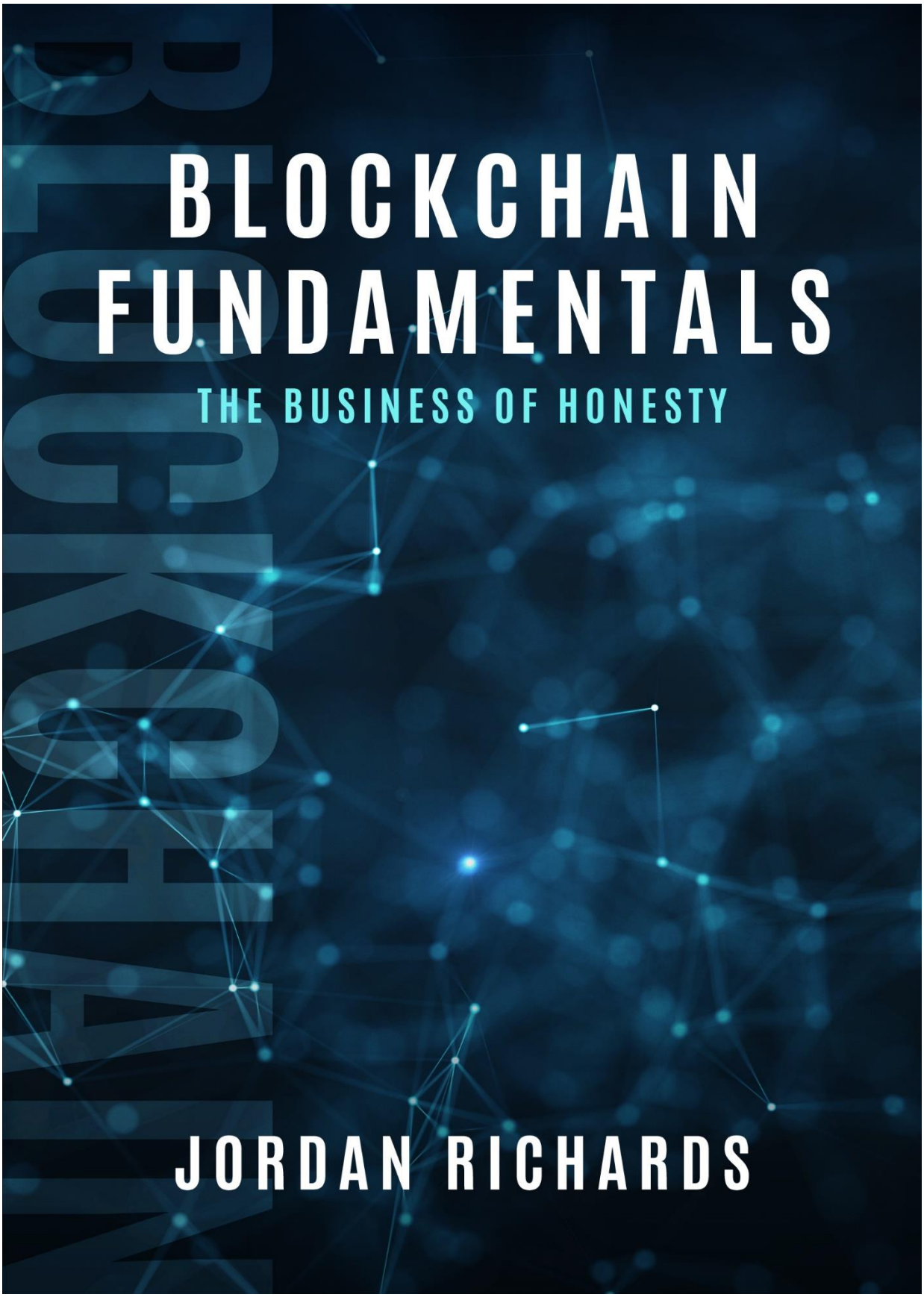

BLOCKCHAIN
BLOCKCHAIN
FUNDAMENTALS
THE BUSINESS OF HONESTY
JORDAN RICHARDS

Blockchain Fundamentals

The Business of Honesty

April 2019

By Jordan Richards

CONTENTS

PURPOSE OF THE BLOCKCHAIN FUNDAMENTALS

This Blockchain Fundamentals guide was written with foremost idea to share the basic understanding of Blockchain and how the core technology behind it works.

The core concepts are the buildings for what we do with the technology forwards.

As with many things in life, having to understand a concept, in an holistic and hopefully simplified way, without having the need for deep dive or cutting edge terminology can enable a business professional to make informed decisions.

This guide is both technical and historical. The purpose is to communicate both the key concepts, as was as the background as to why Blockchain and decentalized applications have arrived to resolve challenges and how this approach to technology will have a great impact on the digital future of our lives.

In many situations in my life, I have been hijacked into strategic meetings and had to make business decsions with consequences at short notice. A lot of the time, one does not get the fully deserved diliegence to weigh the strategy. One thing I do find, falling back on many years experience is how the new technology relates to the past, and how we can take an empircal approach to dealing with it. An overview or guide of the landscape is what I consder the first step of a long continous journey.

BLOCKCHAIN – A LESSON IN HISTORY

In November 2008, Satoshi Nakamoto presented his now famous Bitcoin Whitepaper, titled, A Peer-to-Peer Electronic Cash System to the tech world and in so doing effectively kick-started the bitcoin frenzy. Nine years later and bitcoin would take the world by storm, reaching a peak valuation of over $600 billion in December 2017.

At that point, no less than 24.5 million people were using the technology worldwide, and for every second up to 7 bitcoin transactions were completed.

However, while the general populace (fueled by the media frenzy) cast their glance on bitcoin, venture capitalists, developers, and financial industry leaders (the likes of JP Morgan) focused on its less famous cousin, Blockchain.

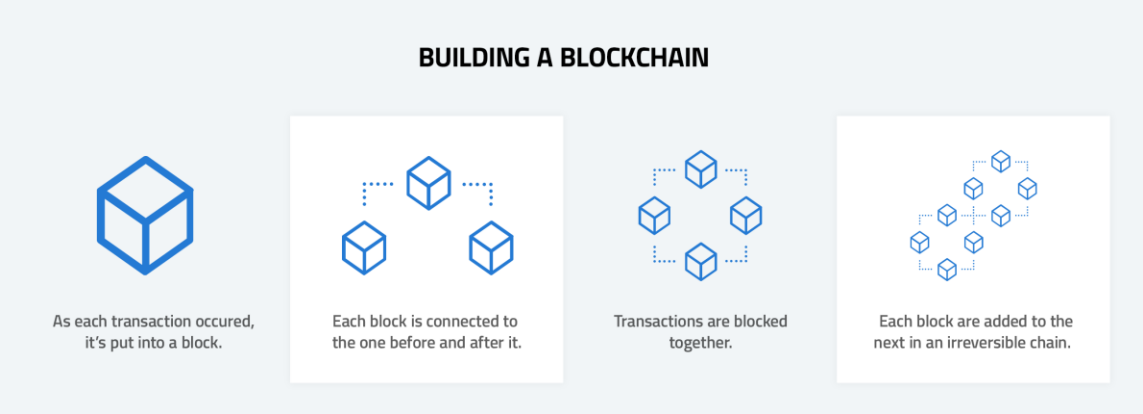
It was in fact, the technology on which bitcoin itself subsisted. Blockchain technology presented a revolutionary way of doing things (case example of which is bitcoin), and it was very much apparent that mastering it was essential to push the boundaries of innovation

WHAT EXACTLY IS BLOCKCHAIN?

In very plain terms, a blockchain is a distributed ledger of information hosted atop a self-sufficient and dynamic network of users (nodes). While this simple architecture sounds a bit rudimental (distributed ledger are not novel technologies), the way a blockchain handles the information stored on its network is what makes revolutionary

Blockchain leverages three core technologies; cryptography, digital signatures and Peer to peer (P2P) networks to retrieve and organize data sets efficiently.

By virtue of this, it creates a seamless and more importantly tamper-proof system of handling information.



P2P VERSUS CENTRAL SERVERS

The traditional protocol of information handling for today's digital world is the client-server architecture. Your favorite tech giants (Facebook, Twitter, PayPal) and virtually every other entity hosting data for user access on the internet use this framework. Here, when a client (user) requests for a

specific resource associated with a network, it is retrieved from a central database and depending on the network's privilege settings, delivered to the user.

The central database is conversely hosted on central servers, which are run and maintained by the parent organization.

This system does come with its attendant benefits. However, a case can be made that it is inefficient on several fronts - cue efficient P2P networks.

TRANSFERRING THE MANDATE TO USERS

Traditional client-server architectures typically rely on central servers for functioning. P2P networks like their names subtly let out are, on the other hand, run and managed by users of the network itself. These user computers are tagged 'peers,' and on the network, each peer with equal rights is regarded as a node.

Practically nodes can be any electronic device, the only requirement being that it should have a valid IP address and remain connected to the network (either via the internet, or local networks) on which the blockchain framework is hosted.

Think of nodes as the functional unit of a blockchain organized in a defined structural framework called a binary tree.

Together nodes in a binary tree integrate to form a composite computing network where specific rules segregate computing tasks to individual users who then execute these tasks as part of the higher functioning of the network. Data associated with the network is shared and stored amongst all constituting members.

Despite being tagged as equal, nodes typically perform different functions on a blockchain network, some of which require more computing power or privileges than the other.

As an example, full nodes run a full copy of the associated blockchain network at all times, whereas a lightweight client typically runs shortened versions of a network.

Both are however confined to implementing the same network consensus – the system of rules guiding how transactions and contracts should be executed on a blockchain.

INTERNET 3.0

This decentralized node based system of a blockchain confers on it several advantages, the reality of which has led to it being called the internet 3.0. Amongst other things, the absence of a centralized server makes a blockchain network wholly redundant and practically impermeable to network intrusions and hacking attempts.

Its' consensus system also absolves the need for any central governing authority. Users (nodes) have full control over the data shared on the network, and proposed decisions are reached via a network-wide vote involving each user.

This peer-to-peer system is what grants a blockchain network its 'integrity,' i.e., it's highly reliable and trusted architecture. It rids the normal transaction/task processing of the centralized server (middleman) and in so doing, drastically improves the speed at which transactions are processed.

SECURE TRANSMISSION OF DATA

Because transactions are processed by virtually any conforming network node and data is accessible (and modifiable) by users on the network, it is imperative for blockchain networks to run a secure system that prevents system-wide manipulation and hacks.

This is achieved through a mechanism that incorporates segments of cryptography, hashing technology, and digital signatures.

BLOCKCHAIN CRYPTOGRAPHY

Like was reiterated earlier on, data transmitted on a blockchain network is accessible and verifiable by all constituting users. However, these data sets (transactions and user contracts) are sent in an encrypted form. Only the sender and intended recipient(s) bear the necessary ‘keys’ to decrypt the data. Encryption of this sort on a blockchain network is implemented using the public key cryptography architecture (asymmetric cryptography)

Similar to conventional encryption protocols, data (transactions) transmitted via public key cryptography are encrypted from the sender and delivered throughput to the recipient. To decipher the transmitted data recipients must possess the public key used to encrypt the sent data in the first place.

This is usually the public key of the recipient. Public key cryptography, however, adds an additional layer of cryptic security to the mix by incorporating a private key.

Private keys are unique to users (node) and are practically impossible to decipher with current computing capabilities. Essentially, they function as an ‘originality stamp’ indicating that a partition of transmitted data is emanating from a particular node on the blockchain network.

Which is why they should be kept a secret, if a third party got hold of a user’s private key, he/she would be able to sign and verify transactions originating from the user’s account. If the private key was ever lost, then the account is rendered useless since the user won’t be able to sign transactions from his/her account.

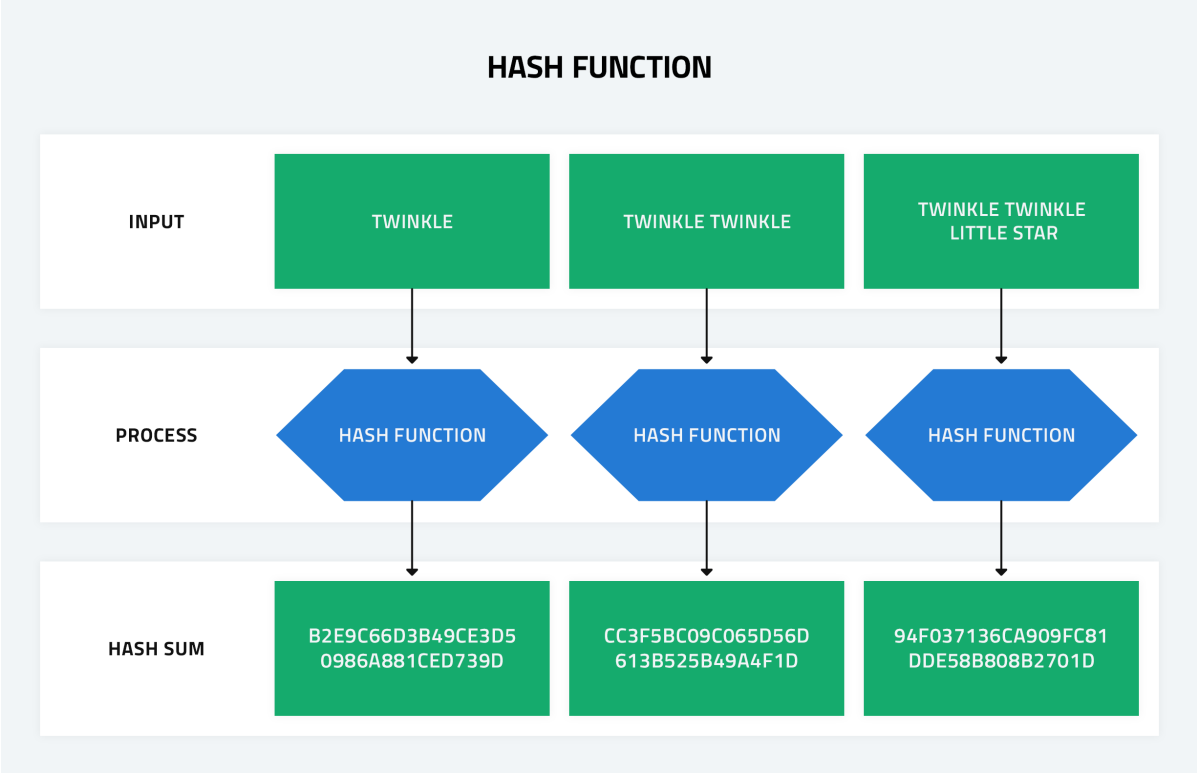
Consider this scenario

Say, User A of blockchain network X wants to send a block of encrypted data to user B. First, the information to be transferred is encrypted using a public key (sender or recipient). In addition to this encryption, a 'digital signature' fashioned out of the user A's private key is also stamped on the data to be transmitted and the resulting block of information subsequently broadcast on blockchain X.

Because user B possesses the public key used to encrypt the data, he/she can decipher its content. And the unique digital signature parsed with the sent information confirms that user A indeed sent it.

MECHANISM OF INFORMATION (DATA) TRANSFER – HASHING

Data transmitted on a blockchain network is usually repacked as another cryptic vesicle called a hash. The process of doing this is called hashing. Hashing maps variably sized data waiting to be incorporated on the blockchain network into a fixed and more maneuverable data set.



Note, however, that it differs considerably from traditional asymmetric cryptography used to secure data in transit on a blockchain. While it does confer additional security and redundancy, hashing was fundamentally designed to; create a dependable means of searching for information on a blockchain while offering tamper-proof protection to data stored on the network

Technically speaking a hash function (the mathematical compute that executes hashing) is a ‘reduce function’ programmed to derive a unique

output from a secondary input. Given an input value, it is relatively easy to obtain a hash output that is unique to the particular data set specified in the input. However, it is practically impossible to retrieve a hash input value from its output (N to 1 architecture).

Encryption and decryption functions, on the other hand, are map or N-to-N functions. Given the key, which was used to send the encrypted data, both the sender and receiver can accurately decipher the encoded data at both levels of the send chain.

Several algorithmic techniques are available to orchestrate hashing, Bitcoin, for instance, uses SHA-256. Regardless of the protocol, for a hash algorithm to be deemed effective, it has to meet the following requirements

First, hash functions must produce unique output hashes for differing input datasets, i.e., they must be collision free

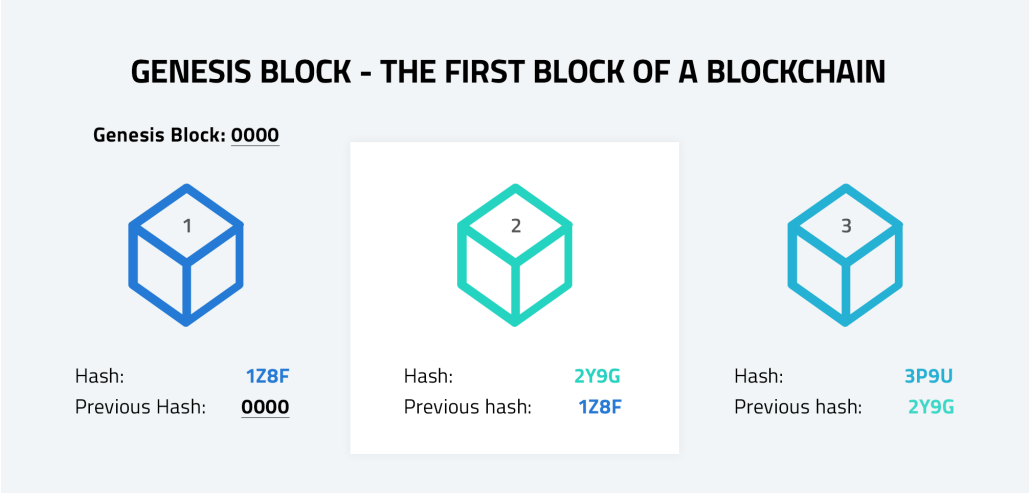
It must be consistent, ie. Hash functions must deliver these output hash for a particular input value at every instance

It must be spontaneous and fast to facilitate rapid information transfer and transaction processing on the blockchain network

And like we already reiterated it should be impossible to decipher the input value from the hash output.

The summation of these characteristics is what grants a blockchain its characteristic immutability and tamper-proof architecture. All data processed on a blockchain are hashed by default. New hashes for incoming data sets (transactions) are created by combining the original hash of the genesis block (initial blockchain segment), all preceding

hashes, and the hashes of incoming transactions. This results in a persistent line of continuity between all network verified transactions written on the blockchain.



As a result, any attempt to change even the minutest detail in one segment or block of the 'chain' results in an alteration of the overall hash signature of the network. Since all nodes on the network run a copy of the blockchain with an updated instance of the current hash signature, a deviation from this hash (as will happened if a node modified a blockchain segment) is immediately rejected by network-wide consensus and then discarded. Only datasets (transactions) tallying with predominant hash signature ever get to be integrated as a data block onto the (block) chain.

This system of hashing and perpetual linkage of all transactions stored on a blockchain, however, creates a complex array of data that needs to be handled efficiently if seamless blockchain operations are to be achieved. To do this blockchains use what is known as Data Structures

DATA STRUCTURES

On a blockchain network, data structures allow for the systemic storing of data in an orderly manner. Two hash functions contribute to making this possible – Pointers and linked lists. Pointers store addresses of other variables and linked list as you would imagine are comprised of individual blocks of data on the blockchain connected by pointers. It makes sense to think of the blockchain network as a chain of backlinking data blocks (each comprised of individual transactions), with preceding blocks referencing previous blocks (aka parent blocks) using a 'pointer' or 'previous block hash.'

Data (transactions) and their corresponding pointers are stored in blocks

For backlinked data to be integrated into the 'block-chain' network, they have to be first parsed into a block. Blocks are container-oriented data structures comprised of a header and sequence of interconnected data. Contained in the header is the metadata, actually three individual batches of metadata. The first metadata batch includes the pointer hash that references other blocks in a blockchain. It practically connects otherwise separate blocks on the blockchain. The second batch of metadata provides information about the mining competition via three subsegments; the nonce, timestamp, and difficulty.

A nonce is an arbitrary number used as a fluctuating counter in deriving a proof of work. Difficulty connotes the complexity of the Proof of Work algorithm designated to the block. And the timestamp indicates when the block was created.

Blocks in a blockchain are 'stacked' in a chronological manner

Picture a set of boxes stacked on top one another, and you get the idea. Older blocks come first before more recent blocks, and the first ever block to be created – the genesis block is conventionally regarded to be at block height zero. Block height can be used as an identifier for a particular block. However, it is not uncommon for several blocks to be on the same block height.

MERKLE TREES

By default, every block in a blockchain must contain a transaction, the first of which is a coinbase transaction. Coinbase or generation transactions are exclusively created by miners and under normal circumstances are entitled to the block reward. Along with other ‘normal’ transitions, coinbase transactions are integrated into formed blocks in a binary rawtransaction format. The blockchain algorithm then creates a ‘txid’ from the binary rawtransact of each transaction by hashing them. These txids form the building blocks of Merkle Trees

Put simply, Merkle trees are an efficient data structure system designed to store data on a blockchain in a secure and more importantly easily retrievable and verifiable manner. Merkle Trees work in this format.

First, hashed txid from individual transactions are paired and then re-hashed.

In the case where the number of transactions is an odd number, the lone hash is duplicated, paired with itself and then hashed.

Subsequent hash outputs from all transactions in a block are re-paired and again hashed

This continues until a single 32 bytes hash value called the Merkle root is derived.

The overall sequence of hashing, pairing and then rehashing to get a final hash value for the block resembles the structure of a tree. Indeed, hashes found on the first row of the sequence are tagged ‘leaves.’ Those

collectively grouped in the middle are ‘branches,’ and the final hash value as was already reiterated is the ‘root.’

Merkle Trees are essential for transaction verification

Because Merkle Trees compress the overall transaction history of a block into an easily retrievable string of hashes, it allows clients to verify transactions speedily. All that is needed is the Merkle root obtainable from the block header and a list of all contained hashes from a node.

eAs an example, suppose a client wanted to verify the inclusion of transaction M in a block with a Merkle root value of KLMNOPQ, the presence of KLNOPQ in the full list is indicative of the fact that transaction M is part of the block.

THE MECHANISM OF INTEGRATING BLOCKS ON A BLOCKCHAIN

On their own, blocks of data (transactions) existing on a node are precisely just that – 'blocks of data.' To become part of the blockchain network other nodes (peers) have to accept them as valid. The rules guiding how data is handled and subsequently integrated into a network is what is known as a consensus protocol. There are several kinds of consensus rules (algorithms) but among the bunch two stand out; a Proof of Work and Proof of Stake.

PROOF OF WORK

This consensus protocol mandates nodes (or a pool of nodes) to provide a 'proof' that they have 'worked' before they can integrate a block into the blockchain. The proof in this scenario is a hash derived from the block header containing the nonce (recall nonce). However, unlike your typical hash, the correct hash for a Proof of Work is extremely hard to generate, often requiring extensive computational resources. This is because there are set requirements (determined by the network) to which the correct value must corroborate with. Verifying the authenticity of the right hash presented by a node is however relatively easy. So, once a node is successful at solving for the hash (within the set requirements), and after announcing it to the network, other nodes can then verify the authenticity of the solution.

The first node to present the Proof of Work for a block is incentivized via a block reward (recall block reward), and since nodes actively compete to solve the hashing puzzle for block rewards, the process is called mining with the nodes themselves being miners. Note however that in reality,

nodes rarely mine singly. Instead, they do so as a group of nodes called a mining pool. Once over 50% of all nodes in the network validate the Proof of Work solution, a consensus is reached, and the block is integrated into the blockchain.

MINING

Depending on the hardware used to validate transaction (solve the block puzzle) mining can be grouped into

CPU Mining – using application-specific integrated circuits (ASICs), custom built to validate and integrate transactions via a Proof of Work consensus algorithm

GPU mining – in this case, the device used to validate transactions is a graphics card. GPU has the advantage of being ten folds faster than CPU mining.

Cloud mining – In cloud mining, miners rent cloud-based computational resources and use these to validate transactions

FPGA mining – FPGA is short for Field Programmable Gate Array. These are specialized computer chips sold as a 'blank' to miners who then program them to perform just the task of mining; They are highly efficient compared to the other mining options.

Aside from providing a clear-cut framework for integrating data onto the blockchain network the Proof of Work consensus protocol (as most other consensus protocols) solves another more implicative issue related to blockchains – that of Byzantine nodes. Byzantine nodes are peers attempting to intentionally falsify transactions, incorporate a compromised block, or send one transaction twice (in which case it is called a double spend) to the blockchain. Because of the computational power required to crack the Proof of Work puzzle, it is challenging for a rogue user to 'mine' a

falsified block ahead of the network (assumed to be composed of majorly well-meaning nodes).

That said if a rogue node manages to acquire significant hashing (computing) power, as is in a 51 percent attack, then it can successfully overrun the legitimate chain of blocks on the network. And in so doing it forces other nodes to accept the fraudulent blockchain as the valid copy. Again, this requires computational power of a very high magnitude, and the cost implication of undertaking such an attack typically offsets any projected benefits.

BYZANTINE FAULT TOLERANCE – THE CASE OF THE BYZANTINE GENERALS

Consider a group of armies each led by a commanding officer with an objective to attack a given enemy. Each commanding officer and his army are isolated from others, and yet all armies must attack simultaneously as a composite whole if the mission is to be successful. A simple solution would be to designate messengers to ferry messages and in so doing establish a correspondence between the commanding officers. This approach, however, comes with a risk.

The messenger can be intercepted by enemy troops, or a commanding general can intentionally send out contrived messages with a view of sabotaging his colleagues for personal interest. The possibility of a general to propagate falsified information and have other generals regard it as truth (which leads to mission failure) is referred to as the Byzantine Generals problem.

The scenario described above is also applicable to blockchain networks. The generals, in this case, are individual nodes, and the information that

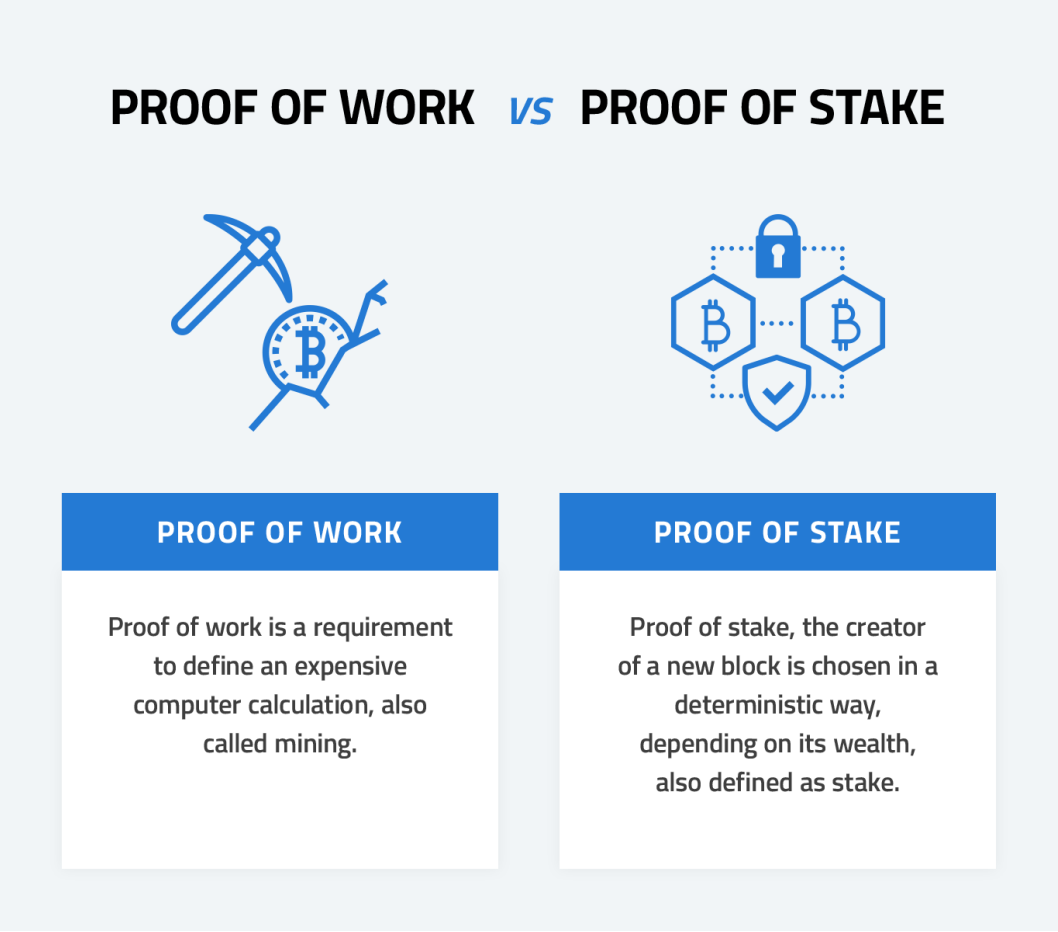
needs to be transmitted is a valid copy of the blockchain itself since there's no central authority permanently hosting a ratified copy.

However, unlike the case of the Byzantine generals, the 'mission' of nodes on a blockchain network is to ensure that only the legitimate blockchain and its corresponding database of transactions ever get adopted on the network.

The ability of a blockchain to resist attempted propagation (and possible adoption) of illegitimate copies of a blockchain is what is referred to as Byzantine fault tolerance. And like we've already reiterated a Proof of Work consensus protocol is one way to achieve this tolerance.

PROOF OF STAKE CONSENSUS PROTOCOL

The first cryptocurrency to field a Proof of Stake consensus protocol was Peercoin in 2012. Here, the node that will eventually create a block, in this case, called a forger, is determined at random from a group of forgers based on the 'stake' (amount of assets) they hold on the blockchain. So while a Proof of Work blockchain assigns this right based on the computational capability of a node, a Proof of Stake basis it on how much a node 'invests' in the network. Additionally, a Proof of Stake architecture does not usually hand a full block reward as is with POW. Instead, forgers collect the transaction fees associated with the forged block as an incentive for 'staking.'



Proof of Stake blockchains enforces its fraud-proof architecture on the premise that forgers will only stake on legitimate transactions. As you would expect this is not always true, nodes with high enough assets can simultaneously stake on the valid copy of a blockchain and a falsified version. If either goes through (with a preference for the contrived blockchain), there is a guarantee that the node will make a profit. This scenario is termed a ‘nothing at stake’ problem. In Proof of work architectures, an attack of this sort is discouraged by the sheer computational power (which translate to financial costs) required to implement it. In the case of a Proof of Stake, there is no comeuppance, since the node will still have its stake and profits recovered either way.

Several modifications to the traditional Proof of Work system have been effected to combat this issue, notable amongst which is the Casper protocol. Basically, these mods are designed to penalize peers who go on to function as byzantine nodes.

Proof of Stake is the perceived future of blockchain technologies

Despite its inherent flaws, the Proof of Stake architecture (or its modifications) is still considered by many to be the ideal blockchain framework. Why? Amongst other things, its cousin, the Proof of Work consensus protocol requires an astronomic amount of resources to operate.

It is estimated that one transaction on the bitcoin blockchain expends as much energy to execute as 29 homes in the United States and on the average both Bitcoin Cash and Bitcoin cost $18 million to run every day.

Proof of Stake comes as the panacea to this flagrant ‘waste’ of resources. By shelving computational mining, it makes a blockchain more effective and resource friendly to operate. More so, processing transactions on a Proof of Stake blockchain is considerably faster.

DELEGATED PROOF OF STAKE

Delegated Proof is a modification of a Proof of Stake consensus protocol. Here, rather than assign the forging right at random, the blockchain ‘delegates’ which node will form the next block from a specific pool of nodes in the network. These nodes (hitherto referred to as block producers) are voted into the block producing pool by other users who possess a voting power equivalent to their asset base on the network.

Block producers are also referred to as ’witnesses’ since in practice they witness the formation of blocks for the blockchain community that votes them into power.

The number of block producers is capped to a certain value. In contrast to a Proof of Stake consensus protocol, they need not hold a high stake in the blockchain. Rather, it is the stake of voters involved in the voting process that counts in determining which nodes eventually become block producers.

Voting in a Delegated Proof of Stake consensus protocol is a continuous process, and each block producer remains at risk of being voted out. This dynamism functions as an autoregulatory mechanism that keeps block producers in check ensuring that they do not compromise the network for personal gains. In the case where a block producer violates the trust of the community, he/she is simply voted out of the witness pool. Voters can also

vote for a select team of ‘delegates’ charged with managing and initiating policy changes in the network.

Note, however, that they cannot implement network-wide changes on their own. Proposed changes or updates survive a voting round involving all users of the blockchain network.

In addition to the advantages a standard Proof of Stake consensus protocol has over Proof of Work algorithms, Delegated Proof of Stake bundle a slew of other beneficial traits.

For one, it is more secure than conventional Proof of Stake algorithms since users have the power to moderate the activities of block producers actively. They are also faster than the former two hashing mechanisms, requiring only a fraction of the time it would take them to process and complete a transaction on the network.

WHY BLOCKCHAIN?

A decentralized network for the win

While centralization does come with its attendant benefits, there's no arguing the fact that it bundles a slew of arguably unnecessary complications and complexities. Bockchains debut as the panacea to the numerous shortcomings of centralized systems. Its decentralized network of nodes and seamless orchestration of self-governance shave off exorbitant administration costs. Decision making is streamlined and more importantly always in the best of end users (the community) as opposed to benefitting administrative authority in the case of centralized architectures.

This decentralized architecture also provides for redundant encryption and 100 percent data protection. In a world where data farming and eventual marketing has become much more of a norm than taboo, the inherent transparency and mutual trust of blockchains cannot be overemphasized. Data hosted on blockchains are immutably imprinted in such a way that they are irretrievable by third parties (there's no central authority to attempt this in the first place).

IT'S SECURE

Concurrent with technology's fast-paced advancement has been a lighting upgrade in the methods of collecting, analyzing, storing and retrieving data. Same cannot be however said for data security.

Hacks and intrusion attempts are still a mainstay in today's tech ecosphere and with every other, week news of successful hack attempts on major organizations surfaces mainstream media. Of course, these hacks come with their dose of severe consequences. In August 2013 for instance,

Yahoo servers were breached resulting in the leak of sensitive information belonging to no less than 3 billion users.

What makes modern computing systems so vulnerable to hacks? The answer to that question can be traced to how computers handle data in this day and age, i.e., the centralized server-end user architecture. If a central server was ever compromised, then all data hosted on its network will be compromised as well. Decentralization on a blockchain network makes such a hack practically impossible. In fact, blockchains cannot be hacked since they (blockchains) do not have a single point of failure. They are thoroughly redundant as data is shared in an encrypted format to all constituting nodes in the network. This redundancy is what typifies the blockchain secure architecture, and it is one of the major reasons why public blockchains like Bitcoin are typically more secure than private blockchains (with fewer nodes).

IT'S TRUSTLESS

In today's business world, trust is central to completing transactions and striking business deals. Consumers rely on the perceived good name of sellers to pay before service is delivered, mutually exclusive business parties conduct business deals from opposing parts of the globe, financial institutions store valuable assets for customers on the premise that it will be retrievable when needed.

While this system continues to serve the 21st-century business world, there's no arguing the fact that a growing number of the world's populace are subject to the not so pleasant consequence of its many inherent flaws. When a single entity wields too much power by virtue of the trust it has,

there's always a tendency for it to overstretch the limits of this power. Incidences of banks imposing obscene rules and specifications on its clients and not unheard of, case in point are PayPal's flagrant sanctions and often overbearing rules and regulations. Blockchains get rid of this centralized trust putting the power to orchestrate the network in the hands of the individual nodes making up the system.

With blockchains, there is no central authority mediating the affairs of the community. The network itself, through a consensus protocol, achieves governance independently and instantaneously. The benefits of this revolutionary approach are far-reaching. Not only do decision making, rules and regulations always align in favor of the community, the system also provides an added sheet of protection since no central trusted authority can be manipulated into compromising the network.

When there's a need to undertake a transaction between two parties, both can create a fulfillment script otherwise known as a smart contract to execute only when specific conditions are met.

Put simply; this script ensures every participant gets his/her end of the deal as specified in the contract after set conditions are met. There's no need for any trusted authority as the blockchain itself serves this function via a trustless native contract.

USE CASES

BLOCKCHAIN AND CRYPTOCURRENCIES

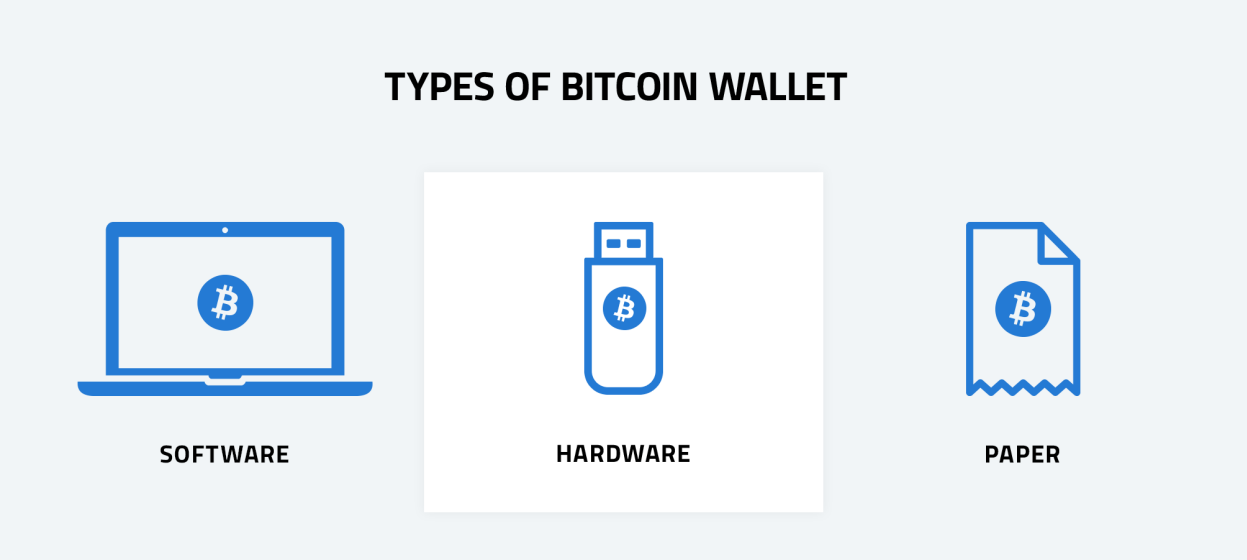
Through the course of this write-up, we have been talking about datasets (transactions) and how they are created, transmitted, and stored on the blockchain. When these datasets (in their fundamental state) serve as a store of value, that is both tradeable and fungible; then they are hitherto classified as cryptocurrencies. Crypto; indicating the redundant cryptographic protocols used to encrypt these datasets on the blockchain and currency; showing that in this case, these data sets have a real-world enforceable value.

The system as we have already reiterated is self-sufficient, and although the name cryptocurrency suggests a monetary store of value (which is the case with most cryptocurrencies today), it is important to note that other ‘valuables’ as is a contract between two parties can be transmitted and stored by a cryptocurrency

Satoshi Nakamoto’s ‘digital cash’ or Bitcoin was the first fully-fledged cryptocurrency. And tallying with its real-world financial use case, Bitcoin, like all other cryptocurrencies having a financial use case is called a cryptocurrency coin. All other cryptocurrencies including those originally derived from the Bitcoin (Proof of Work) blockchain and those fielding a Proof of Stake blockchain are with reference to Bitcoin called Alternative cryptocurrency coins or Altcoins for short.

STORING CRYPTOCURRENCIES

Supposing a user wanted to undertake a transaction, how does he or she interface with the blockchain network to provide a valid public-private key pair for transaction validation? For that, they'll be needing a cryptocurrency wallet.



A cryptocurrency wallet is a device, could be a paper, hardware, software or even an online service that stores a user's private-public key details along with other important data necessary for processing transactions on a blockchain.

Aside from hosting user data, wallets also serve as a virtual interface that allows users to interact with their cryptocurrency account. Wallets don't, however, hold any physical currency, even though their name suggests so.

What they do hold are records made to and originating from the hash address to which they are linked. Think of them as online bank accounts rather than actual wallets.

Cryptocurrency wallets come in different forms, broadly speaking, they can be grouped into three; categories, software, hardware or paper wallets

SOFTWARE WALLETS

Depending on where the software bearing the private-public key combo is installed, software wallets could be either mobile, online or desktop. Mobile and desktop wallets are essentially mobile applications running on a desktop or mobile platform. Online wallets are hosted on the cloud. The three options provide relatively easy access to cryptocurrency assets as well as convenient usage. Their online or 'hot' nature, however, predisposes them to hacks and intrusion attempts

HARDWARE

While software wallets store all essential data on a software program hosted on an online device, hardware wallets store it on a hardware device usually without a direct connection to the internet. This could be a USB stick or hard drive. Transactions can be processed natively on the hardware device without connecting to the internet, although they need to be connected at one point to update the network on transactions made. Their offline state confers added security to a user's private-public key combo

PAPER WALLETS

In terms of security, paper wallets are considered to be the gold standard. They are physical copies of a user's private-public key combo printed on a piece of paper. They are not digital or stored on any 'hackable' device. Like Hardware wallets they are not perpetually connected to the internet and as

such are referred to as ‘cold’ wallets. Transactions are made when a user manually copies them into a software interface or scans the accompanying QR code.

TOKENIZED CRYPTOCURRENCY

Tokens are very similar to cryptocurrency coins. However, unlike the latter, they do not necessarily denote financial value. Instead, they are primarily digital assets/utilities that can perform a slew of functions on the blockchain network.

They could be used to store valuable data, act as a security layer, or can be even traded directly; tokens are essentially specialized scripts added to a blockchain. Consequently, several tokens can be integrated into a single blockchain, each with specific functions.

Cryptocurrency coins, on the other hand, are integral components of their respective blockchains. They are unique to their blockchains and function as the ‘digital currency’ on which the ecosystem subsists on. Tokens can be broadly grouped into;

NATIVE

Native or intrinsic tokens are formed utilities directly integrated into the overall architecture of a blockchain network. They are central to the operations of a blockchain and typically function as a means of incentivizing nodes which participate in specific aspects of network governance. Native tokens do not have any real world backing; they are simply ‘created’ based on the existing architecture of the blockchain network. ETH and XRP are all native tokens

ASSET-BASED TOKENS

Asset-based tokens are backed by a real-world entity and unlike native tokens are not an integral component of their blockchain networks, i.e., the

blockchain can operate with or without the asset-based token. When an asset-backed token is issued, a corresponding real-world item matching the value indicated by the token must be deposited. In this case, the token is functioning as a representative of a real-world item of value on the blockchain network, and as such, carries the same value as does the real world entity on the blockchain network.

THE ETHEREUM ECOSYSTEM

Ethereum is a decentralized blockchain network based on a Proof of Work consensus protocol. Like Bitcoin, it has an integral cryptocurrency coin - Ether used to facilitate transactions on the network. Unlike Bitcoin, however, Ethereum's use case is not limited to just facilitating transactions. Created on 30th July 2015, Ethereum was an upgrade of the Bitcoin blockchain appropriately dubbed blockchain 2.0. It featured a thoroughly robust platform for executing smart contracts and hosting decentralized applications.

Think of the Ethereum blockchain as a singular computing entity – the Ethereum Virtual Machine comprised of composite nodes using Ether as fuel for hosting DAPPS and executing smart contracts. The decentralized application could be anything, and Ethereum Virtual Machine boosted by its decentralized nature proffers scalability and performance.

Users can claim ownership or utilize the services of a DAPP by purchasing tokens. In the case of Ethereum, this is done using Ether.

Smart contracts, on the other hand, are self-executing 'contracts' between two or more parties. It is basically a transactional mechanism that allows for individual parties and their assets to enter a mutual contractual agreement involving the deposit of such assets, fulfillment of set conditions and then eventual redistribution of all held assets based on the premeditated parameters.

Put simply, they allow for conditional fulfillment of specified terms in a contract situation. Smart contracts are not necessarily as smart as their name denotes. In fact, you can consider the name a misnomer since they

only execute the lines of code embedded in their script. Execution is however automatic, and once specific conditions are set, they must be met before contract fulfillment can be complete. In essence, smart contracts foster the verification, compliance to and enforcement of transactional conditions and agreements in a quasi-escrow like manner.

As an example, say user A wants to buy a phone from user B who lives in another country. Both users can create a smart contract that first specifies for an initial amount (the phone's worth) to be deposited. Once the phone is shipped, and user B validates receipt, the smart contract automatically transfers the sum held in escrow to user A.

As is apparent from this example, smart contracts formalize the liaison between two transacting parties. It defines exactly what is to be expected from all participants in an agreement and as such can be hitherto classified as a legal document when all involved parties consent to its provisions and specifications.

Through this mechanism smart contracts provision a fluid system of going about contractual transactions that is much more superior to traditional contract law. While the latter requires exorbitant fees, the presence of a legal counsel, and manual enforcement of set requirements, smart contracts self-verify, execute independently and are practically tamper-proof.

DECENTRALIZED APPLICATIONS

Very few computing systems available today can rival the computing power and extent of established blockchain networks. This is because unlike the former, blockchains pull in computing resources from a multitude of user nodes domiciled in virtually every region of the world.

More importantly, however, this is computing power available at a fraction of the cost of conventional systems. Decentralized applications or DApps leverage on this immense computing power to host applications and programs natively on the blockchain.

A DApp is a smart contract, connecting blockchain users to the architecture/database level of a blockchain. It's comparable to traditional web or software applications, which in their case use an application programming interface or API to link user, server and database. Decentralized applications can be practically anything; a full-scale MMORPG, a next level virtual reality world, a simple application or secure banking portal, you name it.

They open up a real world of possibilities for blockchain technologies and as we shall now see many of these have already been adopted for real world usage.

IN GOVERNANCE

VOTING

As it is with data security, the world as a whole still has to contend with a lump sum of electoral malfeasance resulting from the limitations of current voting technologies. Blockchains debuts as a novel framework that can be

used to forestall the many shortcomings of current electoral processes. Encryption and cryptography on a blockchain network totally address concerns of false or double votes, and because the system is decentralized, fears of electoral manipulation are concurrently put to bed. For countries where corruption is mainstay blockchains present an efficient, cost-effective and more importantly, infallible means of fostering genuine democracy.

NOTARIZATION

Notarization or the act of vetoing legal document signings is another segment of governance that looks set to benefit from the efficiencies of blockchain technology.

Traditional notary services utilize written documents or centralized databases to create timestamps of important events like birth/death dates, certifications, or transfer of ownership rights/titles.

This characterization, however, makes the notarization process prone to mistakes, data losses and even breaches (since they house confidential data).

Blockchain notary services, on the other hand, are set up to create indelible records that are not only hack-free but also tamper proof and devoid of the error-prone categorization of traditional notary process.

A significant handful of governments including that of Sweden and Georgia have already set up instances of blockchains functioning as notary module.

IN BANKING

The financial services sector was the first to fully exploit the nascent capabilities of blockchain technologies to critical acclaim. Occurring simultaneously with the rise of digital currency derivatives of blockchains like Bitcoin and Ethereum was a massive global sensitization on the efficiency and effectiveness of blockchain technologies in remediating real-world problems.

This showcase was fueled by the success blockchains had in circumventing the many limitations of the financial industry. For one, blockchains (as the backbone of cryptocurrency) effectively sidestepped the often ludicrous transaction fees associated with banks and other monetary service providers.

Unsurprisingly this led to a seismic shift from fiat currencies being the defacto means of completing transactions to a cryptocurrency driven financial ecosphere. In 2017, over $2 billion worth of transactions were completed per day on the Bitcoin blockchain.

But aside from the revolution of how entities undertake transactions, blockchain technology is pioneering an even more impactful cultural shift in the way traditional banking institutions provide and handle financial services.

Just a year ago, The Barclays group snatched global headlines when it adopted the now established cryptographic and transparency factions of blockchain technology.

As we've already reiterated both these components are second to none when it comes to providing security, redundancy, and transparency in

digital systems and it's only a matter of time before other leading fin services firms follow suit.

From another perspective, derivatives of the blockchain, most notably Bitcoin have assumed a super financial store of value status. This being on the backdrop of its meteoric rise in overall market valuation within the last decade. Bitcoin was at a point more valuable than gold. Expectedly leading securities and trading firms like Goldman Sachs, CME Group, CBOE, and Cantor Fitzgerald began listing Bitcoin futures and securities on their trading platforms.

HEALTHCARE SERVICES

One limitation that has so far plagued the global healthcare system is the confinement of medical records and researches to individual factions of the industry. This isolation has to a great extent fostered the development of so-called knowledge silos to the detriment of progression in the sector. For medical practices to evolve and improve, researches and records need to integrate with each other to develop a concise picture of the industry's challenges and possible solutions.

The blockchain with its latent interconnectivity amongst users provides the perfect platform to facilitate this. More so, its robust architecture provides a computing platform that is well and truly capable of handling the computing needs of the health industry's dive into deep learning and AI as a tool for improving diagnosis.

THE INTERNET OF THINGS

Like the healthcare industry, computing needs for the rapidly budding IoT ecosystem exceeds the provisions of conventional computing systems. The

average human creates approximately one gigabyte of data every day. Combine this with information coming from other sources like airport logs, weather forecast, etc. and it's easy to picture the true extent of IoT's needs.

Blockchains provide an efficient, optimized, downtime-free and more importantly scalable means of combing through this data to derive insights. Its node-node architecture as opposed to a client (node)-server configuration also speeds up data sharing and retrieval rates while shaving of the network latency period commonplace with the latter.

By 2025, it is expected that no less than 80 billion devices will be connected globally on a macro level. Organizing and administrating such a network will without a doubt be cumbersome for existing administrative protocols.

Decentralization, consensus algorithms, and other blockchain native features can be leveraged to prosper smooth and scalable network administration.

ACKNOWLEDGEMENTS

To my colleagues all across the Information Technology and Energy Sector, but most specifically my good friend and colleague Jason Ensor.

I would also like to thank my well respected colleague Mohammed Harthy for his encouragement and sharing his wealth of information on Robotics (RPA) and Machine Learning.

Thanks to all of the entrepreneurs and groups who have inspired me over the years.

BIOGRAPHY

Best known for his pragmatic, hands-on approach, Jordan Richards has continued to deliver and implement IT solutions to the real-world International experience for over 25 years. A versatile and well-grounded professional, he understands that technology is a tool for a solution to solving business problems, not the solution itself. With such a revolutionary mindset, he has worked collaboratively with business cutting across a broad range of industries, solving problems and finding innovative ways to get results on time.

His services are widely sought-after by industry-leaders, companies, and organizations who need a professional with considerable experience to get things working for them. Furthermore, Jordan excels in technologically implementing enterprise Knowledge Management solutions, Document and Information Management confidentiality implementations.

In the light of showcasing expertise, Jordan has worked directly with the business managing teams of developers and support staff across international Oil and Gas companies.

Jordan is available to discuss this or other points and are available on linkedin: https://www.linkedin.com/in/jordanrichards/