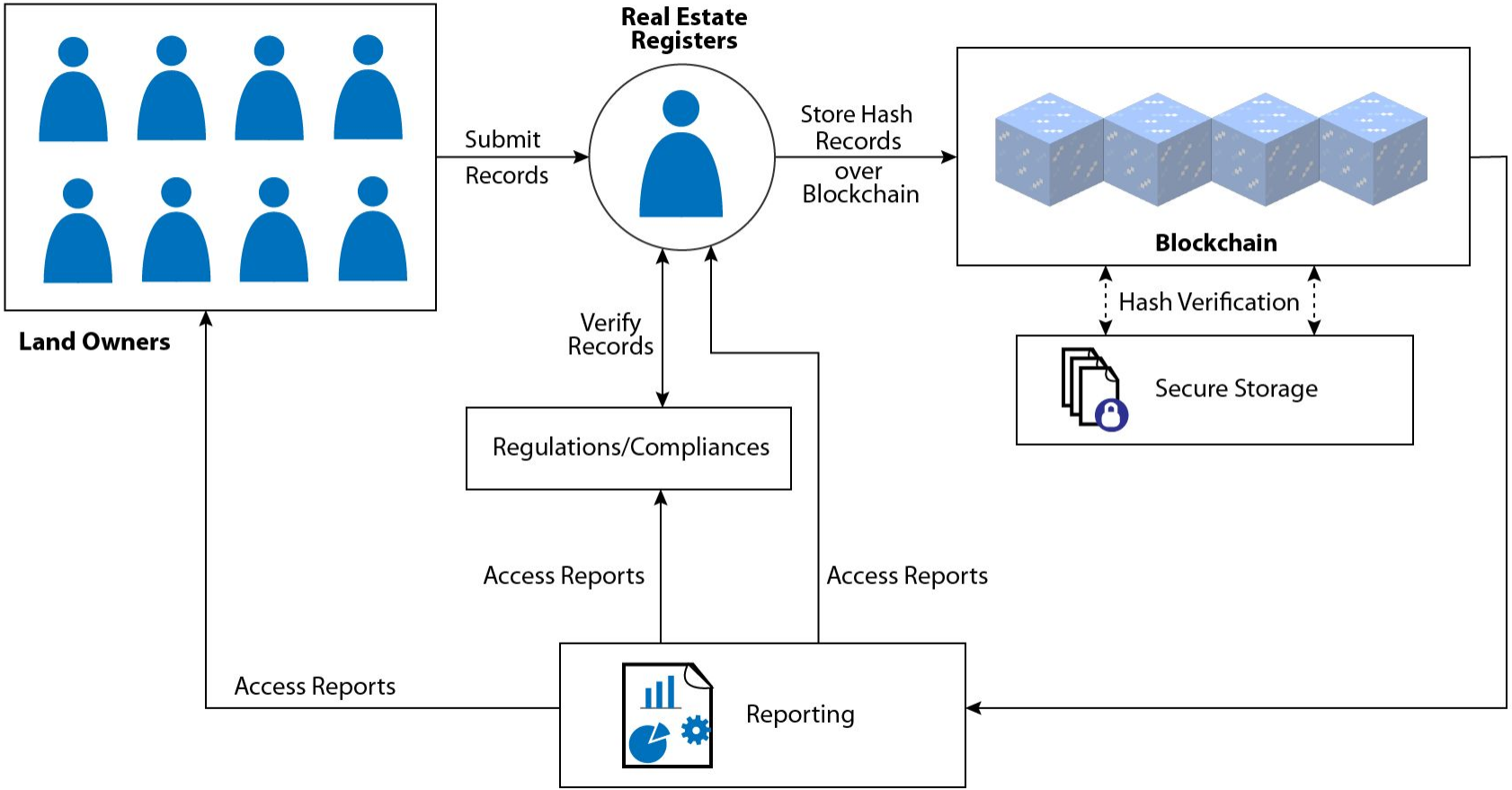
PROBLEM: Real property records are stored and maintained at the local government level. Deeds of trust rely on original paper documents which are exposed to corruption and natural disasters.

SOLUTION: Multiple ledger based solution where each township/county stores their land records as per their jurisdiction.

- All the records will be securely stored and instantly accessible including historical title records
- Tokens can be used over the Blockchain to transfer the ownership of the land titles.
- Micro property ownership can be utilized by using the smart contracts.

BENEFITS:

- Negates the risk of fraud, abuse and the manipulation of land records.
- Provides an entry barrier for the middle-class families to buy micro properties.
- Multiple nodes over the Blockchain prevents data loss during the time of natural disasters.


Real Estate Registers
Land Owners
Submit Records
Store Hash Records over Blockchain
Blockchain
Hash Verification
Secure Storage
Verify Records
Regulations/Compliances
Access Reports
Access Reports
Access Reports
Reporting

Blockchain in Regulations

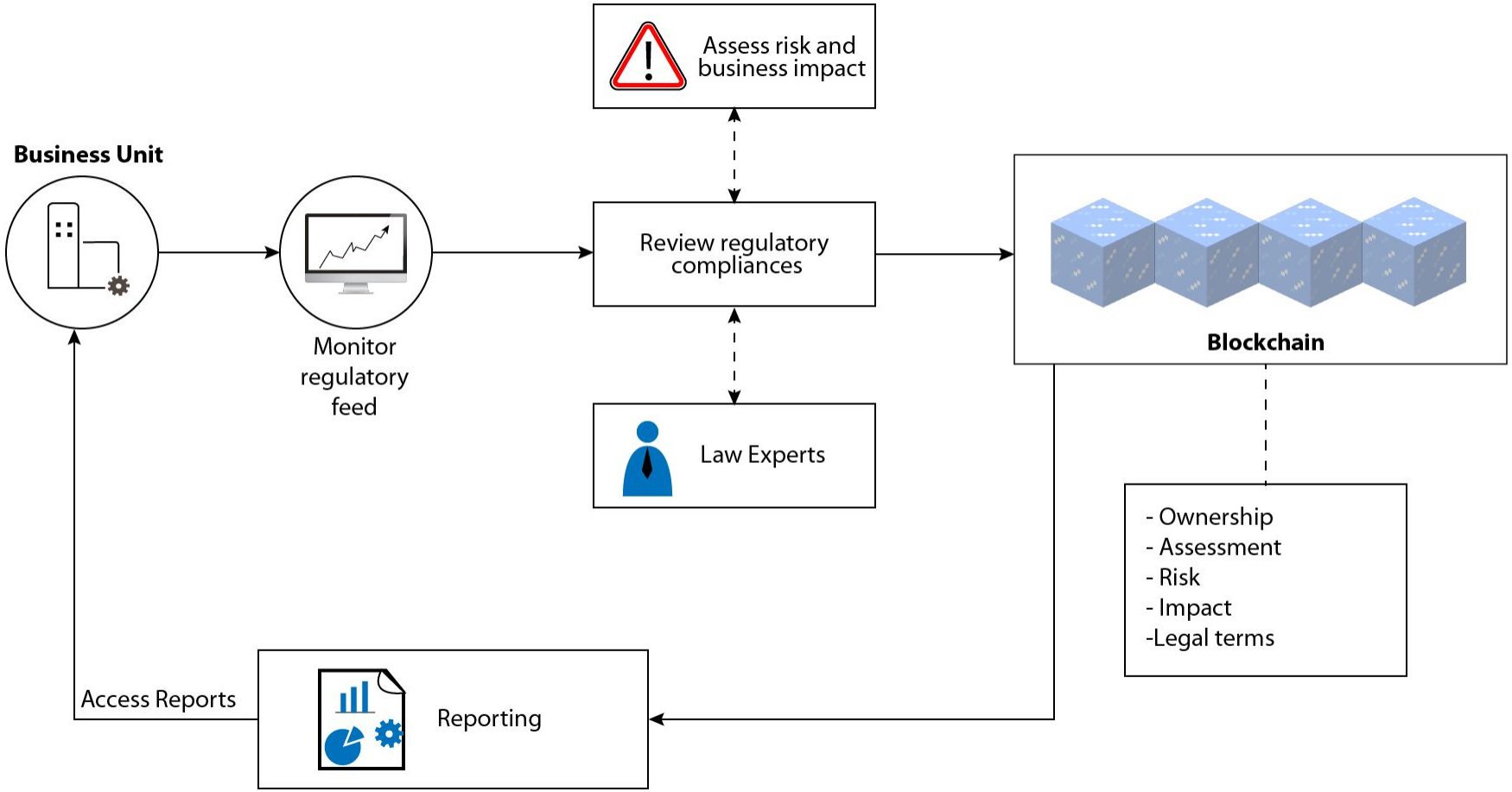
PROBLEM: Regulations over the real estate are not transparent and not adequately visible to all the parties.

SOLUTION: A public blockchain for listing out regulations over the real estate.

- All the regulations are transparent to every party in the value chain.
- Regulations can be put on the ledger as a transaction and then broadcasted to all.
- Ease of transparency for considering the costs and timelines associated with regulatory cooperation and compliance.

BENEFITS:

- Transparent regulations provide an ideal suite for the all the parties involved.
- Jurisdictions will also benefit one single truth of regulatory compliances over real estate.


Assess risk and business impact
Business Unit
Review regulatory compliances
Blockchain
Monitor regulatory feed
Law Experts
- Ownership
- Assessment
- Risk
- Impact
-Legal terms
Access Reports
Reporting

Blockchain in Liquidity

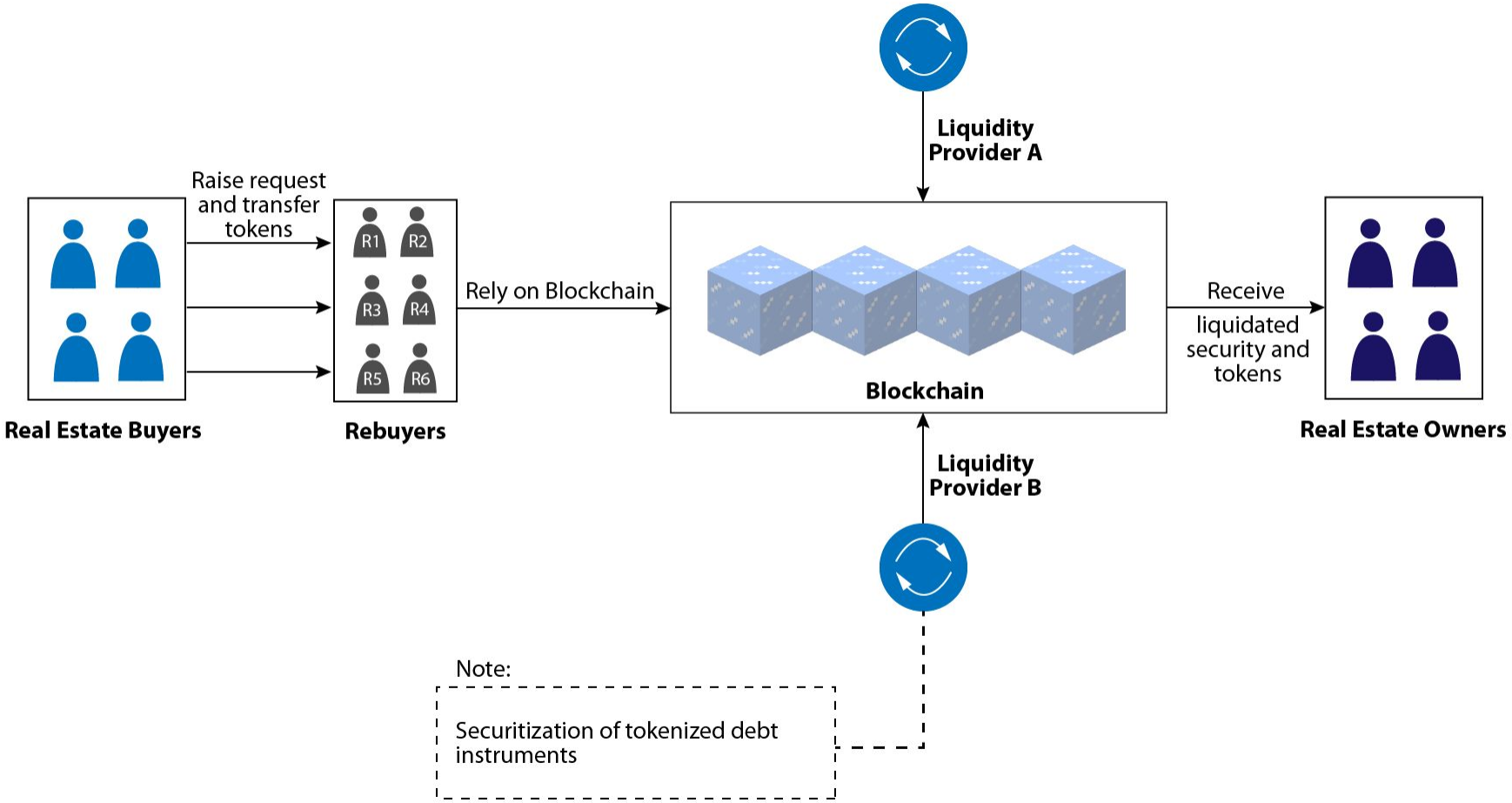
PROBLEM: Currently liquidating the real estate and transactions are not a natural process. It might take weeks to do the same.

SOLUTION: A private or public blockchain, to increase liquidity, process efficiency, and transparency.

- Tokens can be issues over the blockchain which can be used to sell or buy real estate.
- Transactions over a real estate are transparent and visible to all.
- Lenders can extend market reach through novel approaches to the securitization of tokenized debt instruments and their derivatives.

BENEFITS:

- Real-time transfer of ownership without waiting for days.
- Real Estate Investment Trusts can also be utilized by using the tokens for real estate.


Liquidity Provider A
Raise request and transfer tokens
R1
R2
R3
R4
R5
R6
Rely on Blockchain
Blockchain
Receive liquidated security and tokens
Real Estate Buyers
Rebuyers
Real Estate Owners
Liquidity Provider B
Note:
Securitization of tokenized debt instruments

THANK YOU

For more information contact
info@we2blocks.com

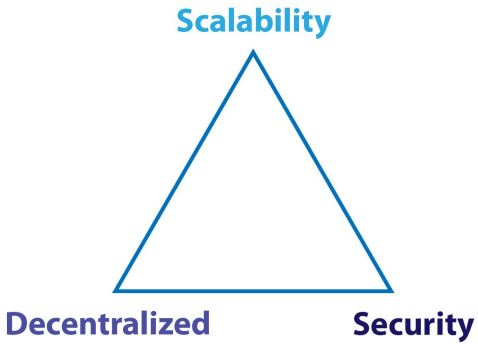
Professional Blockchain Course

Future Scope - Current Research

“Vision is a picture of future, that produces passion.”

Current Research - Blockchain 3.0

- The birth of Blockchain 1.0 was followed by Smart Contracts as Blockchain 2.0 and currently the third generation of Blockchain is rising in form of Hashgraph and Directed Acyclic Graph.
- Blockchain 3.0 is capitalizing on the limitations of it's predecessors by providing scalability, transaction throughput and performance.
- Blockchain currently has a Trilemma between Scalability, Security and Decentralization.



Blockchain Scalability Research

The current research has led to development of scaling solutions which states that not all participants and network nodes need to all the information. A group of nodes can maintain their state and provide a finality over the main chain

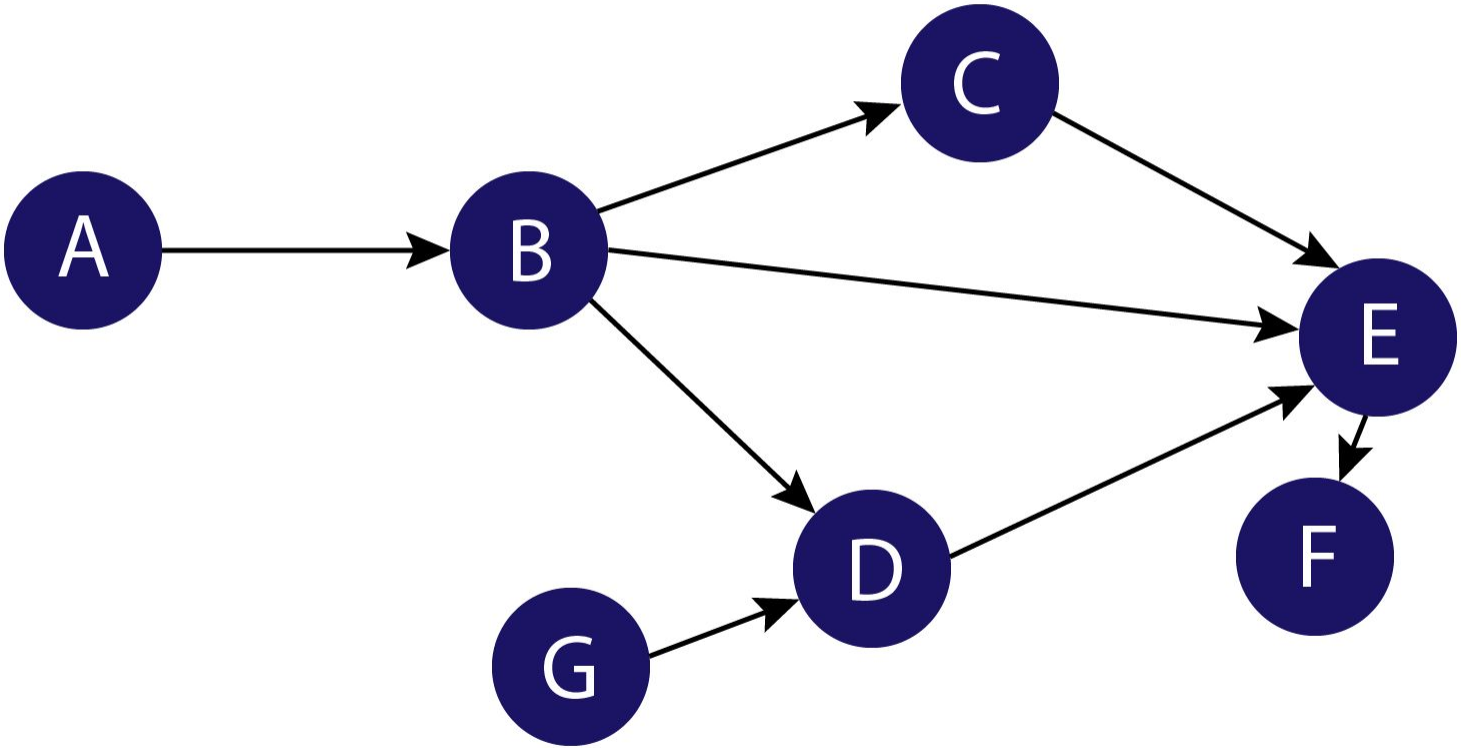
- **Bitcoin lightning network** - The Lightning Network adds another layer to Bitcoin's blockchain and enables users to create payment channels between any two parties on that extra layer. These channels can exist for as long as required, and as they're set up between two people, transactions will be almost instant and the fees will be extremely low or even non-existent.

- **Ethereum sharding** - The entire state of the network is split into a bunch of partitions called shards that contain their own independent piece of state and transaction history. Certain nodes would process transactions only for certain shards, allowing for a higher throughput of transactions.

DAG - A Not So Blockchain Solution

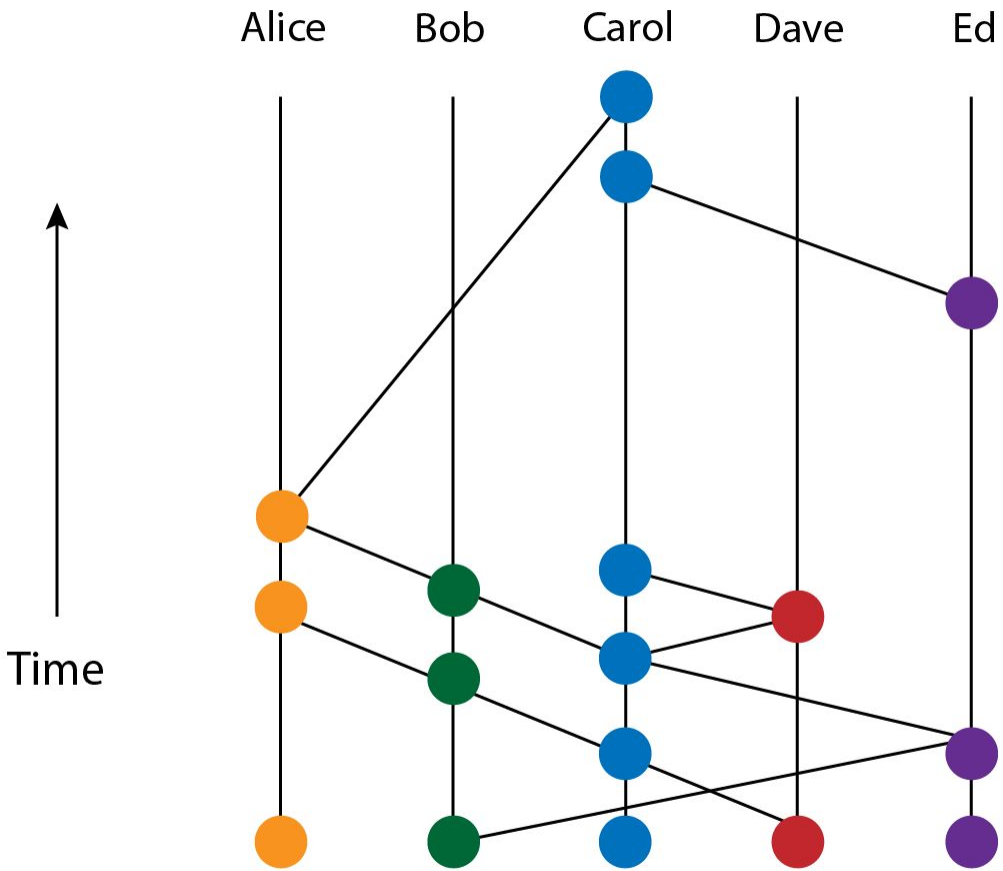
- DAG directly links transactions to other transactions without putting them in the blocks first.
- DAG is more like a mazy network known as “Tangle” and follow horizontal scheme as compared to Blockchain’s vertical scheme.
- There are no blocks or miners in DAG, thus there is no need to wait for the confirmation of the Blocks.
- Tangle has same properties as Blockchain, it is a distributed database present over a peer-2-peer network.
- Unconfirmed new transaction must confirm one or two additional transactions before the unconfirmed transaction can be processed and confirmed itself.
- Markov chain Monte Carlo ensures that network participants do not just confirm their own transactions.

Directed Acyclic Graph



HashGraph - The Latest Excitement

- HashGraph also belongs to the category of Distributed Ledger Technologies that brings in the concept of events, where events are hashed to each other.
- HashGraph was started as consensus library between 6000 banks.
- The current “Hedra Hashgraph platform” aims to drive forward public HashGraph platforms. The leadership council for the same consists of 39 members.
- Events in HashGraph consists of: timestamp, 2 different parent hashes and transactions.
- Hashgraph uses gossip protocol to communicate between 2 computers.
- Hashgraph use “Gossip-about-Gossip” consensus, meaning every participant should know all the transaction history in the Hashgraph.


Alice
Bob
Carol
Dave
Ed
Time

Blockchain vs DAG vs Hashgraph

Technology	Blockchain	Directed Acyclic Graph	Hashgraph
Copyright	Open Source	Open Source	Patented
Consensus	Started with PoW	PoW - Tangle tip	Virtual Voting
Openness	Public Ledger	Public Ledger	Private Ledger
Applications	Bitcoin	Iota	Swirlds
Efficiency(tps)	3-4	500-800	>250,00

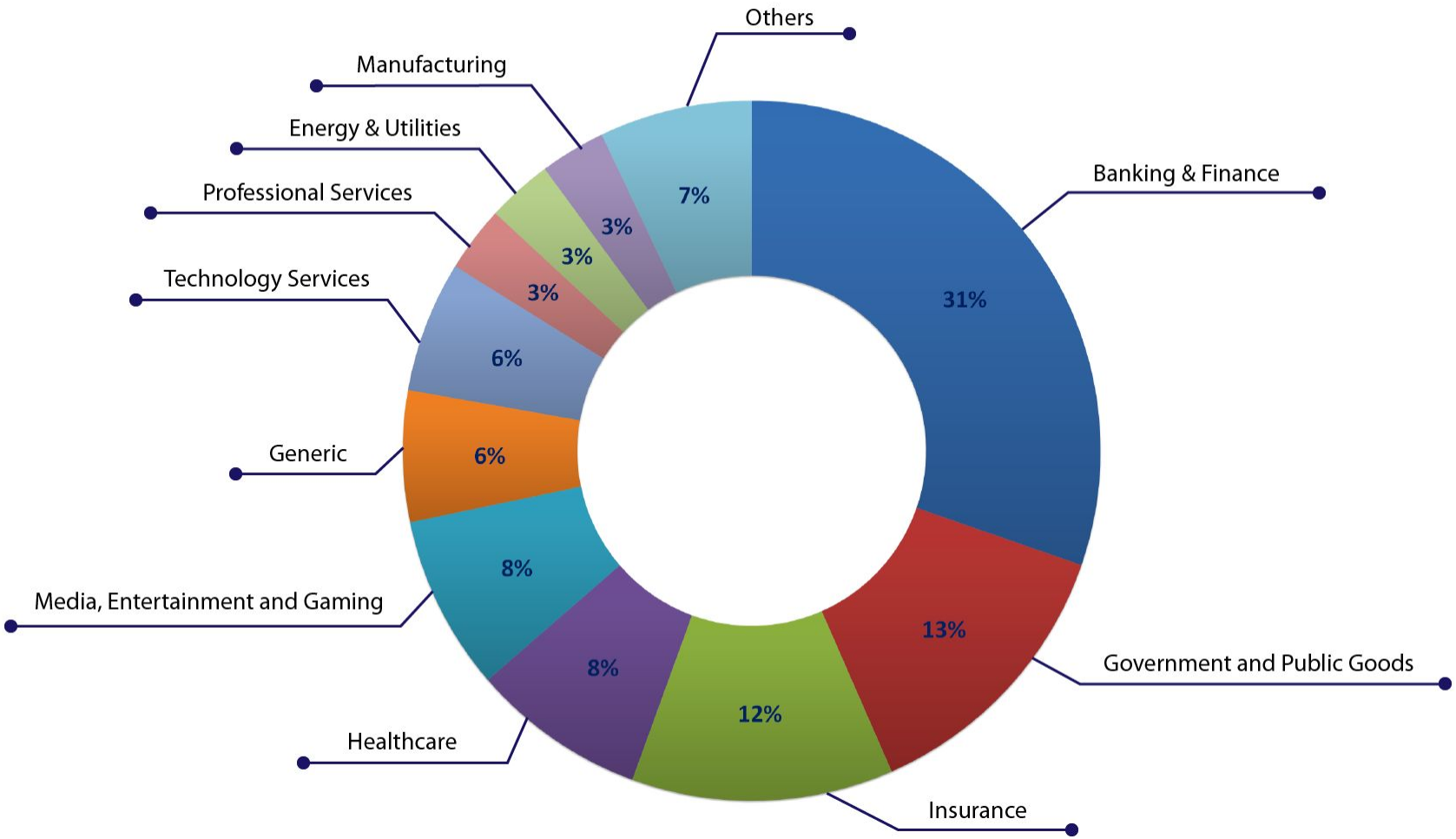
THANK YOU

For more information contact
info@we2blocks.com

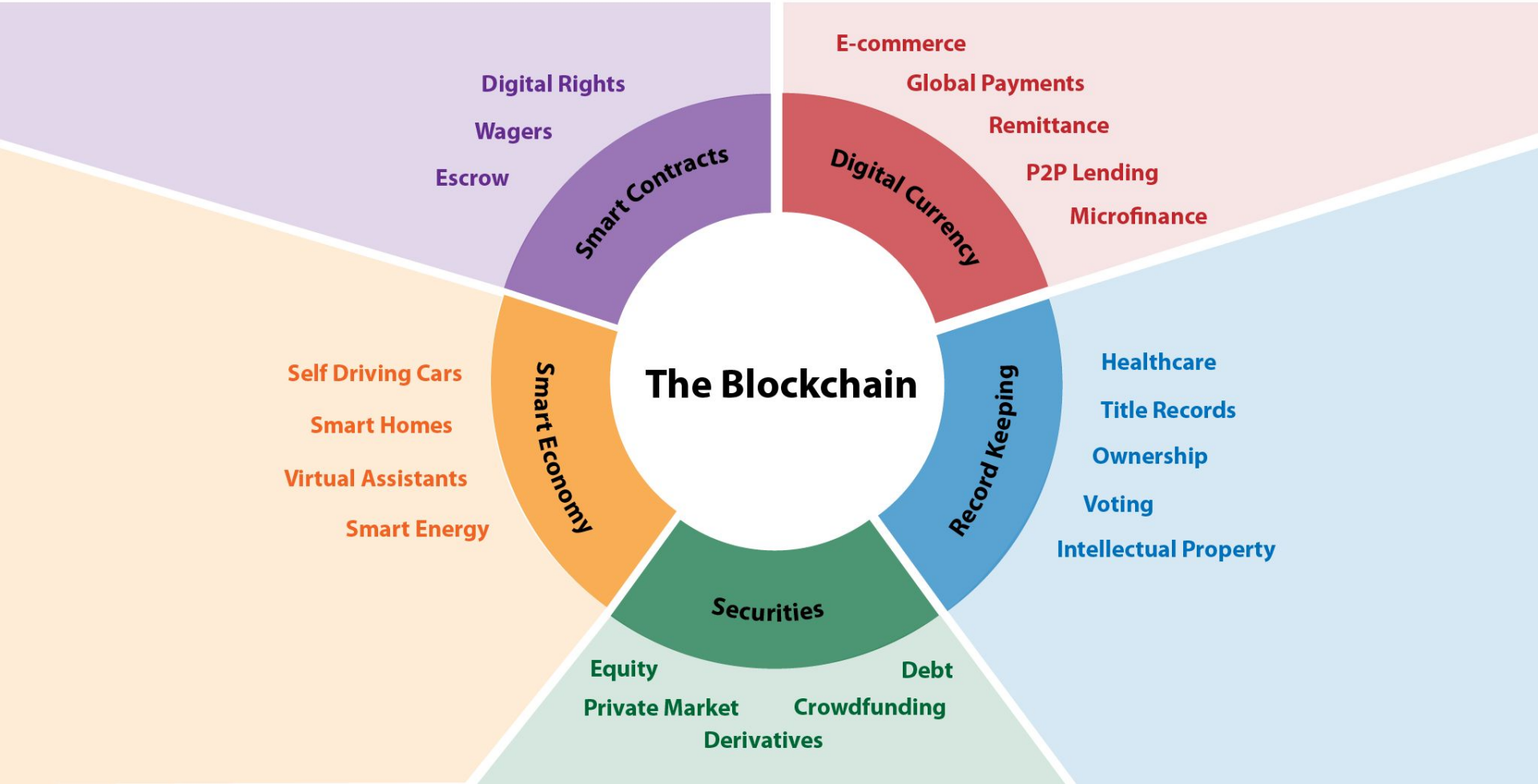
Professional Blockchain Course

Future Scope - Potential Future Applications

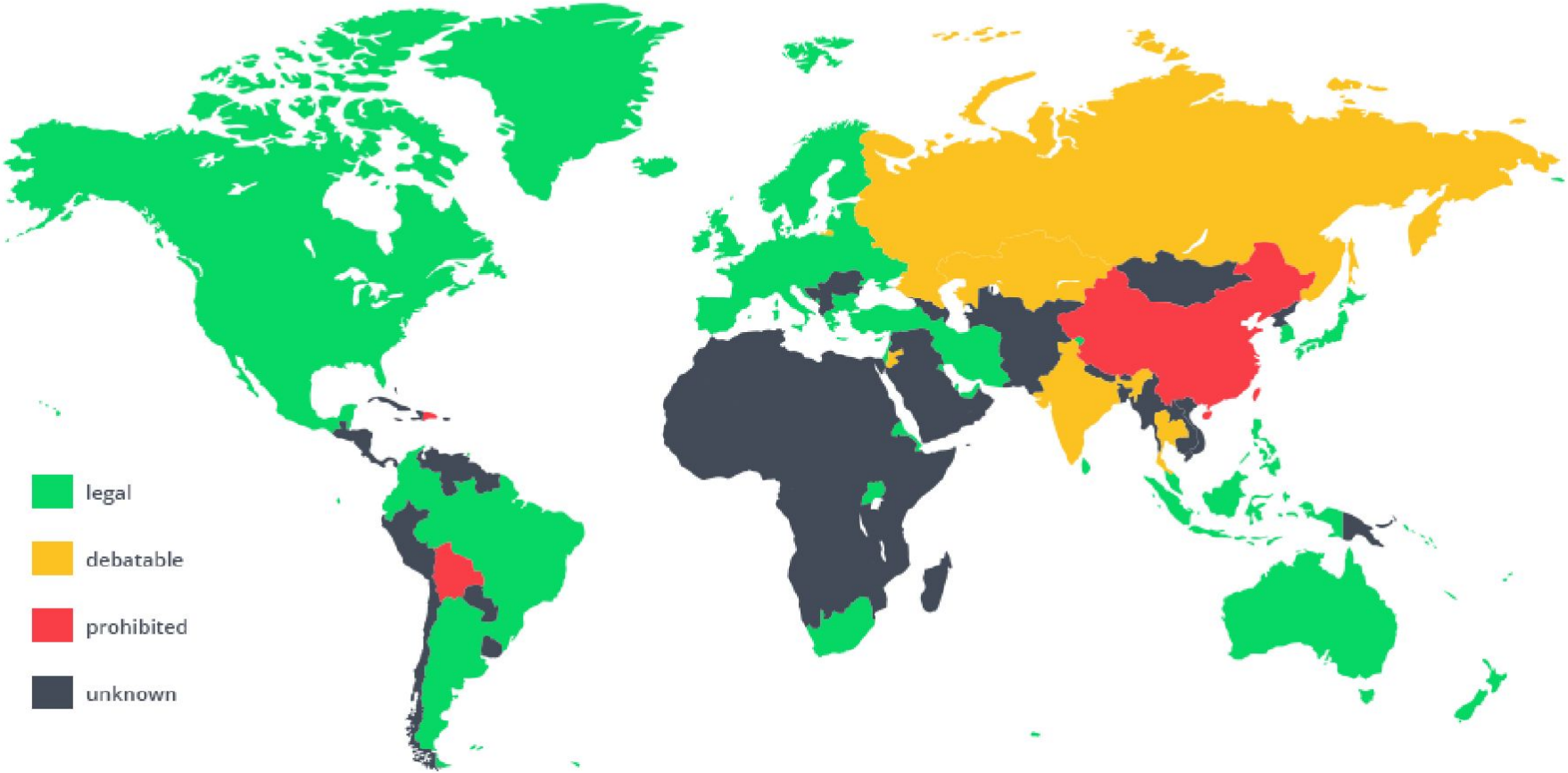
Current use of Blockchain by different sectors



Potential use of Blockchain



Current impact of Blockchain on countries



Potential impact of Blockchain on countries

THANK YOU

For more information contact
info@we2blocks.com

Professional Blockchain Course

Conclusion and Summary

Conclusion and Summary

- The hype of Blockchain is getting converted to real problem solving projects.
- Blockchain market is estimated to grow up to $31 trillion dollars by 2030.
- $2.1 billion dollars were spent on Blockchain projects in 2018 and still only 1% of the companies throughout the world are using Blockchain.
- The growth rate for Blockchain jobs is up to 7000% in 2018.
- Currently, there is only 1 skilled person for 14 Blockchain jobs in USA.
- But, always remember Blockchain is not the silver bullet.
- This would be the right time to get started and learn about Blockchain.

What's Next

- This course was about introducing in depth concepts of Blockchain in the most layman terms possible.
- You can still learn more and start using blockchain for solving problems.
- You can jump to functional side and start learning about Blockchain architecture and how to employ Blockchain in your current legacy systems.
- You can also go towards developer side and choose a platform which suits you to learn more about development.
- We2Blocks will be releasing a in depth Blockchain Architect course soon.
- If you enjoyed the course, do write to us at: info@we2blocks.com.

THANK YOU

For more information contact
info@we2blocks.com