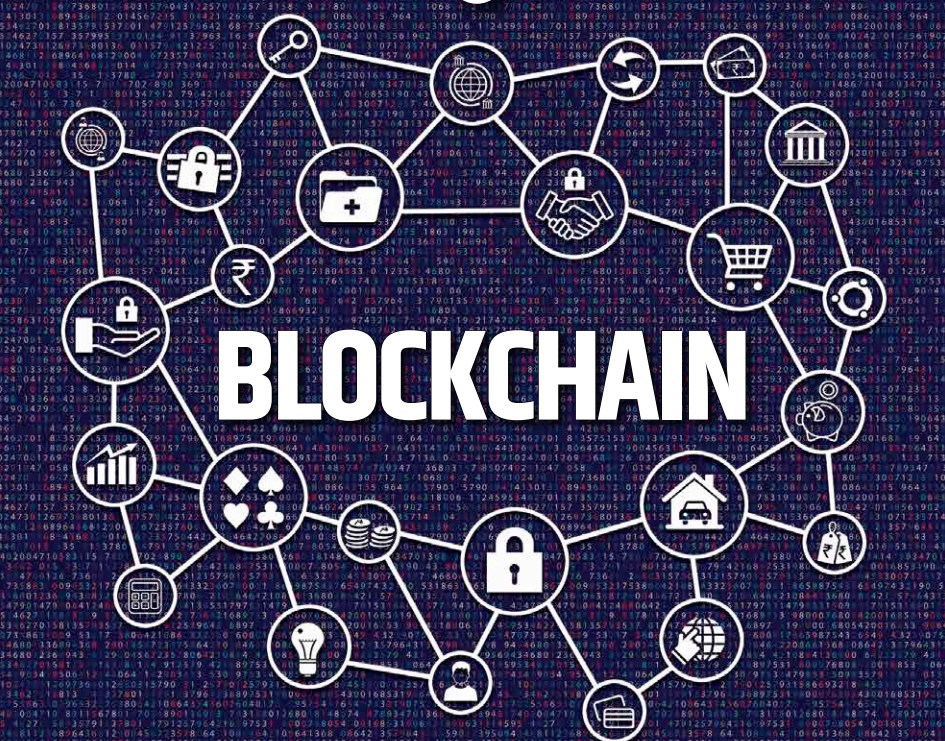
VOLUME 13 | ISSUE 02 | FEBRUARY 2018

digit FastTrack

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY

to



BLOCKCHAIN

- What is Blockchain?
- History of Blockchain
- Understanding how it works.
- Blockchain variants
- Blockchain application : Financial Services
- Blockchain application : Insurance
- Blockchain application : Government
- Blockchain application : Supply chain management
- Blockchain application : Healthcare
- Blockchain application : IoT
- Blockchain criticisms

A 9.9 Media Publication

Free With Digit February 2018

www.digit.in/forum

Join the forum to express your views and resolve your differences in a more civilised way.

digit.in FORUM

Post your queries and get instant answers to all your technology related questions

One of the most active **online technology forums** not only in India but world-wide

JOIN NOW

digit.in

BLOCKCHAIN

powered by

digit

YOUR TECHNOLOGY NAVIGATOR

CHAPTERS

BLOCKCHAIN
FEBRUARY 2018

06 PAGE
Blockchain
The newest buzzword on the block has the entire technology industry excited. Here's an introduction to blockchain.

12 PAGE
History of blockchain
Blockchain isn't just about Bitcoin, there's more to it than just the technology behind the cryptocurrency.

19 PAGE
Understanding blockchain
If the primer on blockchain wasn't enough, then here's an indepth understanding of how blockchain works.

28 PAGE
Blockchain variants
Even as a single entity, blockchains are enough confusing. But the fact that there are different kinds of them... Well, we've got your back.

37 PAGE
Blockchain applications in financial services
The implications of blockchain technology in the financial services are far reaching and can potentially turn the entire industry on its head.

CREDITS
The people behind this book

EDITORIAL
Executive Editor
Robert Sovereign-Smith

Asst. Technical Editor
Mithun Mohandas

Contributing Writers
Abhimanyu Mehta
Rohan Shrivastava
Sahil Dawka
Sanket Nikte
Swapnil Rastogi
Tabitha Thomas

DESIGN
Sr. Art Director
Anil VK

Visualiser
Baiju NV

digit.in

47 PAGE
Blockchain applications in insurance
The mammoth insurance sector known for its resilience to change is susceptible to high impact with the advent of blockchain technology.

56 PAGE
Blockchain application in governments
A Government, being the biggest and most influential service provider, can use the blockchain technology in a plethora of ways ushering in a new era of transparent and trusted governance.

65 PAGE
Blockchain and supply chain management
Organized supply chain management has been around since the 50s. Can Blockchain be the answer to solve its shortcomings?

72 PAGE
Blockchain applications in healthcare
Probably the most crucial application of the technology, it has the potential to literally save lives.

80 PAGE
Blockchain & the internet of things
Internet of Things is an up and coming avenue. It provides unthinkable possibilities for the future. However, it comes with its own share of problems and restrictions.

88 PAGE
Criticisms of blockchain
Not all is hunky dory, there is always a flip side to every coin. Let's understand the faults in the stars of blockchain.

February 2018
Free with Digit. If you have paid to buy this Fast Track from any source other than 9.9 Mediaworx Pvt. Ltd., please write to editor@digit.in with details

Custom publishing
If you want us to create a customised Fast Track for you in order to demystify technology for your community, employees or students contact editor@digit.in

e-mail

COVER DESIGN: PETERSON PJ

Blockchain - the most disruptive technology of the decade

It's the latest buzzword in the world today - Blockchain. You'd think that after all the dismissive articles written by Bitcoin critics, blockchain technology might have died out but no, that's not happening anytime soon. Bitcoin, the cryptocurrency that pioneered blockchain technology is undergoing a tumultuous ride as financial regulators and governments start scrutinising it in greater detail. However, the underlying blockchain technology has been picked up by practically every major technology and finance company on the planet. After all, it's a ledger system that has an enormous potential to save infrastructure costs while providing secure and accurate transactions.

In fact, if you were to build a startup using blockchain in a viable manner, then there's a good likelihood that it'll get funded. What's even better is that the average funding for such startups is a minimum of $1 million. That was for last year i.e. 2017. 2018 is poised to see an even bigger growth as practical applications of Bitcoin technology enter mainstream markets. Ripple, a real-time gross settlement system, currency exchange and remittance network by a company of the same name is already working with 30 percent of the major banking institutions around the world.

Blockchain, like most new technologies needs to be examined closely. Since it has only been around for a short period of time, we haven't been exposed to ways that blockchain can be misused. Or if the existing security aspects of blockchain can be easily subverted. Which is why some companies

are still reluctant to take the plunge. We aren't saying that we've figured everything out, however, if you were in the dark about this new piece of technology, then this FastTrack to Blockchain should cover all the basics. We've covered Bitcoin in much detail back when the cryptocurrency was in its infancy, you can read the same here (*http://dgit.in/FTtoBitcoin).*

Aside from the concept of blockchain, we also explore the different variants that have sprouted, some of which have already been adopted by companies in lieu of traditional centralised ledger systems. As against variations to the technology, we've covered the different domains where blockchain technology is being applied, and has the potential to be applied. We must say that we were pleasantly surprised by the far reaching potential that this technology has brought to fore. We hope that you too shall discover all of that and more as you read through this FastTrack. Lastly, we've even laid out some of the strongest criticisms of blockchain technology in its current form.

Like always, we're all ears to what you have to say. If you liked this FastTrack or hated it, do drop us a mail at *editor@digit.in* and let us know what we could have done better.

Blockchain

The newest buzzword on the block has the entire technology industry excited. Here's an introduction to blockchain.

Blockchain is a not really an unknown term these days considering the growing excitement around cryptocurrencies.

When we talk about blockchain, some of you might relate it to Bitcoin. But it is important to understand that Bitcoin and blockchain aren't the same thing, infact, blockchain is a technology behind the very famous cryptocurrency, Bitcoin.

But is that all there is to blockchain?

The answer to this is, No. The potential use of blockchain is far beyond just digital currencies.

So what exactly is blockchain? What is so exciting about this technology that everyone is curious to explore it?

What is blockchain?

In Wikipedia, blockchain is defined as a continuously growing lists of blocks that are linked and secured using cryptography. Each of these blocks contains a hash pointer, a link to the previous block, transaction data and a timestamp. It is an open, distributed ledger that records transaction details between two parties efficiently in a verifiable and permanent way.

Blockchain is basically a persistent, transparent, public, append only ledger.

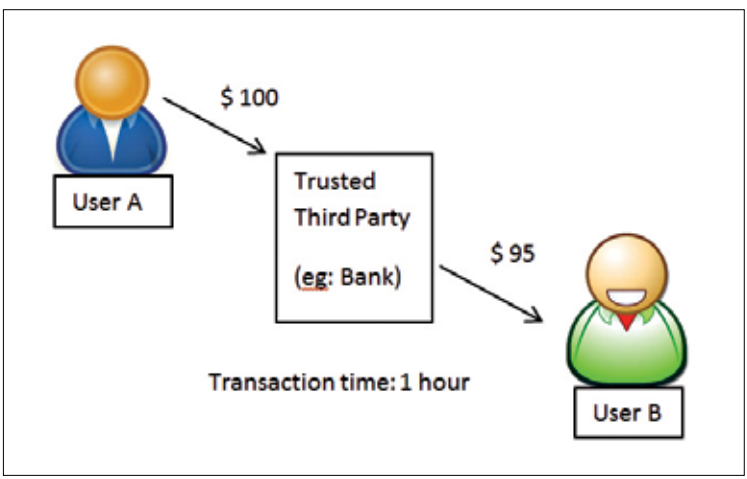
It is a system that you can add data to without changing any previous data within it. The data added previously, remains intact. It does this through a mechanism for creating consensus between scattered or distributed parties that do not need to trust each other, but trust the mechanism by which their consensus has arrived at.

Currently, if we need to make a transaction, most of us use a trusted middle party which is usually a bank.

Let's take an example where user A needs to transfer some amount to user B. User A uses a trusted third middle party to do the transfer successfully to user B. The trusted middle party will make the transfer successfully, but will however charge a fee, and the transaction time would be an hour or so.

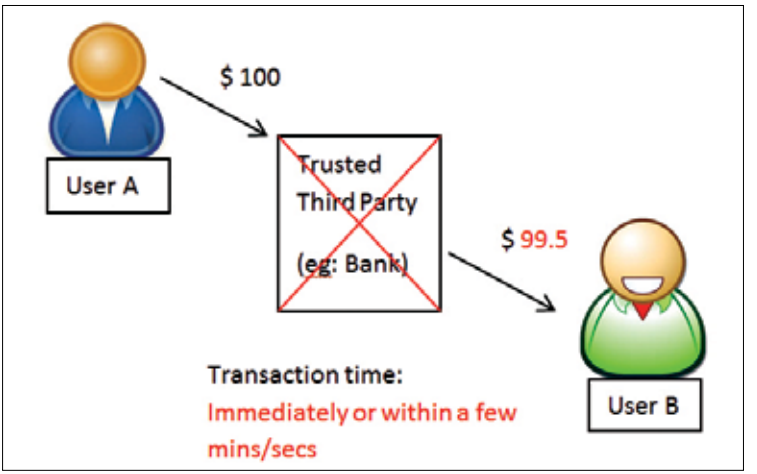
Blockchain attempts to solve 3 things here:

1. To transfer money without the trusted middle party, thereby enabling people to connect directly with each other.



Traditional banking method

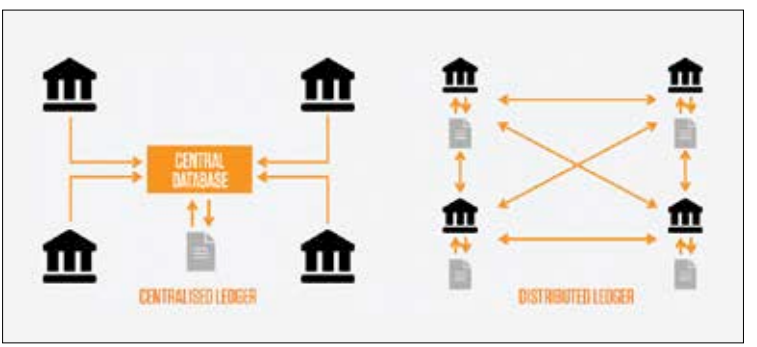
2. To transfer money faster than the traditional system. In fact, it would be transferred instantly or within a few minutes/seconds.
3. Making the costs of transferring cheaper than what the trusted middle party collects.



What blockchain aims to do

Blockchain works on the fundamental ideas of distributed, and open ledgers.

Whenever a new block is added to the blockchain, it is shared with each node on the peer-to-peer network and every node verifies the authenticity of the block. They then arrive at a consensus, post which each node would add this block to their blockchain. Since it is decentralized, we can say that



Differences between centralised and decentralised systems

there is no central hub where the transaction data is stored. All details of the transaction in the blockchain is retained on the entire network, thereby ensuring the history is not in control of one person. This ensures complete security.

In case of a traditional system, we would have a trusted middle party ensuring the authenticity of data, just like a centralised ledger.

Therefore, we can say that blockchain allows for faster, safer and cheaper transfer of money as compared to traditional systems.

Basic idea of how it works:

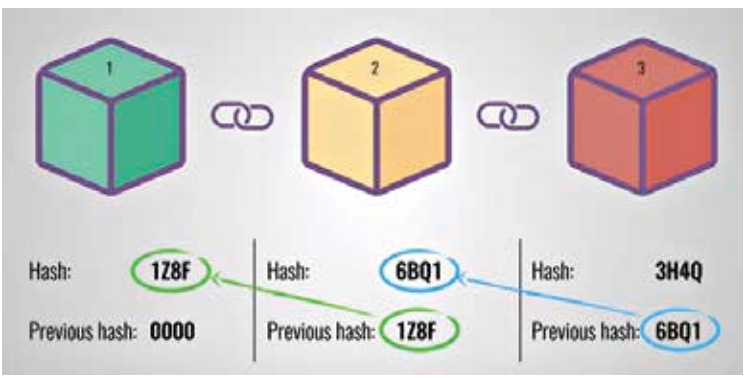
Blockchain as the name suggest, is basically a chain of blocks that contains information.

Each block contains some data, the hash of the block and the hash of the previous block.

The data that is stored inside the block, depends on the type of blockchain. For example, a bitcoin blockchain stores the details about transactions like the sender, receiver and the amount of coins.

A block also has a Hash. You can compare a hash to a fingerprint. It identifies a block and all of its contents and it's always unique, just like a fingerprint. Once a block is created, its hash is being calculated. Changing something inside the block will cause the hash to change. If the fingerprint of the block changes, it is no longer is the same block.

The third element inside each block is the hash of the previous block. This creates a chain of blocks effectively and it is this technique that makes blockchain so secure.



A simple blockchain

In the image below, we have a chain of three blocks. Each block has a hash, and the hash of the previous block. Block 3 points to block 2 and block 2 in turn points to block 1.

The first block is called the Genesis block as it does not point to any other block being the first one.

Now, let's say someone tampered with the second block. This would cause the hash of the second block to change as well. In turn, this would make block 3 and all the following blocks invalid, because they no longer store a valid hash of the previous block. So making some change in a single block will make all following blocks invalid.

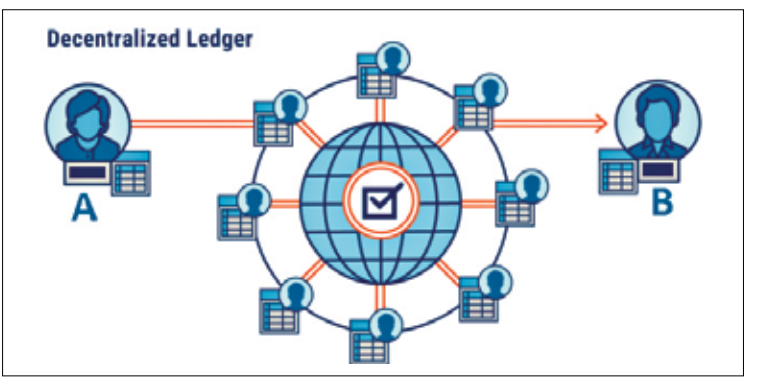
But using hashes is not enough to prevent tampering. Computers these days are very fast and can calculate hundreds and thousands of hashes per second. You can conclusively fiddle with the block and recalculate all the hashes of the remaining blocks to make your blockchain valid again.

To mitigate this, blockchain uses a mechanism called Proof-of-Work, which slows down the creation of new blocks. In case of bitcoin, it takes about 10 minutes to calculate the required proof-of-work and add a new block to the chain.

This mechanism makes it difficult to tamper with the blocks because if you tamper with one block, you need to recalculate the proof of work for all the following blocks.

So, we can say that the security of blockchain comes from its creative use of hashing and the proof of work mechanism.

There is one more way that blockchain secures itself and that is by being distributed.



Blockchain has inspired many new decentralised ledger systems

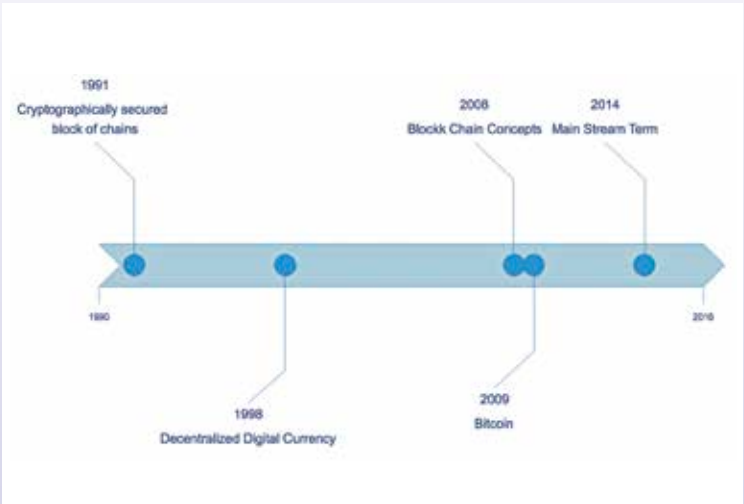
Instead of using a central entity to manage the chain, blockchains use a peer-to-peer network and everyone is allowed to join. When someone joins this network, he gets a full copy of the blockchain. The node can use this to verify that everything is still in order.

When someone creates a new block, it is sent to everyone on the network. Each node would then verify the block to ensure the block has not been tampered with and if everything is fine, each node will add this block to their own blockchain.

All the nodes in this network create consensus. They agree on which blocks are valid and which aren't and reject the blocks that have been tampered with. So, in order to successfully tamper with the blockchain, you would need to tamper with all blocks on the chain, redo the proof of work for each block and take control of more than 50% of the peer-to-peer network, only then will your tampered block become accepted by everyone else, which is practically impossible to do.

This is just a basic idea of how it works and will be further explained in more detail in upcoming chapters.

Applications made on blockchain today are being explored and used in many industries as a cost-effective and secure way to create and manage a distributed database and also to maintain records for all types of digital transactions.



History of blockchain

Blockchain isn't just about Bitcoin, there's more to it than just the technology behind the cryptocurrency.

The idea of Blockchain was first presented in 2008 with a distribution of : "Bitcoin- A peer-to-peer Electronic cash system" , a paper by an unknown individual or group named Satoshi Nakamoto (A nom de plume whose owner(s) still remains elusive).

Blockchain was then, for all intents and purposes, actualized in 2009 as a central segment of the digital currency, Bitcoin. It served as a digital public ledger which would store all the transaction data on the network.

On January 12 2009, the primary Bitcoin exchange occurred between Hal Finney and Satoshi Nakamoto and on October 12 2009, #bitcoin-dev

was enlisted as a talk subject on freenode IRC (an open source venture discussion) and the discussion developed.

The Bitcoin market was established in October 31 2009 and it allowed people to exchange paper money for Bitcoin. This is when individuals start to remember it as a computerized form of cash.

In May 2010, the main Bitcoin buy was of 10,000 bitcoins for a pizza. By November 2010, participation in the Bitcoin marketplace increased the market cap to exceed $1M USD. By Febuary 2011, BTC kept on expanding in esteem and achieved equity with USD ($1 USD= 1 BTC) and by March 2013, BTC market surpassed $1B USD. 10x growth in less than 3 years!

Satoshi claimed to have solved the problem of 'double spend' in digital currency using the blockchain technology in Bitcoin. Double spend is basically the idea of spending digital currency in two places. This is a problem which is specific to digital types of money since it can be copied or produced again easily. This would not be an issue for physical money since it cannot be easily copied and the parties involved in the transaction can easily verify them. In case of digital currency, there is a risk that the holder of the currency could make a copy of the digital currency and send it to the merchant or someone else while holding the original. Bitcoin became the first digital currency to have solved this problem of double spend without requiring a third party or a trusted administrator.

Satoshi Nakamoto vanished from the open (that is from Bitcoin discussions, papers and code contributors) in 2011. Bitcoins, however, kept on being created and marketed by the group which was engaged to address different issues in the code, even during his non-appearance. Bitcoin is used by millions of people for payments, including growing remittances market and its market capitalization hovers between $20-$25 Billion US Dollars.

It was in 2014, that people acknowledged that Blockchain can be isolated from the money and can be connected to different other use-cases. This is the point at which the attention moved from Bitcoin to Blockchain. Relatively every major monetary foundation on the planet is looking into blockchain now and some 15-20% of banks are required to utilize blockchain in the present year.

Smart Contracts

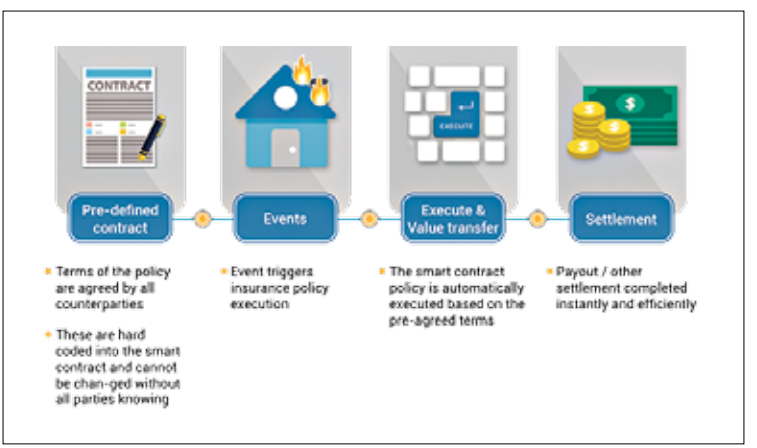
The next development exemplified in the second era was a blockchain framework called Ethereum that led to "Smart Contracts".

In December 2013, a man named Vitalik Buterin released a white paper on what would turn into the "Ethereum venture" – a blockchain platform with the ability to build decentralized applications. Ethereum is a blockchain based distributed computing, public, open-source stage highlighting smart contract facility.

Vitalik was a noticeable Bitcoin lover for quite a long while and was a prime supporter of the Bitcoin magazine in 2012. He tried to update the original Bitcoin protocol and failed to gain agreement within the Bitcoin community, post which he gathered a team of super programmers to develop a completely new blockchain protocol featuring 'Smart contracts' that would allow programmers to build scripts into the blockchain which would act as contractual agreement and execute when the mentioned conditions are met. He named this new blockchain 'Ethereum'.

Smart contract is a piece of code which is stored on the blockchain network. Anything of value, like money, property or shares can be exchanged with the help of smart contracts in a conflict-free , transparent way while avoiding the services of a middleman. It defines the conditions to which all parties using the contract would agree, so certain actions are executed if the required conditions are met. A smart contract is saved on each computer on the network and all of them must execute it to get the same result. In this way users can be sure that the outcome is correct.

Smart contracts are gaining popularity in the e-commerce industry. Every minute change and detail is documented within the blockchain. In



How a smart contract works

other words it allows everything to be recorded during the transactional process and tampering of the data is extremely unlikely making it safe.

Let us try to understand Smart contracts in detail by using an example:

Let us say User A want to ship a truck full of goods to User B. User Z is the trucker who would be carrying the truck full of goods to User B. User A may trust User B, but not the trucker. On the contrary, even the trucker may not trust the sender (User A), owing to the fear of not getting paid.

User A would then sign an agreement with the trucker that he would process the payment only after the goods are received by User B. Such a process would usually involve a third party wherein legal papers and contracts are signed, printed and scanned.

Using smart contracts, this can be made simpler and the rules can be added in the code. User A can use Smart contracts to sign an agreement with the trucker – where the program would mention a code wherein the payment would not be processed till the delivery is confirmed by user B. Once the delivery is confirmed, the payment would be automatically triggered and processed by the smart contract. This can further be modified by adding a GPS tracker attached to the truck, which would eliminate the need for User B to confirm in this entire process and the payment can be processed once the stated conditions are met.

To use a smart contract on the Ethereum blockchain , mini payments of Ether, the cryptocurrency for Ethereum, were required. Since smart contracts are stored on the Ethereum blockchain, anyone can access or inspect the contract for a bugs or irregularities since its contents are public. Additionally, no one can access the funds on the smart contracts, not even the developers.

Using this innovation of smart contracts in the blockchain system , Ethereum developers built small computer programs directly into blockchain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of bitcoin. The Ethereum smart contract platform has a market capitalization of billions of dollars and has hundreds of projects heading towards the market.

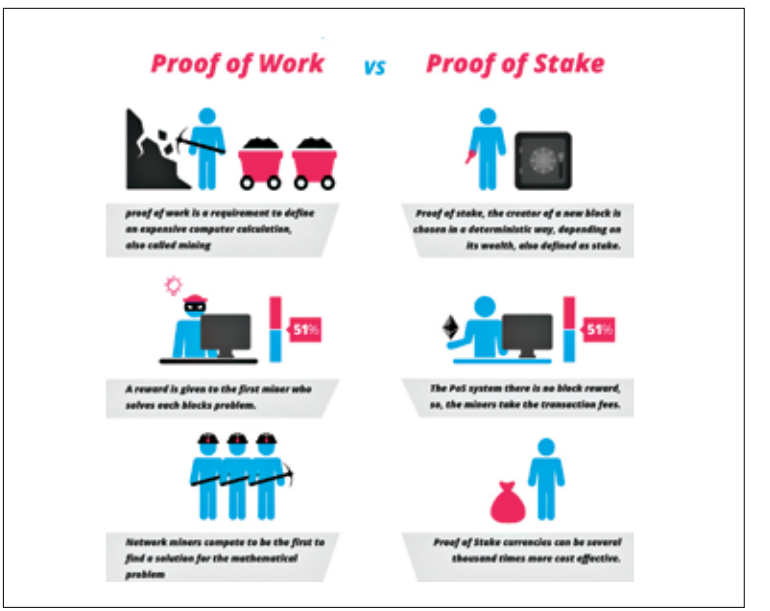
Ever since its launch in 2014, Ethereum has grown significantly and is now considered the second largest cryptocurrency after Bitcoin. By June 2014, the Ethereum project was funded by a crowd sale. Investors realized how Ethereum could unlock a new level of functionality for blockchains and were keen on investing in the same. It has been growing ever since.

Proof of Stake

The next major innovation in the blockchain world was “Proof-of-stake” (POS). A cryptocurrency blockchain network aims to achieve distributed consensus by the Proof-of-stake algorithm. It can also be considered as an alternate process for transaction verification on the blockchain.

Proof-of-stake was first introduced by Sunny King and Scott Nadal in a paper in 2012 and it intended to solve the problem of Bitcoin mining’s high energy consumption. The average cost of maintain a bitcoin network at that time was around $150,000 a day. Today this cost would be around $6-7M USD. In order to understand Proof-of-stake, it is important to have a basic idea about Proof-of-work.

A mining process wherein a user installs a powerful computer or a mining rig to solve complex mathematical problems/puzzles called as proof of work problems is ‘Proof of work’. The verified transactions of several successfully performed calculations of various transactions are stacked together and stored on a ‘new’ block on the distributed ledger or public blockchain. Mining creates new currency units after verifying the legitimacy of a transaction.



Proof of stake helped reduce the average cost to maintain a Bitcoin network.

The work would be difficult for the miner to perform, however it would be considerably easy for the network to check. Each miner on the network attempts to solve the mathematical puzzle first, so as to receive a cryptocurrency as a reward. As more power and efficiency is added to the network, more coins are mined and the number of complex calculations required to create new block increases, thus increasing the difficulty level for miners, thus there is need to recover electricity and hardware costs in case of Proof-of-work currencies.

In case of a proof-of-stake system, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake, unlike where the algorithm rewards miners who solve mathematical problems with the goal of validating transactions and creating new blocks. Blocks are said to be 'forged' or 'minted' and not 'mined', in the proof-of-stake systems. Here, forgers (users who create new blocks by validating transactions) are given a transaction fee as reward and not cryptocurrencies, since the digital currencies are created in the very beginning and their number is fixed.

So switching to Proof-of-stake from Proof-of-work in blockchain led to huge energy savings and a safer network as the attacks become more expensive. Proof-of-stake systems are said to be the future!

Marketers have released organizations constructed around bitcoin and other cryptocurrencies and have additionally decoupled the underlying blockchain technology from bitcoin to develop new equipment and offerings. There are over 250 lively venture-backed startups inside the area and greater than 2 hundred venture capital companies have already invested $1.3 billion into agencies across the rising blockchain environment. It remains early inside the development of corporations around the current generation, with many startups nonetheless within the evidence-of-concept stage – however, if successful, those organizations are poised to generate first-rate value.

Bitcoin's fruitful use of blockchain innovation as a digital currency produced another flood of cryptographic forms of money that are referred to as Altcoins. Most altcoins are very similar to Bitcoin, however each one has its own special qualities. Probably the most well-known altcoins available for use would include Litecoin, Dash and Ether.

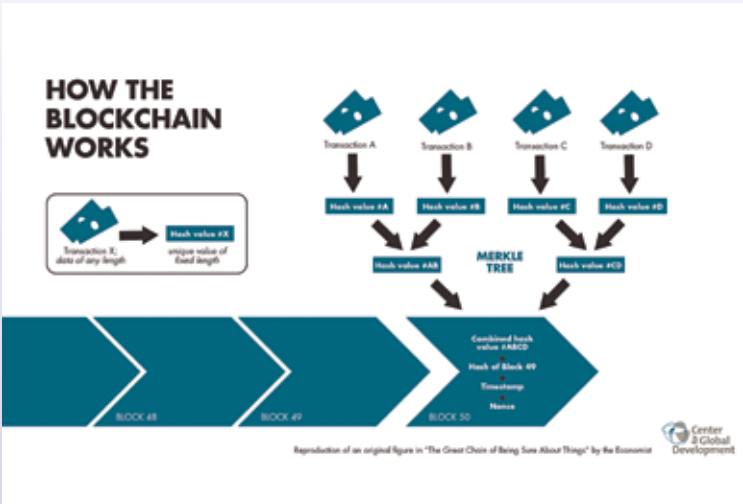
Across the board, utilization of blockchain innovation to date has come predominately through cryptographic forms of money, which have done well to show the influence of the innovation and animate enthusiasm for new applications. Be that as it may, in the previous year, there has been a

quick move in startup action and speculation dollars to an extensive variety of new blockchain applications.

In the meantime, some of the greater hooked up corporations are starting to emerge as dominant players. One example is Coinbase, a virtual forex service sponsored by using challenge capital firms consisting of Andreessen Horowitz and union square ventures. The enterprise allows customers to shop for and sell bitcoins and different cryptocurrencies, in addition to using those bitcoins to transact with online traders. Coinbase has almost five million customers and has raised almost $120 million over five rounds of financing as of 2012.

As digital money and blockchain markets develop, there has additionally been an expansion in new "hybrid" companies. Those companies give offerings, regularly specialized in nature or framework related, to the creating unit of digital currency and blockchain associations. They likewise can give specific projects of the innovation. One example is Bitfury, a startup that began as a bitcoin mining undertaking and has since shifted focus directly into an entire bearer blockchain security and time organization. It has developed restrictive equipment and programming answers that have helped the blockchain scale globally safely. The organization is directly exploiting blockchain to develop another casual property rights registry.

Blockchain innovation today remains at an essential expression point. The innovation is all the more extensively comprehended, and is being connected by business visionaries in ever inventive ways, yet the environment around blockchain organizations, including cryptographic forms of money, is as yet youthful. Early buildup has to some degree died down and now the inquiry isn't around the capability of the innovation. It is about how its applications will be embraced by the market. The dynamic idea of the innovation sets it up to conceivably upset an extensive variety of enterprises.



Understanding blockchain

If the primer on blockchain wasn't enough, then here's an indepth understanding of how blockchain works.

No doubt blockchain technology is rapidly changing the world, but why? What is special about blockchain? How does it work? Now that you know whence it came, it is time to dig deeper so that we may have a better understanding of this disruptive technology.

Follow the money trail

Blockchain came to its present prominence primarily because of a form of digital currency - Bitcoin. It is important enough that at the risk of redun-

dancy we state (again) - Bitcoin does not equal blockchain! Bitcoin is one of several cryptocurrencies, and all these cryptocurrencies are basically different implementations of blockchain technology. But Digit readers will know this already! Though we have covered Bitcoin mining before, cryptocurrency does offer a tangible way of explaining the concept so we shall start from there. Besides, that's also how Vitalik Buterin started thinking about Ethereum. So here we go!

Physical notes are not easily duplicated, but when we get to the digital world, things get a lot trickier! An economy is basically a lot of transactions where agents exchange money for goods and services. We're all trying to get what we want and money is the common medium for value.

At the centre of the revolution

Satoshi Nakamoto's initial motivation described in his paper "Bitcoin: A Peer-to-Peer Electronic Cash System" was for a system that allowed transfer of value between two parties without the need for a middle-man, such as banks. Aside from the unfair advantage that financial institutions possess by being central authorities, it is wasteful to employ their services for small amounts of money that we often exchange in our day-to-day transactions. When you pay with your card at a shopping mall, or use internet banking on Amazon, the Visa and MasterCard companies of the world take a percentage off of every transaction. This is necessary to prevent malicious activity like double-spending or misrepresentation of services. So how does a cryptocurrency achieve this without a third party? Why, using blockchain technology of course!

Trust

The reason we have third parties and central banks regulating and arbitrating money is that we need some entity to place trust in. We trust our

government. We trust the law. Our economic system is based on trust. With cryptocurrencies, we don't need trust. This is a design goal for cryptocurrencies, and blockchain technology in general. Trust, while heartwarmingly reaffirming of the good the world when it isn't broken, can be disastrous when it is. Rationally, it makes sense to reduce risk as much as possible. Hence, it is a good idea to eliminate the need for trust, while still maintaining reliability and preventing malicious activity.

In this context we can examine what trust is, in the first place, and how it plays a role in economic and technological systems. In the most basic description possible, trust is an assurance of reality. When you trust someone, you believe them and allow them to affect how you perceive the world (think Truman Show). While asking someone on the road for directions, this may sometimes lead you to a wrong address, but more often than not there is no way other than trusting another. The world revolves around trust. Even if someone gives you wrong information today, you can verify it for yourself - but what about the past and the future? We implicitly trust historians and books for an account of our ancestors, and trust politicians and policies with our future development. To make the concept of past trust and future trust more relevant, consider the case of a digital currency where there are no physical tokens as proof of ownership, with which we wish to have a functional economy. In this case, without a central authority to place

Image: BTC Keychain

The need for physical tokens is so strong, that people have made them for bitcoin as well.

trust in, we have two problems: how do we agree on a common reality, and how do we make our economy robust (that is to say, how do we prevent one from fooling many into believing a false reality)?

The first problem has a simple solution. If everyone agrees on the history of transactions, any disagreement or false claims can be settled by majority. So we broadcast transactions publicly and store their order in a common database, or ledger. The ledger itself is the blockchain. Everyone has a copy of it, and everyone is continuously updating it. Whose update gets written to history depends on another concept which can be 'proof of work' or 'proof of stake'. This is also the solution to the second problem, as the proof decides reality. Technically we democratizing trust and not eliminating the need for it. Still, pretty neat, isn't it? The best part is, it is not limited to a list of transactions, the actual blocks in the blockchain could be about all sorts of data! But enough talk about ideas, now we shall discuss implementations!

Immutable history

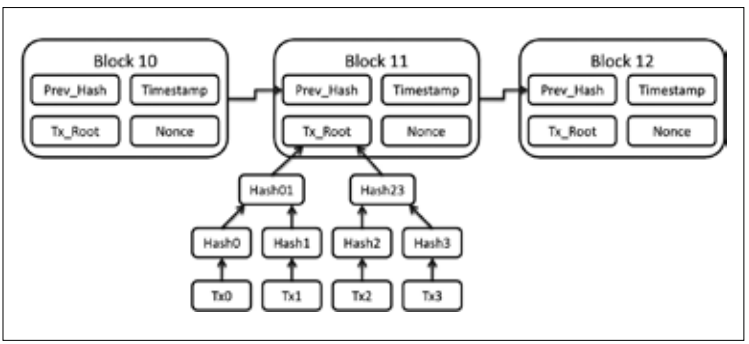
So a consensual history sounds fancy, almost utopian, but how do we do that? This is where blockchain comes in, very literally. If you understand this, you understand blockchain. But before that, we must do a quick review of a couple of cryptographic concepts - Hashes and Merkle Trees.

A hash is an output of a special function, called a cryptographic hash function (surprise!) such as SHA2, which has the property that the output is of fixed length for any given length of input. The output is usually much quicker to compute from the input. This property is useful for proof of work/stake applications. Ideally, every unique input will give a unique output, which is why it is colloquially called the fingerprint of the data that is being hashed. If we change even one character in a million character input to the hash function, we get a very different output which lets us know that the data has been corrupted/tampered with.

The Merkle tree is a data structure where the leaf nodes are labelled with the hash digests of some data, and every other node is labelled with the hash digest of its child nodes. This cascaded hashing allows for storing reduced amounts of hash digest values for a large set of data. Since we are essentially grouping hash digests into a single hash layer by layer, the older unchanging data can be discarded. Version control software such as Git use this structure for tracking changes and verifying integrity.

When it comes to Bitcoin, the ledger of transactions are themselves the 'coin'. A particular number of transactions compose a 'block' and this data

is then hashed along with the hash from the previous block (and a nonce-junk value). In Bitcoin's case the proof of work is to determine a nonce value that results in a certain number of zeros at the start of the resulting hash. Whoever finds it first adds their signature to the block and is 'awarded' some value, and the updated ledger is published so everyone can copy it and race to find the next block. In this way, the history of transactions is being recorded in a series of hashes. The slightest change to any detail of the past will ripple through and make every block after it look different. And since everyone on the network has a copy, unless you control more than half the network, you can't change history!



A schematic of how a Merkle tree is integrated into a blockchain

Let's say we have a hypothetical hash function that produces 64-bit hex codes. (This offers too few possibilities to be practically useful, but let's go with it for the sake of understanding.) We are using it to create a blockchain for the content of this FastTrack booklet, so that we don't have to check it for errors at multiple stages. We supply the first chapter of this FastTrack as input and obtain the digest - 8fa3. This string is appended to the second chapter and hashed to obtain the second digest - 4e32 (which represents the content of both chapter 1 and 2 uniquely). As we write this third chapter, we notice an extra question mark in the first chapter where it shouldn't be. Now we must go back, correct the text, and pass it to the hash function again. This time we obtain b402, even though only one character was changed. Similarly we redo the second chapter's hash with the correct hash from chapter one to obtain cd7c. What we just did is called a fork - we altered history because we were the only ones using the blockchain. On a practical distributed blockchain, this is NOT supposed to happen unless

there is something really wrong and everyone (or a majority) agree to it. This is how some hundred million dollars worth of Ether was recovered last year after being lost to a hack. Though the hacker was successful in stealing the funds, the beauty of the blockchain's design meant that everyone could see where the loot went. The only problem was that no one could access it (without the thief's signature/private key). Aside aside, assuming we have successfully completed the FastTrack and sent it for print along with the blockchain ledger, we no longer have to recheck everything anymore - we just hash our final chapters one by one again and compare them with the blockchain!

This concept of chaining blocks of data through time using cryptographic hash functions is the fundamental understanding of a blockchain. In the case of a cryptocurrency, the data is the list of completed transactions, but it could be anything else. In the case of Ethereum, the data is the computational state of a machine, thus every successive computation is recorded as a state change in the blockchain. In this way, any Turing complete application can be designed to run on an appropriately designed blockchain, such as Ethereum. Of course, the details are much more complex than that, but that's what the developers of the blockchain are for. They build the compiler for the blockchain so users can program decentralized applications in an

Now you can say no to central authorities!

abstract way. With this approach, simple but powerful applications can have around 10 lines of high-level code.

Consensus of the past - Timestamping

A blockchain platform inherently maintains a consensus about the transactions or computations that have already occurred. Even though there is no central authority, it achieves this by distributing the authority among its users. Changes are publicly announced and incorporated by everyone in the order they are received. As the data is represented by the hash and all subsequent blocks, the blockchain also serves as a distributed timestamp server. Once the hash of a data block is incorporated into the blockchain, it will be replicated across the entire network. All successive blocks in the chain are dependent on this and since the hash is unique to the data, it is undeniable proof that the data existed at the time of incorporation into the blockchain. In essence, blockchain technology employs a linear cause and effect model to record events, and verifies truth by distributed consensus. What happened in the blockchain, stays on the blockchain!

Consensus of the future - Smart Contracts

However, this distributed consensus platform is not only useful for past events, but future events as well. In the blockchain we have a distributed ledger that cannot be changed. This is like a permanent record of your words. The words themselves, may be talking about the future, like making a promise! Promises and trust are very related, as trustworthy people are defined as those who keep their promises. Promises can also be viewed as future transactions, as the person making the promise gets something in return for keeping their promise. In the human world, we can make selfless promises, but we still obtain trust in return, if nothing else. With blockchain, the issue of accountability of promises is taken care of by the property of being distributed, but the issue of trust resides further away in time (when the promise is/isn't fulfilled) and cannot be immediately resolved by virtue of being distributed.

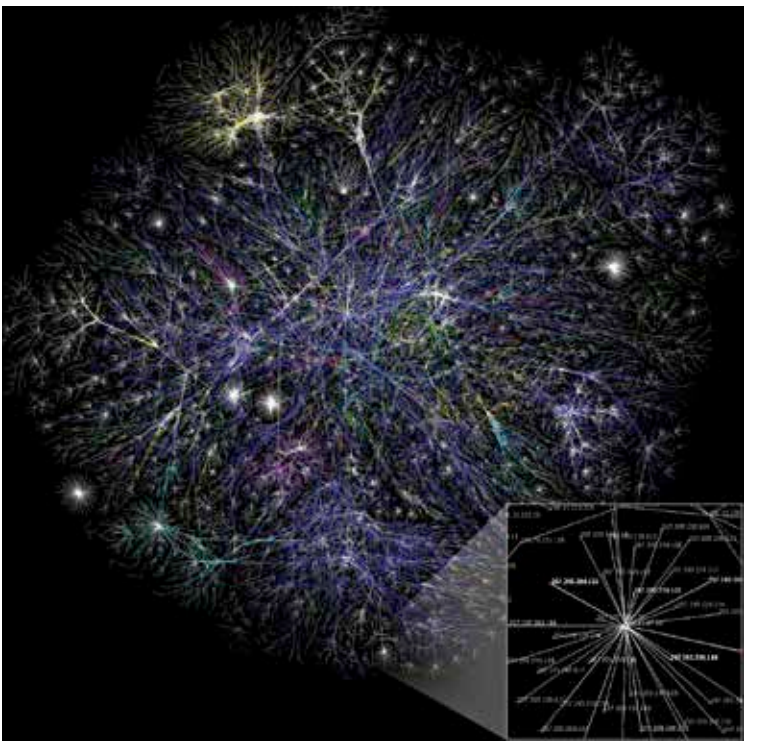
Enter the Turing complete blockchain. With the capability to build a program that lives in the blockchain, we can design 'Smart Contracts'. In the simplest case, imagine a transaction inside an if statement. Perhaps there is also a deadline in the condition, This transaction is only fulfilled when the conditions are met, and not otherwise, because that is the way a smart contract works. There is no need for a third party, or even for the two parties

to worry about verifying the terms of the contract. As long as the contract is formulated keeping all necessary conditions in mind, a smart contract can be deployed using the blockchain that will basically take care of itself.

Re-Decentralization - DAOs

Combining all these wonderful features of blockchain we can envision another type of entity that lives on the blockchain platform - the decentralized autonomous organization, or DAO. We've tried to use the word decentralized as little as possible in our explanation because using buzzwords before getting a grasp of the issue tends to get in the way of real understanding. If you've been paying attention and feel your neurons firing, you may have beat us to the buzzer.

An organization is a meta-agent with an agenda, having access to a pool of resources, run by a collection of agents. These agents are usually of two



A map of the internet from 2005. Today's internet is much more centralized!

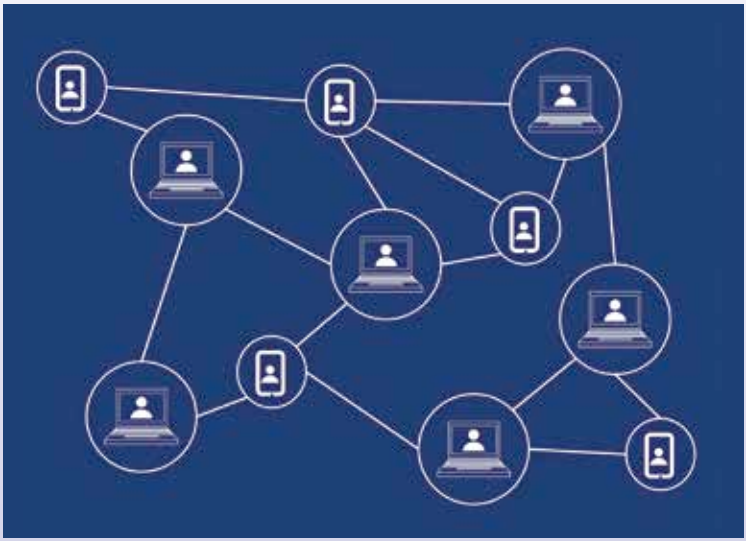
types, when it concerns the functioning of the organization - governing agents and executive agents. Governing agents make decisions on behalf of the organization and executive agents enact them. On a blockchain, a well designed collection of (self-preserving) smart contracts can serve as both. Tie its access to a pool of resources needed to function and survive, and you have created an autonomous entity that carries out transactions/ events in response to certain criteria and according to the rules specified in the smart contract. Once adequately designed and deployed, it functions on its own without need for human interference.

Blockchain technology is already being applied to various industries as we explore in the latter chapters, and that's only the ones people have thought of so far. The possibilities are almost endless! Imagine a decentralized file storage service where you get paid according to how much data you store. Imagine an application that budgeted the government's tax money according to a combination of criteria determined by political science experts and democratic voting by members of the blockchain. No chance for siphoning or bribing, which means, bye bye corruption! Of course, that's merely a dream, but it is a dream worth dreaming don't you think? See more in Chapter 7.

Read more about the InterPlanetary File System to know how blockchain can decentralize the entire internet

Is blockchain as big as the internet? Not really. But it does have the potential to reshape it. When the internet was being born, it began decentralized. Since then however, the capitalist ecosystem created an extremely centralized internet with a few big players getting all the traffic, and all the data. Since data is the modern resource, the world does indeed need to be brought to balance again, and blockchain is definitely a way to go. Why should Facebook profit off your life? Steemit is a fairer world. With the coming of IoT, it is safe to say blockchain technology will become ubiquitous.

The existence of blockchain is a promise in itself, a promise of a better world. Quite in the theme of things, it is upto all of us to decide which version of reality becomes immutable history. The main type of transaction that needs to be carried out is a value (read: data) transfer, away from the central giants, the Googles and Amazons. More than anything, blockchain technology is motivated by a direction - Power to the Edge!



Blockchain Variations

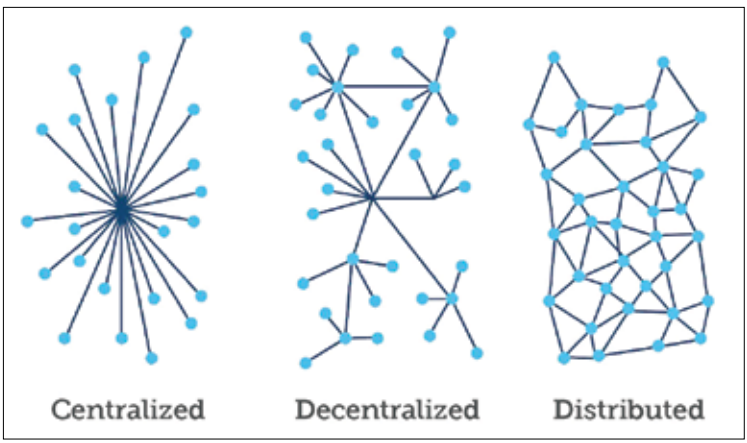
Even as a single entity, blockchains are enough confusing. But the fact that there are different *kinds* of them... Well, we got your back.

A Quick Primer

Blockchain, or generally known as distributed ledger technology, is an encrypted decentralized method of record-keeping. The system enables all the members to keep a copy of the ledger. A change to the ledger is only recognized when a majority of its members verify the change. Upon verification, a new block is added into the chain with the new data. This

monumentally reduces the chances of tampering with data, as the culprit would have to make changes to all the ledger copies.

This form of ledger has been developed as a solution to trust issue of humans and removing the need of a middleman in all our transactions. Blockchain is the first mainstream system that would eventually form the Web3 internet. That would be a purely peer-to-peer internet, no middleman whatsoever. Whether you are booking cabs without Uber or Ola, hotel rooms without Oyo or shopping without Amazon, all transactions would be recorded and maintained by the members of the service itself.



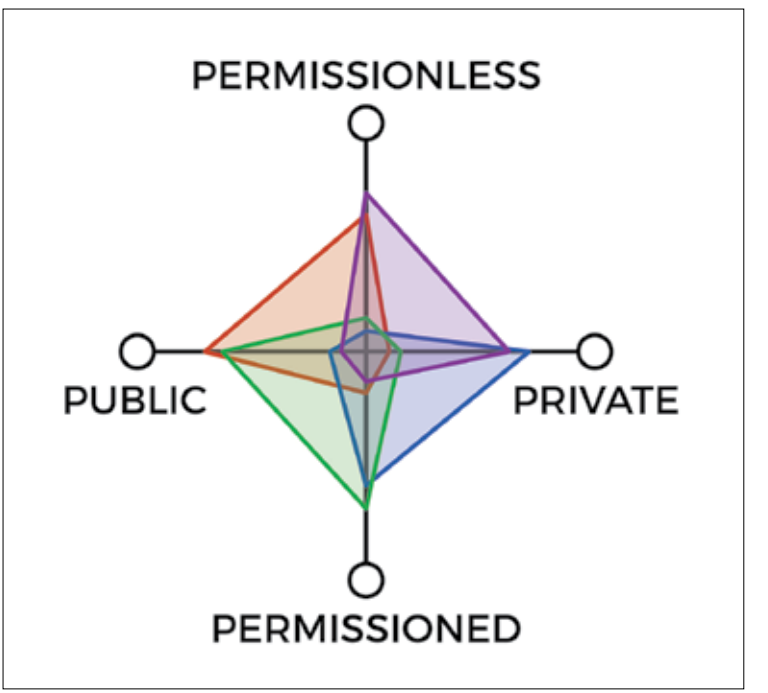
Types of ledger systems

Important Terminologies

Smart Contracts - Similarly to traditional contracts, they provide the terms of a transaction. But unlike their traditional variants, smart ones operate without a middleman and are witnessed and verified by all the members of the ledger. They come along with a time constraint and keys for all the members of the transaction, including the products. If the transaction prolongs the date mentioned in the contract, a refund takes place and all the members of the ledger are updated. The transaction gets fulfilled when the product key is received by the member key mentioned in the contract. And again, as soon as this happens, all the members of the ledger are notified of the new owner of the product.

PoW and PoS - Proof-of-work and proof-of-stake are two of the most widely used methods for transaction validation. In PoW protocol, a member

validates the creation of a block by solving a result for a hash function. Then all the other members validate the result by putting the result back into the function. If the result fits in the function, the member who proposed the result and its proof is rewarded. This method assumes that a member would not cheat the system as they would require spending on real-world resources, computers, and electricity, to solve these functions. PoS is developed to overcome the two major drawbacks of PoW - massive requirement of resources and a chance of one member controlling the majority of blockchain with incredibly powerful hardware. Instead of rewarding for the amount of work done, PoS system rewards the member based on how much their existing wealth they were willing to lock up for the validation. The wealth of each member has an age attached to it, higher the age and the value, increase the stakes proportionately. The proof, in this case, is the stakes you had in the transaction by locking up your funds. Therefore, the more money you lock up, the more chance of a reward.



Blockchain permissions

Public and Private - A public ledger allows anyone to read through it. Private, on the other hand, is a little exclusive in nature and only allows a select few to peek. Both follow the principles of distributed verification but differentiate in the number of mining nodes. Also, a public ledger due to security measurements is slower than private.

Permissionless and Permissioned - A permissionless system is an open system that does not maintain a set of requirements for becoming a node and therefore allows anyone to join in. Permissioned, on the other hand, maintains rules that decide who can become a node and who cannot. These permissions define the stakes of the nodes, therefore, reducing the risk of malicious behaviour.

Two-axis blockchain classification - *Public-Private* and *Permissionless-Permissioned* are used together to classify a blockchain. A permissionless public blockchain allows anyone to become a node and validate the transactions. In a permissioned public blockchain, anyone who meets certain requirements can become a node. Permissionless private systems only allow a specific type of people, but because there are no requirements, the stakes are reduced for each member. Finally, a permissioned private blockchain only allows a specific group of people, usually very small and all of them undergo a set of requirements to increase their stakes.

The Three-Headed Beast

As of the writing of this article, a blockchain can be one of three broad categories. Public, Private and Federated. Public blockchains are the purest form of the technology. Anyone can join the chain, read it, create a node, mine and validate transactions. There is no centralization whatsoever. Though some of the public blockchains have minor restrictions, they still welcome anyone and are distributed. Private blockchains, on the other hand, are on the other end of the spectrum. They are managed by either a small group of people. And they decide who can read through the blocks, create a node and operate on it. They still follow the encrypted nature of pure blockchains. Finally, the federated blockchains are the middle ground, sort of. Instead of containing all the management into one person or a group of people, a federation or a consortium of organisations together handle management. But the fact that the last two variants are centralized, defeats the purpose of blockchains. So in order to remove confusion another term, distributed ledger technology, was coined. This term umbrellas all the three forms of a blockchain.

Public Ledgers

The open nature of public ledgers comes with its own benefits and drawbacks. One major benefit is they are usually open-source. So anyone can take the code of an existing product and make a new version based on it. These new versions are called forks of the original version. The decentralized structure reduces the cost of operations by removing the middleman. This particular fact has become a major disruption in the financing industry. The point of making a currency was to centralize money and now this new technology has questioned the existence of such central bodies. Similar dilemmas are being faced by some other industries that need security of encrypted transactions and large-scale decision making. These kinds of systems enable dodging the bureaucracies. But what takes the titular attention is the fact that there's no central body managing it. This brings the question of security of the transactions. The answer to these questions are the various proofing methods like PoW and PoS. But because both the methods have major drawbacks, concern still looms over security.

Some widely known examples:

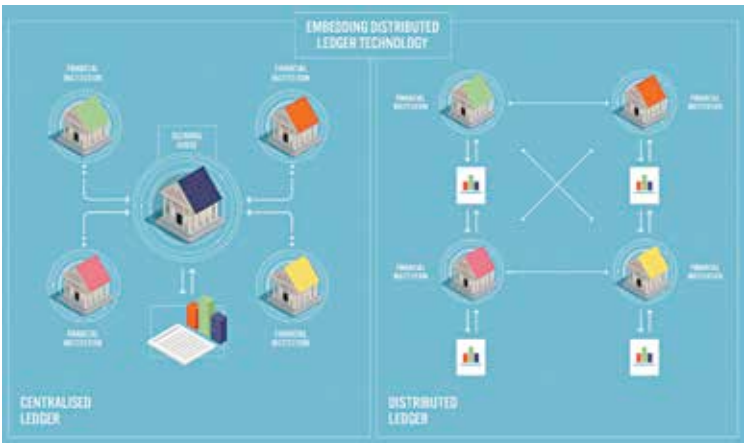
Bitcoin - This is an obvious one. The concept of blockchains was introduced to the world by this insanely popular cryptocurrency. This is also the reason why most people are unaware of other important uses of blockchains. Because of Bitcoin, cryptocurrencies have now become the only mainstream use of blockchains.

Ethereum - It is one of the forks of bitcoins and has its very own blockchain system. Albeit based on the one from Bitcoin, but functionally different. Two key differences are its use of smart contracts to be outside the blockchain and modifiable for specific requirements and a recent switch from PoW to PoS protocol.

Private Ledgers

At the organisational level, some operations might require a high level of security and zero room for compromise. Some organisations might even have regulatory compliances that demand security of information and restrict transparent access only to an elected group of people. For such scenarios public ledgers become harmful. But the encrypted nature and faster decision-making abilities of blockchains can still be used by creating a central group. This group controls the blockchain and decides the rights provided to its members. The consensus in such a system completely

depends on the elected group. This method might go against the nature of blockchains, but it works brilliantly for security demanding operations like database management and auditing. Ideally, organisations should elect a diverse group of people who would not be influenced by each other



Differences between ledger systems

or common sources. This ensures that even if the management is small, it has a relatively higher stability. Private ledgers can even be set up for specific jobs or even specific projects. Due to a smaller management pool, the scalability of such ledgers is much more flexible than a public variant. Even the time to validate transactions is much faster due to the same reason. The closed nature also makes sure that this advantage of flexibility and speed does not dissolve.

Some widely known examples:

Monax and MultiChain are popular platforms to build organisation centric blockchains. Both try to simplify the process through comprehensive education tools and maintaining active communities. They even provide smart contract SDKs that come along with regulatory compliances. Most organisations prefer to customise their blockchains as per their needs.

Federated Ledgers

Very similar to the private variants, but instead of being based inside a single organisation, federated ledgers are for a wider reach. Even though

the membership of such ledgers is controlled, it spans a much larger variety and a number of people. All the members of the participating organisations could be part of the ledger system. Federated ledgers, or consortium ledgers, are the most promising DLTs for governments and banking systems. They provide the ample democracy needed for the diversity of populace while maintaining security and speed in decision-making. Being the middle ground between public and private ledgers, federated ledgers encompass the advantages of both sides. It's a mix of speed and stability. The middle ground of drawbacks means a reduction in the impact, which further increases the effectiveness of such ledger systems.

Some widely known examples:

Corda - A DLT system developed by r3. It's tailor-made to eliminate age-old financial operations which never evolved with the internet. One key difference in Corda system is that only the members of a transaction can look at the transaction to maintain privacy. But because all the members of Corda are part of a distributed ledger system and utilize customized smart contracts, the transactions are much faster than traditional methods.

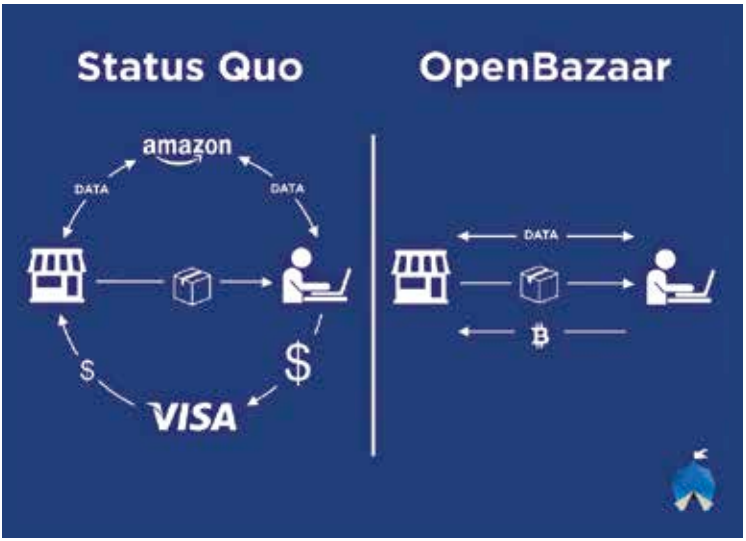
Energy Web Platform - Although as of writing, the project is still in development, it does look promising. Energy Web Foundation along with key people and organisation from the energy industry plan to create a DLT system to increase efficiency in the energy sector. Their plans are to accelerate towards cleaner and more cost-effective sources of energy. Things are quite vague with this one, but judging by the state of energy in our age, a solution from any source is welcome.

Bringing The Heads Together

The three broad types of DLTs treat their systems in their own way. But they share a common objective to establish a newer, more efficient system of validation. Public ledgers focus on transparency at the expense of speed. Private ledgers focus on greater efficiency while maintaining privacy. And Federated ledgers are all about using volume and diversity to solve issues of larger forms. The concept of DLTs over blockchains expands the effectiveness threshold of a decentralized management system. A switch to a completely autonomous society is far-fetched. Our foundations are based on centralisations; the very governance operates with the principle of a single body for everything. In the meantime, private and federated ledgers would provide a smooth transition to study and understand this system.

Classification Based On Implementation

Bitcoin initiated the outcry of blockchains, but as stated earlier, cryptocurrency is clearly not the only opportunity that blockchains open. And when looked through a broader lens of DLTs, the possibilities increase exponentially. Below are some types of these new opportunities.



Blockchain First - Get your hands dirty and work directly with blockchains. Develop new ones or fork from existing once. This path is not for everyone as its still being paved. The blockchain technologies are quite new and are constantly being evolved. Cryptocurrency and apps like OpenBazaar and Ujo Music come under this category.

Blockchain as a Service - Working with and testing blockchains require large amounts of hardware and infrastructure investments. Large cloud companies are developing ways to provide this infrastructure on the cloud. Thereby mitigating the need for giant capital to invest in the hardware. For example, Microsoft has partnered with ConsenSys to provide Ethereum blockchains on Microsoft Azure as a service.

Development Platforms - Blockchains are complicated and not everyone's cup of tea. But that doesn't mean everyone won't benefit from them. These development platforms provide tools and support to developers in creating blockchain solutions. They designed for a faster development

process than working directly with blockchains. Hyperledger provides open source ledger frameworks and educates people about DLTs. Parity is a client that allows interacting with the Ethereum blockchain.

Vertical Solutions - These are the best examples of how far the idea of blockchains can be taken. Beyond a point where they've broken the fundamentals of the technology. The concept of DLT applies to such solutions. They aren't designed to be open services that allow anyone and provide complete transparency. Instead, they're built for specific industries, only to address the issues of that industry. Often times they end up centralizing the system to cooperate with regulations and privacy requirements. Corda, as mentioned earlier, is part of such a system.

APIs and Overlays - The aim of this approach is to introduce decentralization into existing app ecosystems. These are apps and consumer services that utilize the DLT system to make the operations faster and reduce costs. Harmony APIs, by Factom, allow management of sensitive documents while integrating with existing software ecosystems. Tierion is used to check the integrity and timestamps of data and files associated with a blockchain.

Blockchain Applications in Financial Services

The implications of blockchain technology in the financial services are far reaching and can potentially turn the entire industry on its head

Anybody who reads news and is even slightly aware about the financial world needs no introduction to the impact of Bitcoin. It has created millionaires overnight and is one of the most trending searches today. But the impact of blockchain (the underlying technology behind Bitcoin) in the financial sector is much wider. If anything, Bitcoin can be considered as only the tip of the iceberg. Cognizant, the global consulting firm, reports that according to a survey of 578 financial institutions and 1520 executives, around 50% of the respondents expect the technology to transform the industry altogether.

Blockchain technology has several features that make it attractive to the financial services, it's immutable, has built in redundancies, multiple verifications through a consensus network, tamper proof, transparency etc. It can connect all the stakeholders like customers, vendors, partners, governments etc. in a transparent and real time network. This means it can be applied to a plethora of scenarios like payment systems, loan and other capital markets, fund raising, banking transactions, customer information and data management, regulatory compliance, insurance, brokerage etc.

We will look at a few critical business domains that blockchain can revolutionise (if we were to write about all the applications, we would be writing a research paper worthy of McKinsey or HBR)

Commercial banking

Bitcoin and other cryptocurrencies may be all the rage today but banks are more interested in the distributed ledger technology that blockchain offers. Leveraging this technology, banks can ease lending, asset management, registration and tracking, contract execution and improve customer service.

Smart contracts are the cornerstone of the application of blockchain in banking. Smart contracts are self executing programs that act as contracts. They self execute upon certain conditions being met. Simply put, they follow the logical reasoning of 'Perform X if Y happens'. Imagine home loan processing and repayments executed through smart contracts. With an integrated network of banks, credit score institutions, KYC and asset registry, the loan processing time could be virtually instantaneous. The network will process and verify all the details of the applicant like credit score, KYC, financial history and property ownership. The loan could be approved in real time. When the sale of property is confirmed and asset registry has been updated with change of ownership and transfer on the applicant's name, the amount could be remitted to the builder or previous

owner instantly. Cause- purchase of property with all criteria met; Effect- funds transferred. A mountain of paperwork and hours of manpower saved. Industry wide annual cost savings could potentially be in millions of dollars. EMI and repayments could also be similarly automated. Cherry on top, if the funds are in cryptocurrency form, that would be a complete holistic blockchain only process!

Asset management is another area where this technology could have a huge impact in terms of cost savings and quicker turnaround time. Again

Application of blockchain in trade finance opens exciting new possibilities and avenues never before envisioned

using the DLT (distributed ledger technology), any asset sales or transfer will be recorded on the network as a new block. Since every block has to be verified through a consensus and once applied is irreversible, banks can track their own assets as well the asset held under mortgage more effectively.

KYC (Know Your Customer) data can also be stored on the blockchain network and verified through the consensus model. This will decentralise the data making it secure than a vulnerable centralised server and easier to process and access.

Trade Finance

Along with consumer lending, blockchain and smart contracts can have a far greater impact on trade finance. International trade finance, one of the

pillars for a growing economy is a largely paper based and cumbersome process resulting in time inefficiencies. Through smart contracts and a global network, the details and contract terms can be verified and payments done through an automated process saving time and costs. Several other services like letter of credit facilities, factoring, receivable and inventory finance etc. could also be automated on the blockchain. Import export transactions could become smoother by eliminating all paperwork and can happen in real time.

Some of the banks investing in blockchain technology

Banks have been experimenting with this technology since 2016. Back in September 2016, Barclays and tech start-up Wave executed the first international trade transaction using an electronic bill of lading transferred digitally via blockchain technology. Apart from Wave, other startups like EssDocs and Bolero are also addressing the bill of lading process to shift it on the blockchain technology. R3, a global banking blockchain consortium has 80 members comprising of banks and financial institutions are looking to soon implement the proprietary blockchain based Corda software. This is aimed at cutting costs and increasing efficiency in the processing of sight letters of credit.

For banks to unlock the full potential of blockchain technology, they cannot operate in a vacuum. A holistic ecosystem needs to be developed by onboarding the shipping and freight companies, agents, insurers, ports and customs and all the stakeholders involved in any international or domestic trade. Now we are talking about digitising trade and not just trade finance. A gargantuan but not impossible task.

Payments

There are several issues and risks associated with using the Bitcoin system that prevents banks from using it for payments. Instead, they are developing their own cryptocurrency on the blockchain system.

Ripple, the San Francisco based blockchain company has proved to be the biggest driver of revolution in payment systems in the banking industry. Through its blockchain network, it provides global financial-settlement solutions for banks to transact directly and reduce settlement time and costs. Its cryptocurrency, XRP which is the world's fourth largest crypto-currency by market capitalisation is being increasingly used by banks for cross border payments. Thailand's Siam Commercial Bank and Japan's SBI

With the distributed ledger technology, payments can be done in real time and in much secure manner

Remit use Ripple's blockchain as an instant-remittance service. Remittance service refers to payments or transfers from individuals of one country to individuals of another country. In this case an 'instant' is defined as 2 - 5 seconds- so within seconds of a remittance request being entered in the system, the receiving individual can collect the money. Compare this to the traditional system that takes around 2 -3 business days to complete the transaction and you will get a sense of the benefits accorded by blockchain.

Recognising banking as the biggest market and user of this technology, Ripple has established a private blockchain network of global banks consisting of several top international banks like Bank of America Merrill Lynch, Royal Bank of Canada, Banco Santander, UniCredit, Standard Chartered and Westpac. This network will have formalised standards and rules for payments and transfers between banks enabling real time transfers and reducing costs drastically.

Going beyond Ripple, banks are collaborating to form a private blockchain network to launch its own cryptocurrency, Utility Settlement Coin, which is expected to be launched in 2018. Recognising the fact that there are

Ripple has been making waves in the payment industry

several issue with Bitcoin like the 51% attack (which means that individuals or miners controlling more than 50% of the network can prevent a consensus for new transactions to take place) and that they would have no real control over it has prompted the banking industry to collaborate for this project. This currency will be used to clear and settle financial transactions in real time across borders. Since they are stored as a block which renders them immutable and irreversible, payments and transfers can be initiated even before the actual assets change ownership. These coins will be stored on the blockchain and can be exchanged into real world currency. Implementation of this project will result in time and cost savings, reduce back office delays and overall improve customer service.

Capital Markets

Clearing and settlement is the backbone of capital markets- equity and other securities issuance, purchase and sale. Currently, it is effected through a myriad and tangled web of transactions. Accenture has estimated that the biggest investment banks could save $10bn by using blockchain technology to improve the efficiency of clearing and settlement.

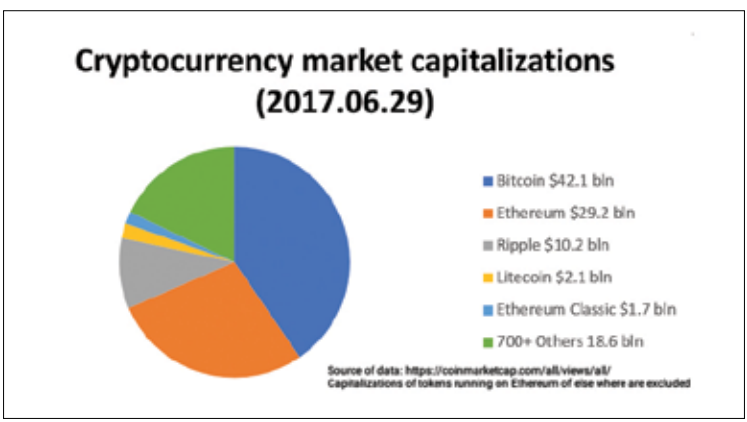
By shifting the entire system on a blockchain platform, the entire process can be automated to a real time basis. Also, the DLT will make global security transactions easier and payments can be still be instantaneous. Again, due to the consensus feature, fraudulent transactions can be easily spotted and halted. Tied in with the payment solutions discussed earlier, the entire process can be revolutionised and digitised. This will also have the added impact of improving liquidity of all securities in the market and also enhance transparency. Regulators can have easier access to the data thereby improving the security of the clearinghouses and instilling added sense of trust in the public.

Going beyond implementation by current security exchanges, this technology could also potentially lead to a decentralised non-intermediary based security exchange. A peer to peer exchange if you will.

A Revolution in Fund Raising- ICO's

This is the decade of startups. Fundraising has never been so easy. Every other day we read about millions or even billions of dollars being invested in startups of various stages and across industries. Blockchain companies like Ripple and R3 also have also raised millions in angel and venture funding. So is it conceivable that this sector will escape the effects of the blockchain technology? Of course not.

Let's take a quick look at the traditional funding route for startups. At an early stage, as early as ideation, one can raise funds from individuals or



Cryptocurrencies have taken the world by storm and are an asset and marketable security in their own right

even early stage investment companies called angel investors. After reaching a critical mass in terms of customer acquisition or proving the viability of the product, more mature investors enter the picture with a bigger money chest called Venture Capital (VC). VC funding is done through stages or series like series A, B, C and so on. For mature companies, Private Equity (PE) comes into the picture. Any startup or company looking to raise funds has to approach multiple angel investors or VC's with their financial data, presentation, working prototype etc. There is no single point of dissemination. After the initial approach, there are again multiple meetings and presentations and finally a term sheet or agreement is drawn up that outlines terms like amount raised, equity shared etc. and funds are transferred. This is a long and arduous process.

Then crowdfunding broke this traditional mold. It allowed for any individual to invest in a company directly through a portal like Kickstarter. Building up on this model, Initial Coin Offerings (ICO) are akin to crowdfunding- anybody on the network can invest up to any amount.

An ICO can be centred around a cryptocurrency like Bitcoin or it can issue its own new cryptocurrency with its own blockchain. In the first scenario, the company issues a crypto-token on the Ethereum blockchain which can be purchased by the investors at a given rate like 10,000 tokens for investment of $100. This rate is completely up to the company's discretion. These tokens can be used to typically purchase products or services the company offers. They are also pegged to an existing cryptocurrency like Bitcoin which are publicly traded. There are exchanges that are built for

At this stage we have barely scratched the surface of blockchain technology in financial services. How the landscape will change, only time will tell

listing of ICO tokens where the market prices are reflected. So, the prices of these new tokens also change and if the prices increase from the ICO price, the investor can sell them at the exchange and make profits. So this means that there can be two types of investor- one that invests or buys the tokens to be used later for purchase of services or the more traditional kind who believes that these tokens will appreciate in value and a profit can be made. A company following the second path of issuing a new cryptocurrency will need to develop its own blockchain and will be selling the new coins instead of tokens. This will not be pegged but will be traded as an independent cryptocurrency.

Move over IPO, ICO is here to take over.

Let's take a quick look at a typical ICO process.

- The company issues a white paper outlining the product or service, fund usage, growth plans, expected returns, whether they are issuing tokens or a new currency, where the tokens can be used etc.
- The company also sets a specific target investment to be achieved.
- A smart contract outlining the deal and details is entered into the network
- Willing individuals or investors register on the Ethereum platform and receive a new ETH wallet address into which they deposit their investment amount.
- At the end of the ICO, if the target investment is achieved, the investors receive the tokens.

- Note that if the target is not met, all investment is null and void and the invested funds are returned to the investors.

There have been several successful and some unsuccessful ones too, including a few scams, that have raised funds from ICO's. Ethereum itself raised $18.4 million on its ICO when it offered the token Ether. The ICO to watch out for is Telegram's $1.2 billion fundraising plans. Successful or not, it will definitely signal a turning point in this technology giving it an added impetus.

Financial services is a giant, it could be called a lumbering giant due to its sheer size. The scope of blockchain technology in this sector is immense. Banks have already started adopting and experimenting with it. The next few years will be exciting to say the least and promises to change our lives.

Blockchain Applications in Insurance

The mammoth insurance sector known for its resilience to change is susceptible to high impact with the advent of blockchain technology.

The hype surrounding Blockchain is currently centered around the monetary implications which currently shadows the far reaching implications of the technology in other areas. The distributed ledger technology due to its inherent nature of providing safe,

compartmentalised records with built in redundancies has the potential to turn the insurance industry on its head.

There are several areas where this technology can be applied which will benefit the insurance provider by lowering costs and also benefit the consumer in terms of quicker and better service. In fact, McKinsey, a management consulting company has estimated that for all blockchain related applications across sectors (excluding Bitcoin only related solutions) nearly a quarter of them are in the insurance sector. Let's explore a few areas where this technology could turn the existing system on its head.

Smart Contracts & Claims management

Honestly, how many of you have ever read an insurance contract or agreement word by word? The legalese is akin to Greek and Latin for the layman and the fine print enough to let out a string of expletives. The normal modus operandi is to understand the broad terms from the provider or the agent and then run to them in case of a claim. Blockchain could change all that with smart contracts.

Simply put, smart contract is a self executing code triggered upon certain parameters being met. This means that the parameters are known to the insured and the insurer; so you, as the customer, know exactly what you are getting into. The contract with all its parameters and conditions is recorded on the network as a block. This data contains the identity or identities of the insured, the provisions of the contract and the terms and conditions. The beauty of a smart contract is due to the immutable nature of blockchain. This ensures that there is complete transparency and almost zero chances of need for arbitration. Also due to the security features of the network, both the parties can rest easy in the knowledge that their data will always remain confidential and private.

Currently, if a claim is to be filed, it usually involves a mountain of paperwork, verification process and the patience of a zen master to follow up with the insurer for weeks or even months. Since smart contract is a self executing protocol, it automates the payments upon verification by the network. Under the aegis of blockchain, all paperwork will be become redundant. Once a claim is filed, the network verifies the details of the claim, compares it with the recorded data and if it's a match, processes the claim and releases the payment. This in turn is recorded as another block on the network.

The process of the claim can also be initiated by a trusted third party and not necessarily the insurer or beneficiary. For example, in case of life

The biggest game changer in the sector, it promises to eliminate a lot of headaches from the claim process

insurance where the claim is typically filed by the nominee or beneficiary it can now be initiated by the hospital in the course of their record keeping. The hospital will be a node on the network and the record it creates will be logged in as a claim filing. Multiple verifications can be done by connecting the various institutions involved on the network like the police department, the concerned municipal department etc. These nodes are trusted third parties on the network and are known as "Oracles". Similarly, in case of medi-claim or auto insurance the approved hospitals or garages are connected on the network and a claim gets logged from their end.

This model was demonstrated at an hackathon event in London in 2015 by a startup, InsureETH, in the travel insurance sector. Using smart contracts, they built a payout model for insured flight tickets when cancellations or delays are reported from verified flight data sources. This does not involve filing of any claim but uses data from public sources on cancelled or delayed flights to affect payouts. This process makes claim filing hassle free for the insured / beneficiary and is absolutely customer centric.

So basically, the network takes over the role of an intermediary or clearing house or administrator. Obviously this means a lot of cost savings in terms of manpower, paperwork and administrative hassles for the insurance companies. A win-win for all.

Smart Know Your Customer (KYC) Data

Today, almost every service provider, right from financial services to an internet provider requires KYC documents and information from its customers. And usually, its the same information required. But since there is no sharing of data between companies, the consumer has to provide the data separately to all the companies. There is one problem and one fear that the customer has with this system. The duplication of data becomes extremely tedious for the customer and there is always the fear of the data being leaked to or stolen by other parties. For the companies, its a time consuming process entailing high administrative costs and manpower. Enter blockchain to the rescue.

The consumer stores their KYC information on a block in the network which is protected by a encryption key. This data is verified by the network and once consensus on this is achieved, the block is accepted in the chain. The creator or customer can then share a public key with the relevant parties or companies that need those details. This means that the institutions can verify a customers KYC details instantly. If a customer wants to apply for insurance from multiple agencies or even transfer policies from one insurer to another, they do not need to go through the KYC process again; they simply need to share the public key with the relevant institution.

A seemingly simple solution of digitising customer data can have far reaching benefits for the provider and the policyholders

Another method of sharing of KYC details is through the use of "Oracles" which were discussed earlier. The insurance companies can obtain the necessary information from trusted third party sources like Government institutions after getting the relevant approval from the data owner.

In India also, companies are actively looking at blockchain based solutions to store KYC data and reduce costs. Thirteen insurance companies have come together create a central registry of policyholder data. This will eliminate the need for iterations of the same data for the same customer across multiple policies.

Since a blockchain is built on a system of distributed ledger, with every block recorded with a date and time stamp and a unique hash ID, it is nigh impossible to hack or alter the records. Any changes in the data like change of address, name etc. is recorded as a new block. Compared to the current method of storing data on a centralised server which is vulnerable and susceptible to cyber attacks, this is a boon for the insurance companies and the customers. Just look at some of the high profile data thefts: Yahoo: 1 billion accounts hacked in 2013, 500 million in 2014; eBay: 145 million hacked in 2014; LinkedIn: 117 million in 2012 and these are just the tip of the iceberg. Battling this is a nightmare for financial institutions, a problem which blockchain technology tackles very efficiently. In terms of costs and manpower, there is significant reduction and the element of human error is completely eliminated.

Fraud Detection and Prevention

Insurance fraud is a plague tormenting the industry for years. Multiple claims, fraudulent claims, forged or phony documents are some of the issues that blockchain technology can tackle and eliminate.

As we saw in smart contracts, every claim filed is recorded as a new block on the network. The network independently verifies this claim against the given parameters. Since a block once created cannot be changed, multiple claims are automatically detected on the network and immediately rejected.

In this network, the claims are also verified with trusted third party institutions like hospitals, garages, Government departments etc. thereby ensuring the veracity of the claim. E.g. a mediclaim filed by the insured is verified against the hospital and pharmacy records which are also connected on the network.

The verification process can be expanded to validate asset ownership and double checked with police theft records to ensure that an authentic

Fraud estimates in the sector are pegged at around 3% - 5% amounting to a lot of losses in a industry of gigantic proportions

payout event has occurred. Everledger, a startup, is applying this concept in establishing proof of ownership for precious stones. It is creating a registry that will record the ownership and details of every stone which will be recorded on a block with a unique series number that is engraved on the stone. Once a critical mass is achieved, it will become an industry standard and unless the seller can provide electronic proof of ownership, they cannot sell or claim insurance.

Going beyond just verifying claims, even the identities of the claimants can be verified on the blockchain network and checked against police records and previous claim history.

Since all of these process are automated, human error and internal fraud is also eliminated. The costs associated with insurance fraud like payouts on spurious claims, dedicated manpower and management will be drastically leading to a leaner organisation and affording the insurance companies to reduce premiums.

Managing Independent Agent Contracts

We all know at least one insurance agent in our circle of family and friends. The industry has grown with and given rise to an immense population

of agents with at least on nearly every street. Even with this population explosion, there is no dearth of individuals waiting in line to join up and the companies welcome them all with open arms. This system spawns its own humongous set of data and contracts. An agent payout is typically layered with premium and number of policies sold and structured with a fixed credit period. Add to that the bonuses for exceeding the targets and special rewards announced time to time. This record keeping and management is no less onerous than customer database management.

The KYC process for any service can be greatly improved by using blockchain

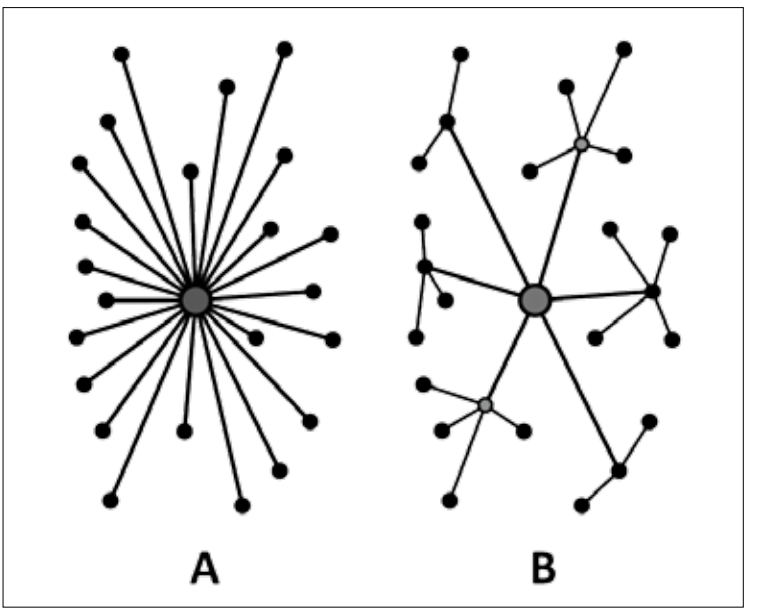
The efficient solution provided for KYC and customer contracts, can also be provided for agents. The data of every agent can be recorded on the network and a smart contract can be executed between the agent and the provider. The data will contain the agent's KYC, which can be checked against previous records for blacklisted agents or duplicity and bank account details. This data can also be instantly shared and compared with the relevant governing bodies for license verification. Since blockchain is almost hack proof, both the parties, the insurance company and agent, can rest easy on the veracity and confidentiality of the data.

The contracts will also have automated payouts upon meeting of certain criteria. Once an agent reports a sale and records premium received, the network will verify that the agent is an active and licensed agent. Then it will cross check with the insurance company records that the premium has been received and thus confirm the sale recording it on a new block. If KYC is also recorded on the same network, customer data can also be verified for authenticity and triple verification. Once the sale is recorded,

the agent payouts will be transferred automatically to the bank accounts as agreed upon in the contract. Since blockchain uses a distributed ledger technology with several interconnected nodes, all of this verification is done in the shortest possible time.

Decentralized Autonomous Organization

A decentralized autonomous organization (DAO) is the epitome of application of blockchain technology in the insurance field. It is a self-regulated autonomous body with no central organisation and no human employees. It relies wholly on the peer-to-peer network of blockchain that manages the policy and claims for a group of policyholders. Imagine an Uber or Airbnb for insurance. Like Airbnb, it is a peer to peer network that connects all the users on a single platform facilitating transactions.



A DAO can eliminate an intermediary altogether adding more efficiency and transparency to the entire process

The decentralised network records all the data and any subsequent transaction like premiums paid, policy terms, claims and payouts on the blocks of the network. The network verifies all transactions and acts as a corporate

entity without any human intervention. Dynamis is a new player that is making a foray into DAO-based insurance using a blockchain solution.

Application of blockchain in the insurance sector is a gargantuan task. Apart from the insurance companies and customers, applying the technology in the sector would involve several stakeholders like external service providers like doctors, hospitals, pharmacies, garages, governmental departments like registrar office, health department, police and fire department etc. depending upon the solution. At this point this vision seems to be a question of when rather than if.

Blockchain application in governments

A Government, being the biggest and most influential service provider, can use the blockchain technology in a plethora of ways ushering in a new era of transparent and trusted governance

Around 25 years ago, little did anyone know that the World Wide Web would take over the globe and transform the way we conduct businesses and even interact with each other on a day-to-day basis. There was virtually no means of online shopping or entertainment or any business done online. All of that has changed over the last two to three decades. Almost every aspect of our lives has been taken over by the internet. This large scale adoption of the World Wide Web as we know it today didn't happen overnight. In its initial stages, the internet and its supporting technologies were met with uncertainty and its share of criticisms.

While the internet did see a phase of people welcoming it with open arms, blockchain technology may or may not see the same level of acceptance. One of the main reasons is that even if its adopted, most of the work done by this technology will be behind the scenes. For it to enter the mainstream and to see everyday people using blockchain is not going to be an easy task, largely given how complex a network it is. Bitcoin, the most popular of blockchain-based applications, is challenging how people view the idea of blockchain. However, adoption in everyday lives is far from being around the corner.

But think of larger governing bodies and institutions like healthcare, insurance, or even governments that are buried under piles of paperwork. There is real potential for blockchain to be put to optimum use here. The benefits of blockchain can be circled down to three main aspects — speed, efficiency and security. Think of these benefits from the perspective of the public sectors organisation and you will see why the marriage between governing bodies and blockchain technology could be a blessing in disguise for agency officials and citizens alike.

Around three years ago none of the government agencies across the world were even considering the use of blockchain. Today several countries including our own are running pilot tests in various states to verify the application of blockchain in the public sector. These tests are being run at two levels -

1) Broader architectural tests to determine if blockchain can offer better functionality on the broader spectrum of everyday governance
2) Internal communication between various agencies of the public sector or even internally between various levels of the same agency

Let's look at some examples of countries that have already adopted blockchain or are looking forward to in the foreseeable future.

Estonia

The Estonian Government has always been one to adopt technological changes before most of the world can even catch up. They have done the same with blockchain technology. Their KSI (Keyless Signature Infrastructure) technology based on blockchain helps secure all public sector data. All one million health records have been put into the blockchain system. They are even turning their voting system into a completely electronic method using KSI. Another application of the KSI is to warn the government about any possible threat attacks, so that governing agencies can nip any such attacks in the bud.

Dubai

Dubai has gone one step further and has set up a Global Blockchain Council, the job of which is to determine how to effectively use the technology at hand for securing transfer titles, public records, health records, business transfers, cryptocurrency, diamond trade, to name a few. They have entered a partnership with IBM to find a trade and logistics solution which allows them to monitor any shipments in real time thus cutting out the chances of fraud and money laundering that is a common aspect in the industry. Dubai is of the opinion that effective usage of blockchain could save the country millions in administrative fees every year.

Singapore

Singapore has explored the possibility of using blockchain technology for inter-bank payments. The Monetary Authority of Singapore created its own digital currency used for transactions among banks in the country. The use of blockchain for inter-bank transactions meant higher levels of transparency, lesser time and money spent on administrative costs, higher levels of security, lesser chances of money laundering. With their pilot tests having been successful, Singapore has launched cross border payments using DLT (distributed ledger) technology.

India

The state government of Andhra Pradesh was the first in our country to wholly welcome blockchain technology with open arms. After running pilot tests in two of its many departments in October 2017, they have now begun assimilating a number of other agencies under the blockchain umbrella. The first couple of tests were ran to see if blockchain can help combat cyber

The Indian government is embracing this new technology to provide better services for its citizenry

security threats, especially where land transfer titles were concerned. A similar pilot was also run to assess the use of blockchain technology in the verification of titles of vehicles under the Transport Board of the state. Telangana also followed suit and has Karnataka hot on its heels. The first ever Hackathon in Karnataka was held in January this year. The state government funded event aims at inviting students and IT professionals to help understand how to best apply blockchain to the state's governance structure.

Why governments need blockchain

If these examples of countries that have embraced blockchain are anything to go by, it doesn't seem like world leaders need a lot of convincing to cast their votes in favour of using blockchain for governance. With each passing day, world leaders are beginning to favor the concept and are looking at newer ways to adopt the latest in technological keywords. Regardless of what critics might have to say about blockchain, one thing's for sure. The technology that backs blockchain is nothing short of transformative. And if experts are to be believed, it reminds them of the early days of the dot-com where the motto was simple — 'adapt or perish'.

Most governments across the globe applying this emerging technology are fully aware of advantages in being the first ones on board. They get to play the role of being primary movers. Add to that the fact that the result of this means millions saved. How you ask? Blockchain is designed to be decentralised. What this means for governments is that eliminate hundreds and thousands of man hours in administrative duty of intermediary officers. This also reduces the chances of clerical errors that come from mishandling of data that could potentially change the lives of millions of citizens.

Why blockchains will work for governments

There are a few aspects of this technology that make it lucrative for governing bodies to want in.

1) Decentralised

There is no single point of authority. Authority lies in the hands of everyone who is a blockchain member. This indicates that all members are likely to benefit from a blockchain, but it additionally means that everyone is responsible for the data in this chain. If anyone breaks security protocol, it can easily be traced back to the offender. Accountability is real with blockchain.

2) Immutable

All data in a blockchain is 'read only' and cannot be edited by blockchain members; not even its own creator. Once it is on the blockchain, it remains

Enhanced, tamper-proof security is a cornerstone of blockchain technology and the main argument in its favour

there for posterity. Everything on a chain is time-stamped, thus making the chain as permanent and secure as records could ever be.

3) Almost in real time

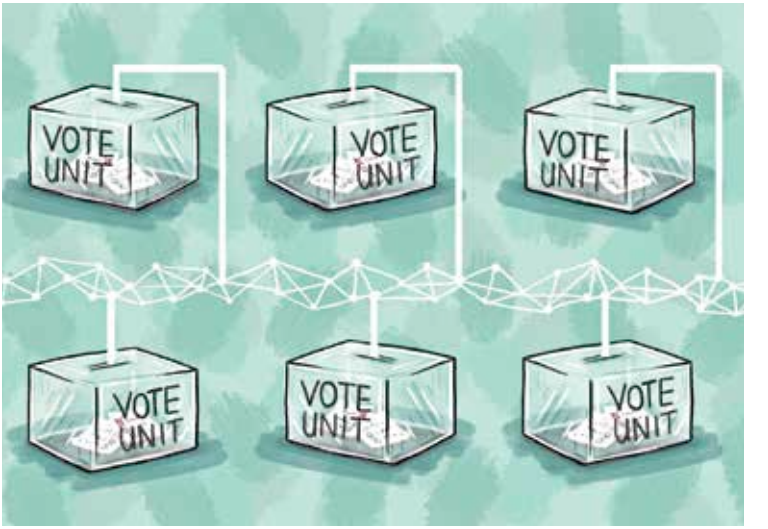
Traditional methods of data collection and sharing are long and tedious. They involve risk mitigators who evaluate the data before clearing it. And this comes at a cost as well as it makes the entire procedure lengthy. Blockchains will help eliminate the need for an intermediary resource. Plus, with the inclusion of smart contracts into the ledgers, members can also safeguard transactions that are created using mutual and secure consensus on the network.

Putting it into action

When you think about any of the branches of government, whether its federal, local or state, you picture overflowing cabinets of paperwork. Things changed when most records became digitised. While that hasn't been a total success in India as yet, we know we are getting there slowly and steadily. Nonetheless, these digitised records were not utilised until the internet came along in its current form. The internet as we know it today has helped make public sector records more accessible and transparent. With the application of blockchain, these records can be better maintained and become even more useful to both the government and the taxpayer. The taxpayer can now be in control of what information the governing bodies has on them, and also control the access for the same. The official agencies, on the other hand, can reduce their own burden by having an auditable paper trail that is time stamped and immutable. It can also help them trace any deviations. For instance, tax defaulters will stick out like a sore thumb when they try to evade their tax payments.

Blockchain enabled e-Voting (BEV)

Elections are a trying time for governing bodies and voters alike. For decades now, we have all dealt with the chaos of standing in a long winding queue for hours to cast our vote. While our nation is striving to become 'digital' in the true sense of the term, not much has changed as far as our voting systems go. Things get even worse as you move towards the rural areas. There have been talks for a while about making the whole voting system electronic. This would mean that a voter could vote from either a physical booth using an Electronic Voting Machine (EVM) or via their mobile phones/laptops.



Secure and accurate voting is a real possibility with the adoption of blockchain technology

When it comes to larger national elections, collecting and evaluating the votes is a logistical nightmare for everyone involved on the management side of things. Add to that the rampant corruption involving double voting, fraudulent voting, buying votes for a certain someone/ party etc. While blockchains might not be able to completely eliminate traces of the bribes, it could definitely help with other problem areas of traditional voting systems. By linking your vote to a blockchain, you get access to other members' votes as well. And given that the data is immutable, you get one vote that cannot be changed and is tamper-proof. This would additionally mean that all members of the blockchain could also count the votes for themselves, since all the data is linked and permanently time stamped.

Public services and networks

While the government has been collecting information and data from its citizens for years and decades now, most information gets stored in ineffective methods. The data cannot be accessed by certain other government agencies that may need access to them.

Blockchain could allow its members to determine how much information they want to share and with which governing agencies. Each member

Dusty files, overflowing cabinets, repeated trips to the department for a piece of paper could be a thing of the past with the adoption of blockchain technology

has a public key, which when upon sharing provides basic unidentifiable information about them. This information is the kind that is easily available and does not give out specific or personal information about the user. The private key held by every member gives them the power to determine which member of the blockchain gets access to what and how much information about them. This kind of freedom to the taxpayer while reducing the burden of administrative fees on the government may well be one of the primary reasons why every governing body should at least consider blockchain technology.

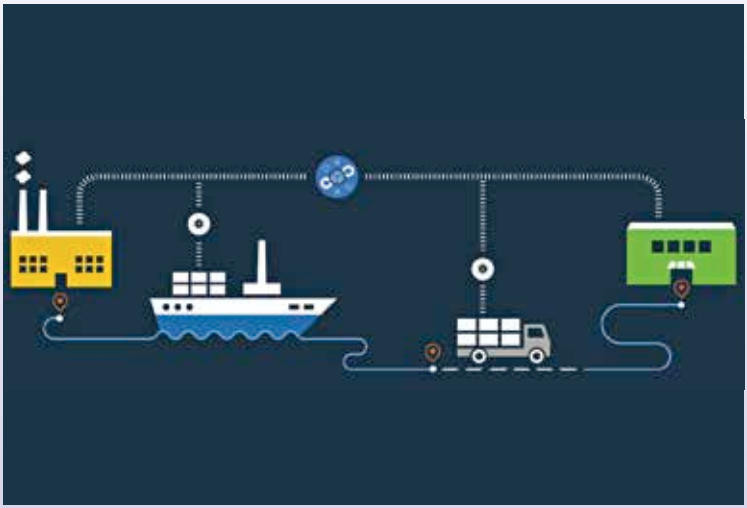
Looking into the future:

Blockchain is not all gold. It has its flaws. But these are flaws that can be corrected, remedied or completely done away with in the times to come. Some of them include issues such as scalability. For instance, the bandwidth of Bitcoin is only 5 to 7 tps (transactions per second). The tps for Visa on the other hand is in the thousands. For blockchain networks to grow and become as fast will take time and will need a lot of research and development from engineers.

Leveraging blockchain is not just a technological question. Leaders who take decisions to backup this emerging trend need to understand how their decisions are forever going to change the way business has been done. Changing things back to the way they are now, once blockchain is adopted, is close to impossible. And while blockchain may have various areas where

The current capacity of transactions is comparatively low on Bitcoin, but with the adoption of blockchain technology, other applications can be made more efficient over time.

it can help ease the burden of governance, there are certain areas where it cannot be applied. That being said, world leaders are taking notice of blockchain and they do understand the implications their choices have on their citizens and the rest of the world. If we find governments that are willing to take the lead and apply blockchain and encourage the technology to expand, we may just have a winning formula on our hands.



Blockchain and Supply Chain Management

Organized supply chain management has been around since the 50s. But it has become a hassled and outdated regime. Can Blockchain be the answer to solve the shortcomings of a sector which is ever growing and shows no signs of stopping. We analyse the possibilities...

Since the introduction of the shipping container in 1956, manual paper-based processes are still common and the information about the status of goods is locked away in organizational silos. Today 90 percent of goods in global trade are carried by the shipping industry but the supply chain is slowed by the complexity and sheer volume of point-to-point communication across a loosely coupled web of land transportation providers, freight forwarders, customs brokers, government's ports and ocean carriers. This problem can be tackled with a distributed permission platform accessible by the supply chain ecosystem designed to exchange event data and handle document workflows. Companies such as Maersk and IBM are employing blockchain technology to create a global

'With the help of Smart contracts, we can fine tune the process of supply and demand'

tamper proof system for digitizing trade workflow and tracking shipments to end costly point-to-point communications. The collaboration will launch with the potential ability to track millions of container journeys per year and integrate with customs authorities on selected trade lanes. In a recent test by Maersk shipping, a single container of flowers from Mombasa in Kenya to the port of Rotterdam in the Netherlands, resulted in a stack of nearly 200 instances of interactions between more than 30 entities. Using blockchain means eliminating these peer to peer communications. Let us

try and understand even more clearly what the problem is and how blockchain intends to solve it.

Why blockchain?

As the internet-of-things continues to grow at a rapid rate, sensors and devices are becoming more commonplace to communicate information in business networks for data such as location, temperature and other properties that need to be shared. A private blockchain ledger can help create a tamper-free record. This opens up new ways of automating business processes among partners without setting up a costly centralized IT infrastructure and all participants have access to the same data. Let's look at how supply chain benefits when data is shared.

The private blockchain passes through all the multiple carriers in the supply chain. The business contract specifies the conditions that must be met during the shipment from the factory to the grocery store and all parties must adhere to the terms of the contract. A temperature sensor embedded in the package stores the data locally and sends it to the data cloud. The cloud information is shared across all peers. After every carrier meets the contractual obligations, the shipment arrived its final destination without exposure to excess temperatures.

'Blockchain eliminates the need for any third party vendors and is a direct transaction between the producer and the buyer'

Using blockchain allowed all business partners to access the same temperature data without requiring central control. the result is a happy customer with peace of mind about food in their carts. With blockchain, shipment data will be stored publicly or pseudo anonymously in a shared database. Now with blockchain you can track a chronological history of any asset in transit during manufacturing and change of ownership. No one can tamper with the information because everyone has the copy of the same data as it involves an append-only database.

Smart Contracts

The backbone of any blockchain enterprise that solves the problem of supply chain is the concept of smart contracts. But what exactly are smart contracts. Let us have a closer look.

Smart contracts (also called distributed apps) are very popular nowadays. The term "smart contract" was first used by Nick Szabo in 1997, long before Bitcoin was created.

'Smart contract is a digital agreement between one or two parties'

Szabo is a computer scientist, law scholar and cryptographer. In simple terms: he wanted to use a distributed ledger to store contracts. Now, smart contracts are just like contracts in the real world. The only difference is that they are completely digital. In fact a smart contract is actually a tiny computer program that is stored inside a blockchain. Let's take a look at an example to understand how smart contracts work.

You probably are familiar with Kickstarter, the large fundraising platform. Product teams can go to Kickstarter, create a project, set a funding goal and start collecting money from others who believe in the idea. Kickstarter is essentially a third party that sits between product teams and supporters. This means that both of them need to trust Kickstarter to handle their money correctly. If the project gets successfully funded, the project team expects Kickstarter to give them the money. On the other hand, supporters want their money to go to the project if it was funded or to get a refund when it hasn't reached its goals. Both the

product team and its supports have to trust Kickstarter. But with smart contracts we can build a similar system that doesn't require a third-party like Kickstarter. We can program the smart contract so that it holds all the received funds until a certain goal is reached. The supporters of a project can now transfer their money to the smart contract. If the project gets fully funded, the contract automatically passes the money to the creator of the project. If the project fails to meet the goal, the money automatically goes back to the supporters. As smart contracts are stored on a blockchain, everything is completely distributed. With this technique, no one is in control of the money.

Why should we trust a smart contract? because smart contracts are stored on a blockchain, they inherit some interesting properties. They are immutable and they are distributed. Being immutable means that once a smart contract is created, it can never be changed again. So no one can go behind your back and tamper with the code of your contract. And being distributed means that the output of your contract is validated by everyone on the network. So a single person cannot force the contract to release the funds because other people on the network will spot this attempt and mark it as invalid. Tampering with smart contracts becomes almost impossible. Smart contracts can be applied to many different things, not just on crowd-funding. Banks could use it to issue loans or to offer automatic payments. Insurance companies could use it to process certain claims. Postal companies could use it for payment on delivery, and so on. Right now there are a handful of blockchains who support smart contracts, but the biggest and well known one is Ethereum. It was was specifically created and designed to support smart contracts. They can be programmed in a special programming language called Solidity. This language was specifically created for Ethereum and uses a syntax that resembles Javascript. It is worth noting that Bitcoin also has support for smart contracts although it's a lot more limited compared to Ethereum. So now we know what smart contracts are and what problem they solve.

When a product is discharged from a manufacturer, it has certain pre-conditions including temperature conditions, expected date of delivery, fragility etc. When we use blockchain for supply chain management, we make all these conditions a part of the smart contract which is to be strictly adhered to by all the intermediate carriers. This solves the problem of multiple peer to peer communication and makes blockchain a truly effective solution for supply chain management.

The Journey of the Coffee Bean

To understand better how a Supply chain transaction looks like with the help of blockchain, let us look at another example.

If you think your coffee was made in a coffee maker in under two minutes, think again. The coffee bean's journey has been long and It has passed through many farmers, traders keepers etc. It has always been near impossible to track where or how your coffee was made until recently when blockchain technology took over and brought accountability into the supply chain. Today you can trace your coffees journey from Brazil, India or Indonesia from the very beginning. Let's look at this process from the start:

1. **The planting process** - the farmer plants the coffee seed in the best possible soil to protect it from harsh sunlight and nourishes it with water and supplements. After the seed is ready, the seed is then passed on for inspection.
2. **Inspection** - the inspector records all of the coffee details of the bean, including the type fertilizers used, the barn It came from etc. and then stamps the tamper-proof origins certificates digitally then registration details and crop information such as variety temperature and humidity are recorded finally after getting stamped with a quality certificate, the bean is sent off to the next phase.
3. **Transportation** - the journey begins with the insurance. After a long journey, the coffee bean reaches the warehouse with a lot of other coffee

'With Blockchain, we can be sure that everyone that is entitled to be paid in the supply chain process, is paid in real time'

beans from all over the world. Blockchain ensures that the coffee bean gets delivered to the right address. All the workers and handlers get paid in real time and importer gets his delivery on time.

It's all because of blockchain that you are sure of the authenticity of the origins of the coffee bean. It has brought transparency into an age old system of management. Blockchain ensures that nothing gets in the way of brewing your perfect shot of espresso.

Conclusion

The standard problems that blockchain still faces include that of security and the existing mentality of people when it comes to traditional architectures. A lot of money and time has been spent by the large companies to synthesise a procedure and expecting the whole system to change overnight is perhaps far fetched. However, there is no denying as to how easy and time saving the entire process of supply chain management will be made by introducing aspects of blockchain into it. It ensures tamper free exchange of data and even ensures that the shareholders and transitory workers get paid for the work they do in real time. Through smart contracts, we can be sure that all the pre-conditions and requirements for the product are met. Security is also a huge issue as no one would want worldwide information to be hacked especially when the information is as vital as that of goods and products which the world runs on. So in conclusion, it is safe to say that blockchain is still an incipient concept, but one with great and remarkable possibilities and in the near future, it might bring in something similar to a second global industrial revolution.

Blockchain Applications in Healthcare

Probably the most crucial application of the technology, it has the potential to literally save lives

In the current state of affairs of the health service industry, all records are being collected and stored in a disjointed manner. Let's look at the example of a patient who has been admitted into a hospital. The hospital has to rely on the patient to be able to provide accurate information about their medical history, any allergic reactions to medicines in the past, current medication lists, etc. If the patient is in a critical condi-

tion, then the healthcare provider will have to rely on the family members/caregivers to provide said information. What about the emergency drugs, if any, needed for such patients? There is no real medium to confirm the source of the drugs procured or to track the delivery of the drugs from its point of origin to the hospital drug store.

If blockchain technologies are applied to the healthcare industry, service providers might potentially be looking at a method of having accurate information about their patients. This is just the tip of the iceberg. There is so much more that can happen if blockchain and the entire healthcare industry join hands.

While critics of blockchain will point out that as a technology it is difficult to adopt and put into use, the truth is that it can exponentially change the face of the healthcare industry in more than one way. Here's how:

EHR or Electronic Health Records

Let's revisit the example we began with. When a patient is admitted into a hospital, they are asked about their current and past medical history. Forms are filled at the counter at the entrance. Then the patient is taken in for testing, where a medical officer will ask similar questions yet again. Finally, once the patient lands up in a ward/bed, the doctor on duty is bound to ask questions that sounds irritatingly similar to the questions asked and already answered multiple times in the same day.

Truth being said, the hospital staff does this questioning and re-questioning because it is their policy and is part of the protocol. But it became part of the protocol for one simple reason - they had to be sure about the information they were taking down and they simply didn't trust their current method of information gathering. EHR or Electronic Health Records, which is currently the favoured method of collecting patient records and data, is not effective when it comes to multiple institutions. In reality, patients end up leaving scattered medical records over multiple hospitals and healthcare centers over the years.

With blockchain technology, the medical records of a patient (both current and historic) are owned by the patient and can be shared with medical care practitioners by using a public key that the patient can share with the hospital upon their arrival. Blockchain can help streamline the patient data and make it accessible to the patient as well as health care providers.

Given that blockchain is based on the premise that it is immutable, the trust factor is also higher than for the current system. Doctors should be

able to verify the source of the data that they have access to and can trust its validity.

Billing and insurance fraud

When you are admitted in a hospital, you completely and fully rely upon your doctor to provide you with the best care. Once your bill arrives, you rely upon your insurer to communicate with your healthcare institution and do the needful. You trust everyone in the system to do their job and you continue paying premiums every month to your insurer to stay covered and hope for the best medical care any time you need it. Little do most of us know that a significant chunk of medical insurance is lost to fraud. There are people out there who extort money from the system by indulging in fraudulent methods of collecting insurance. This could be done by falsifying records or by prescribing methods of treatment that are unnecessary for the patient in question.

Blockchain relies on nodes of information that are linked to each other. Every time a node is added, information automatically gets updated on all other previously linked nodes. Given this nature of the technology, a person having access to the network will see the same information as anyone else with the same access key. If the government were to make it

Most insurance fraud cases are from medical or health insurance which can be effectively prevented using blockchain technology

mandatory for all medical insurance to be on a blockchain; medical insurance fraud would come to a standstill. All information about a patient from the time of admission into the hospital until their return home would be documented and readily available to healthcare practitioners, institutions and medical insurance companies alike. This would mean that a fraudster could no longer rely on medical billing personnel to falsify bills and other related information. Furthermore, blockchain requires all information to be time-stamped and immutable. So even if tampering were to occur, it can be traced back to the fraudster.

Drug traceability and improving compliance

The pharmaceutical industry is an extremely large and sometimes ineffectively monitored one. When it comes to judging the efficacy of a drug, it largely has to do with the chemical composition of the drug in question. When a patient goes into a pharmacy, they place full and complete trust in the pharmacist to give them a drug that is apt and safe for use. The pharmacist places trust in his one level up (the distributor) to have provided them with a safe drug with a trusted source of origin. The distributor trusts his one up, so on and so forth. The whole industry is currently modeled on the 'one up and one down' system. Multiple levels of the drug creation isn't documented

Providing drug traceability feature to consumers will increase transparency and the people's trust in the sector which has been shaken in recent times

anywhere and made accessible to everyone in the system. Blockchain can help remedy this situation.

Blockchain technology can help track a drug from the time of its inception as an idea. So right from the nascent stages of animal testing, results of tests can be recorded on the blockchain and be available to the doctor who is prescribing the medicine to his/ her patient. Since the information is time stamped and tamper-free, the source of origin is known to everyone in the chain. This becomes even more important in the case of customised medication. While the idea of customising medicines based on gene therapy is not as widespread today, it could well be the face of modern medicine in the years to come.

For instance, white blood cells from Patient A can be sent from the hospital to a lab miles away to create a medication suited specifically to A's genetic type. The creation of the drug would depend on the white blood cells being transported and shuffled back and forth between a number of labs. If there is no clear traceability, the drug that becomes available could be ineffective for Patient A, could be a counterfeit, or worse could be based on white blood cells taken from Patient B (patient sample mix ups). Blockchain could help put the drug's entire lifecycle in blocks that are viewable by everyone involved in the procedure of creating the drug.

Another extremely important aspect of drug traceability is stopping counterfeit drugs from entering the supply chain. Given that everything in blockchain is time-stamped and immutable, tampering is impossible. This would mean that fraudsters couldn't unload real drugs and replace them with counterfeit drugs without the system catching it. Even if they did try, the crime could be traced back to them. Also, in case of delayed shipments, blockchain could help in determining which party last handled the drugs. This will help in speeding up the process of the drugs reaching their intended destination.

Clinical trial

The process of getting a new drug into the market is usually an extremely long and tedious one. Before a drug receives approval from the regulatory board, it has to undergo various phases of testing. Right from testing on animals to finally being tested on humans, the collection of data is a logistical nightmare for everyone involved. Let's not even begin to debate the chances of data tampering that can happen when there are multiple levels of personnel involved in research that is worth millions or more. While

there are heavy fines imposed on companies/ individuals who indulge in data falsification, sometimes they could be victims of simple clerical errors. While the current system of data collection has proven almost effective over the years, blockchain could well be the solution. With its property of linking immutable data, it could help verify the source of the information as well as it's veracity. Add to this the fact that it makes data almost impossible to lose. So even the tiniest of observations from a larger clinical trial will get logged for future reference.

With every passing day, the government keeps increasing the auditables for clinical research and trials. Using a technology like blockchain can help pharmaceutical companies have a ready paper trail and a tamper proof one at that. Other than this obvious advantage, there are other reasons why distributed ledger technology (DLT) could prove useful for the healthcare industry as far as drug testing and trials are concerned.

Blockchain technology can help in easing the tedious process of clinical trials for regulatory approval

When it comes to clinical trials, medical records of the subjects are crucial. These records need to be maintained and studied accurately for best results. The traditional method of saving and sharing data is tedious and opaque. Blockchain can help make this method digitised, uniform across the globe, and transparent. There have been instances in the past where drugs have been deemed safe for children, but research in the later years have proven otherwise. Such fatal errors can be avoided by using a more effective method of data sharing such as blockchains or DLTs. The transparency of shared data could also mean that researchers can share their findings with other scientists who can easily verify the source of origin of the data provided, as well as add their own summations and suggestions to the initial findings of their peers. This would mean better and more effective drugs could enter the mainstream market sooner than they did in the years gone by.

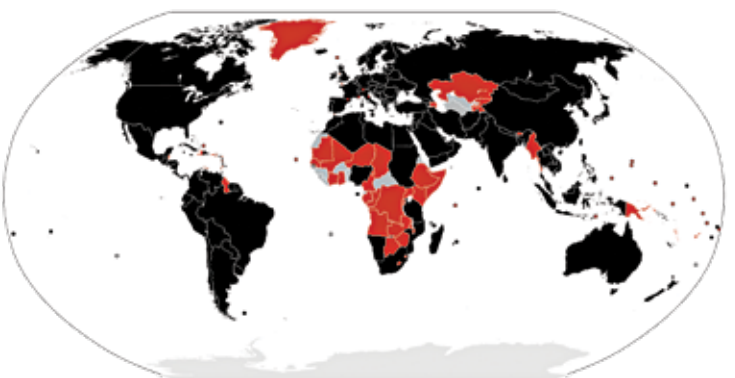
One of the biggest advantages of using blockchain for clinical research is that it costs lesser than traditional methods of data collection and sharing. By using blockchain technology, companies can distribute their research work

among a larger network thus leading to faster and more effective results. Lower overheads would mean a larger number of drugs could be synthesised simultaneously without affecting the quality of the final product.

Case study

The US body of CDC (Centers for Disease Control) has recently discussed the possibility of launching a test to see the effectiveness of Blockchain as far as disaster relief is concerned. According to CDC officials, the ability of medical personnel to collect medical data in real-time becomes even more important in situations where life threatening viruses are concerned. If accurate data is collected from the ground level and shared with researchers who may be sitting miles away, but is done so in a matter of minutes and hours, it could help save a number of lives.

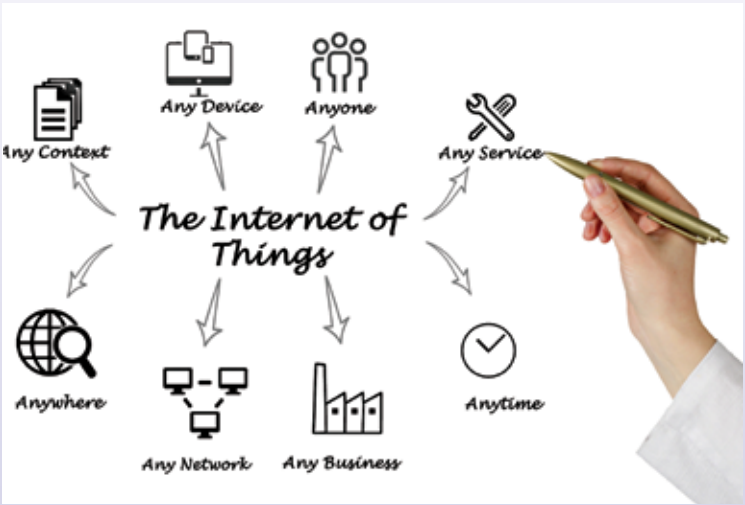
In the current scenario, when samples are collected from ground zero of viral outbreaks, the data is pooled together and then sent to institutions and organisations that will verify the data, clean it up and then reveal its findings. This entire process is lengthy and may not be wholly accurate either given the lack of transparency between the various layers and levels of people included. By applying blockchain technology, the CDC is hoping to open up possibilities of collecting information from researchers working on the ground and those working in the lab as well as law-making agencies. This would help the CDC find solutions to life threatening situations faster, thus enabling timely help for those infected. It will also help contain the outbreak and confine it to a smaller area.



Capturing and sharing real-time data of a global pandemic could mean the difference between life and death and blockchain offers the perfect solution for this

Healthcare industry needs more transparency

The entire healthcare industry functions on the basis of inter-operability. Traditional methods of data collection and sharing that have been employed in the last few decades, even though digitised, have not proven to provide transparency to all layers of healthcare personnel involved. If medical data has to be put to its maximum use, there needs to be provisions made for inter-operability and data portability. Given the fact that distributed ledger technology like blockchain has digitised signatures added to everything, verifying its source becomes an easy task. This authentication allows the industry to ensure that all medical records and resulting data are cryptographically secure. The constantly looming threat of hackers, falsified data, lost data and the likes could be silenced with the application of blockchain in the healthcare industry.



Blockchain & the Internet Of Things

Internet of Things is an up and coming avenue. It provides unthinkable possibilities for the future. However, it comes with its own share of problems and restrictions. Is the new concept of Blockchain a once and for all solution to all these challenges?

Introduction

By now we have an idea of what Blockchain is and how it is implemented in a distributed system. Let us revise the salient features of a blockchain structure that make it stand out from all other data communication models:

1. **Distributed ownership** – By definition, a blockchain is a distributed transactional ledger that is recorded chronologically and publicly. This feature differentiates it from all other existing transaction models. Tampering around is not a possibility in blockchain as all the data is publicly distributed.
2. **Hashing mechanism** – Every block of a blockchain system comprises of a 'hash' which is like its digital fingerprint. This fingerprint gets altered every time a change is made in the dataset of the block. Also, every block has a hash address component that keeps track of the last hash. This is done to maintain a digital continuity in the ledger and to make sure that no block is tampered with. Because if any block is tampered with, its hash will change and thus render the hash address of the next node useless, hence nullifying the entire continual chain. This security measure is one of the main reasons that it has gained such popularity and give a perfect platform for the exchange of cryptocurrency like Bitcoin.
3. **Proof-Of-Work** – Nowadays, we have computers capable of an insane amount of computation in almost no time. Thus, it is possible to bypass the re-hashing mechanism of the Blockchain system by calculating the new possible hash and fooling the next block into believing there has been no tampering. As a failsafe to this loophole, Blockchain implements an elegant solution known as 'proof-of-work' that gives a delay of 10 minutes every time a new hash is created. This assures that the blockchain is truly tamper free. All these features make blockchain the safest and best possible solution for digitisation of data assets and public transaction ledgers.

The internet is evolving into a new technology paradigm based around smart systems, blockchain platforms, and IoT. In the coming years, these technologies will interact and converge in new and unpredictable ways. The convergence of IoT and blockchain will be a major part of this evolution, enabling new automated service systems and business models. Being that as it may, there are still many unresolved issues regarding Blockchain that remain. Internet of Things is the merging of our engineered physical environment with information systems to create smart, adaptive objects and environments. Blockchain is a fast-growing, increasingly complex network

'Blockchain might be the solution required to solve the problem for connecting all devices to a single platform'

of connected physical systems that are able to process information and communicate peer-to-peer in order to enable common services. The devices today are becoming increasingly ubiquitous ranging from autonomous vehicles to sensors monitoring industrial processes to smart homes and smart cities. IoT is here to stay and according to a survey, it will connect about 26 billion devices by 2020. The development of an IoT infrastructure to our economies will probably be the greatest engineering challenge of our time. There are a variety of problems that come with these complex infrastructures and security is one of the biggest of these problems. Before mainstream Internet of Things adoption can really take hold in a safe and sustainable fashion, these, among other issues, will need to be resolved. Let us have a thorough look as to how Blockchain might be a permanent solution to some of the problems such an infrastructure faces. Also we shall look at some clever ways in which Blockchain is already being implemented by some startups.

Why BlockChain?

The Blockchain is a secure distributed database for recording transactions – millions of computers networked to create a distributed database for recording and authenticating exchange of value. With the blockchain, value of any kind can be exchanged directly peer to peer without a centralized authority to record and validate the transaction. The Blockchain can

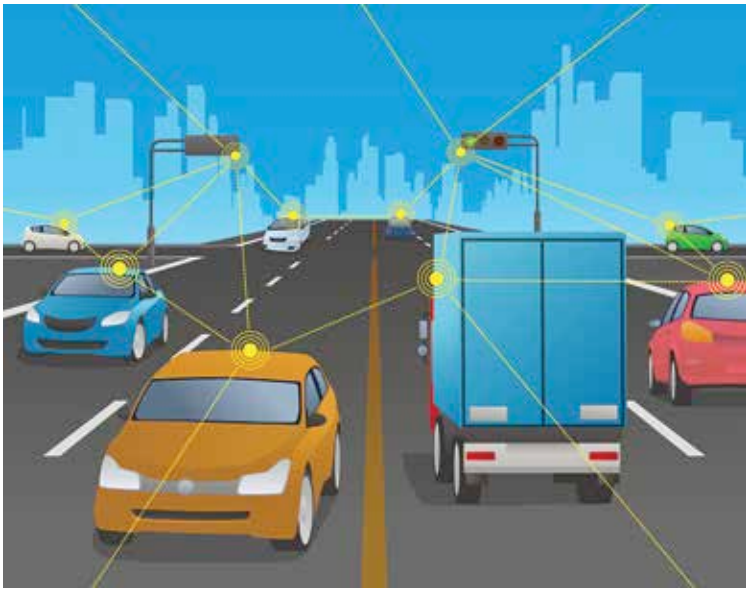
'SLOCK is a startup which makes smart locks based on the concept of Blockchain'

provide an automated and secure transaction infrastructure for next generation IoT systems in its capacity to track billions of connected devices and enable the frictionless processing of transactions and coordination between devices. This decentralized approach could eliminate single points of failure, bottlenecks and make data and transactions more secure, thus creating a more resilient ecosystem for devices to run on. Blockchain would also automate transactions enabling fully autonomous service systems to run without any manual work component. This would lead to a reduced cost and reduce settlement time from days to seconds. Bitcoin magazine states that; "Smart contracts, a feature of 'Bitcoin 2.0' technologies such as Ethereum, could soon operate the Internet of Things, control objects in the physical world, and power a new decentralized version of the sharing economy, for example sharing services similar to Uber and Airbnb that operate in pure P2P mode without centralization management" This holds true because leveraging Blockchain for IoT offers new ways to automate business processes and build distributed autonomous service systems. The true value of underlying technology of Blockchain has only just begun to be explored, and potential applications to the Internet of Things and Smart Systems are vast.

Blockchain and the Internet of Things

Blockchain is likely to disrupt many industries in the coming five to ten years. These are some of the industries it's already disrupting

1. **Banking and Payments** – some people say that the blockchain will do to banking what the internet did to mass media. Blockchain technology can be used to give access to financial services to billions of people around the world including those in third world countries who don't have access to traditional banking. Technologies like Bitcoin allow anyone to send money across borders almost instantly for very low fees. 'Abra' is a startup that is working on Bitcoin based remittance services and many banks like Barclays are also working on adopting blockchain technology to make their business operations faster, more efficient and secure. Banks are also increasingly investing in blockchain projects and startups. IBM predicts that about 15% of banks would have started using the blockchain by the end of 2017.
2. **Cyber Security** – Although the blockchain ledger is public, the data is verified and encrypted using advanced cryptography(as already discussed). This way, the data is less prone to being hacked or changed without authorization. The Blockchain eliminates the need for middlemen, making it more efficient than many legacy and traditional systems.
3. **Networking and Internet of Things** – Samsung and IBM are using blockchain technology for new concepts called 'adept' which will create a centralized network of IoT devices operating like a public ledger for a large number of devices. It would eliminate the need for a central location to handle communications between them. The devices would be able to communicate with each other directly to update software, manage bugs and monitor energy usage.
4. **Insurance** – The global insurance market is based on trust management. Blockchain is a new way of managing trust and can be used to verify many types of data in insurance contracts like the insured person's identity. So-called Oracles can be used to integrate real world data with blockchain.
5. **Smart Contracts** – This technology is very useful for any type of insurance that relies on real world data, for example crop insurance. 'Eternities' is one blockchain project that is building tools that are useful in the insurance industry.
6. **Public and Private Transportation** – The Blockchain can be used to create decentralized versions of peer-to-peer ride-sharing apps allowing both car owners and users to arrange terms and conditions in a secure way without the need of third-party providers. Startups working in this area include 'Arcade City' and using Blockchain for building such



'Blockchain can be implemented into public and private transportation and hence save a lot of time and money'

a wallet can allow car owners to automatically pay for parking highway tolls and electricity/fuel top-ups to the vehicle.

7. **Cloud Storage** – Data on a centralized server is inherently vulnerable to hacking, data loss or human error. Using blockchain technology allows cloud storage to be more secure and robust against attacks. 'Storage' is one example of a cloud storage network using blockchain technology.
8. **Charity** – Complaints in charity space include inefficiency and corruption which prevent money from reaching those who are meant to have it. Using blockchain technology to track donations can let you be sure that your money is going to end up in the right hands. Bitcoin based charities like 'Big Game foundation' use Blockchain to let donors see that the intended party has received the funds.
9. **Voting** – Probably one of the most important areas of society that blockchain might disrupt is voting. The 2016 US election was not the first time certain parties were accused of rigging election results. Blockchain technology can be used for voter registration and identity verification and electronic vote counting. It would ensure that only legitimate votes

are counted and no votes are changed or removed creating an immutable publicly viewable ledger of recorded votes. This would be a massive step forward in making elections truly fair and democratic. 'Democracy Earth' and 'Follow my Vote' are two startups aiming to disrupt democracy itself by creating blockchain based online voting systems for governments.

10. **Retail** – When you shop you trust the retail system of the store or the marketplace. Decentralized blockchain based retail utilities work differently. They connect buyers and sellers without middlemen and associated fees. In these cases trust comes from smart contract systems which eliminates the need for a middleman.

Conclusion

Developing solutions for Internet of Things requires unprecedented collaboration between all the shareholders and the devices in the transaction. All devices need to be integrated and connected as a whole to be a part of the Internet of Things architecture. Such a collaboration is quite possible, but expensive and very time consuming.

However, one of the biggest problem the actualization of Internet Of Things faces is a threat to security. For such an integrated system to exist where all the devices are compatible with each other, there needs to be unshakable trust and security which the enterprise is based upon. Blockchain has not yet matured to offer such a safe environment for vital data. Imagine the horrific situation where such vital data gets hacked. The men-

'If security is not implemented in Blockchain enterprises, it would mean compromising not just vital data, but the very lives of people'

tality of people about Blockchain is also a big hindrance. Most systems and companies are based of traditional architecture and a lot of money and time has been invested in setting them up. To get these companies to change their entire hierarchy is one of the biggest challenges that Blockchain has to overcome in today's day and age.

Security needs to be built in as a foundation of IoT systems, with rigorous validity checks, authentication, data verification and all the data needs to be encrypted. For applications, software development organizations need to develop code with a universal standard and give priority to threat detection, analysis and testing. Without a solid bottom-up approach, we will create more threats with every device added to the IoT. The dream is hard to achieve, but not impossible. Thus, we can conclude that blockchain technology is an attractive option if we need to overcome the drawbacks that IoT faces currently.

Criticisms of Blockchain

Not all is hunky dory, there is always a flip side to every coin. Let's understand the faults in the stars of blockchain.

When the internet in its current form began gaining popularity, media across the globe went into a frenzy. It has been a while since any other technology grabbed their attention as much. Ever since blockchain technology came into existence around seven or eight years back, it has been hogging a lot of limelight.

Blockchain is being touted as the next big thing. It is the system upon which, tech pundits are predicting, most future business applications will be built and streamlined. It will be the new method of data collection,

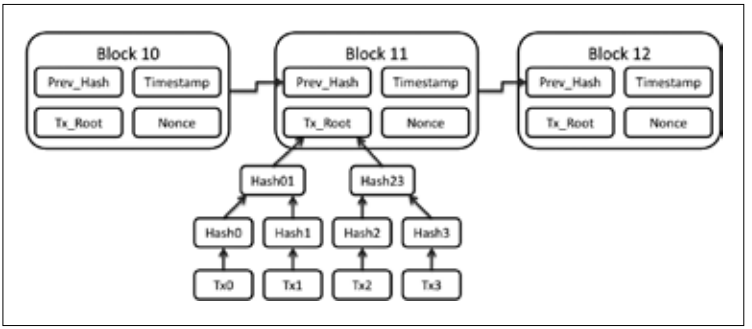
data safeguarding and even trading. While the last few years of success seen by companies like Bitcoin and Ethereum have convinced people about the merits of this technology, there have also been cases when people have lost millions because security levels of the tech leave much to be desired for. Here's a look at why this dynamic and rather interesting blockchain technology and its users might be posed with unique threats in the near future.

Is Blockchain One Giant Distributed Computer?

Every time you read about blockchain and how it works, one of the factors that jumps to the forefront is that the technology is dependent on a number of nodes that key in as well as save information at the same time. If your idea of how this works meant that all these nodes have a mutual relationship with each other, your idea isn't wholly accurate. In reality each node/computer downloads the same information and saves it in the same order. This means there is a lot of duplication, and this duplicated data stays for 'blocked' in this 'chain' for posterity. A large network of individuals/nodes accept that a transaction made is true and is verified. And furthermore all information about the said transaction will remain timestamped and tamper free on the chain that it is linked to.

Forever Is Costly:

Understanding how the blockchain works is important so that you can interpret one of its greatest flaws or drawbacks at the moment. Real estate, whether offline or online, has never come easy. By having to download all the information on a blockchain every single time, individual nodes are pressed for capacity. Take for instance Bitcoin, the largest company applying blockchain technology, perhaps the most popular of the lot too - currently their entire accumulated network history has crossed a cool 100 GB. Think about that. Even your costliest smartphones or cheaper laptops are going to get clogged with that kind of data on it. Bitcoin accumulated this data over a period of years. But to get a real picture of how problematic this issue can be, let's look at a newer entrant into this field. Ethereum is a relatively new company that has entered the business world with its promise of revolutionising the way smart contracts are built and worked upon. They have made quite a wave ever since their inception. Ethereum has already accumulated data north of 200 GB in a much shorter life span. Yep, you read it right. 200 GB. That's a lot of system space. Let's not even



Such an endless and ever growing chain will amount to terabytes of data increasing storage costs for existing and any new node added on the network

begin to mention the amount of electricity this whole network consumes. We will get to that soon.

The premise on which blockchain works is that everything that is linked on a blockchain is forever. All information is time-stamped and will remain in the system for posterity. However, unless there are immediate innovations made in the tech industry that allows for cheaper hard drive space, this might be far from true. There is an urgent need of increased access to system space, barring which the blockchain will not be able to reach its true potential. Inability to provide this extra space could mean jeopardizing already existing transactions on the blockchain too.

In order to make money off the blockchain business, nodes have to download all the data on their chains. A lot of users, much to their dismay, realised that payments would not come through until all of the information had been downloaded to their computers. In most cases this would mean a couple of days. And this isn't a feature advertised by blockchain companies (for obvious reasons). The growing network of this technology would only mean longer waiting periods for your moolah to hit your wallet.

Can Bitcoin Really Put VISA Out Of Business?

Think about the last time you went to the supermarket because you needed a snack. You pick up a bag of chips and head to the checkout counter. The counter is as busy as it can be on that particular day. You have to wait about 10 minutes to get to the counter, where you hand over your VISA. The card is swiped, receipt and bill printed,and you are on your way out of the store. Now picture the number of people across the globe who were

also using their cards while you were buying yourself a bag of chips. Don't think just about the folks in the same store as you. Think about a lady at the mall, friends at a movie theatre, patrons at a restaurant - all of them swiping their cards at the same time. Know how that is possible? VISA has a network strong enough to allow about 2600 transactions per second. Per second. That's a lot. And given the strength of the banking industry, that number is likely to keep increasing proportionally to the amount of funds pumped in to do so!

Let's superimpose this understanding onto blockchain and its supporting technology. If a blockchain network is made up of several nodes, then does it mean that the bandwidth of the network is the same as the speed of a single node? Well, as simple as that sounds, how do you determine which node to base your speed on? Regardless of how this bandwidth is calculated, what this actually means for the end-user is that until the data is recorded on all nodes in the system, the transaction cannot be verified and thus, cannot move forward. Given this calculation of sorts, blockchain technologies like Bitcoin are currently unable to provide for

Plastic currency such as VISA, MasterCard and AMEX aren't going to be rendered obsolete by blockchain technology anytime soon

more than 7 transactions per second (tps). Yep, 7 tps for Bitcoin vs 2600 for VISA. That's a lot of ground to cover.

Add to this the fact that bitcoins transactions are recorded only once in every 10 minutes. The entire idea behind creating blockchain also included quashing any digital double spend. Given that rollbacks are standard in these scenarios, the procedure includes waiting for 50 minutes to allow for all records across nodes to reflect any and all changes. Let's take you back to the initial supermarket scenario. What this would mean for you would be standing 50 minutes in a line to get a bag of chips. No real biggie, eh!

Security threats still exist albeit in a different fashion. Instead of hacking the entire server, hackers need to hack the systems of the top miners gaining a backdoor entry into the system

At the moment, the estimated number of active blockchain users around the globe is around one in a thousand people. If this number were to increase, even by a small percentage, the results could be nothing short of chaos.

Mining Woes:

Blockchain brings with it the concept of mining. You've obviously by now read about the role that miners play in the chain of events as far as this technology goes. Miners will usually have entire computer systems that are dedicated to a singular task - mining cryptocurrency. Their job is to create new blocks in a blockchain. The current payout for creating a new block for Bitcoin is 12.5 bitcoins (north of 92,00,000 INR). This payment will be halved when 210,000 blocks are added. This is estimated to happen in June 2020. It's no wonder then that mining has grabbed so many eyeballs. Everyone wants in, given that there is so much money at the end of the day.

Miners have to burn a lot of electricity to make this work. Not every block gets instant approval to be added at the end of a chain. The miners work hard to make a block 'beautiful' (get the math to add up) before it can be approved and reach monetary potential for its creator. Given that new blocks cannot be added more than once in 10 minutes to avoid transaction rewriting, a lot of energy is consumed in that wait time by n number of miners trying to shake down blocks to create one beautiful one! The energy

consumed by miners is usually the amount that could help power a relatively medium sized town. Add to this the fact that there is specialised equipment for mining that comes at a cost.

Given that blockchains like bitcoin want to avoid a 51% attack, they will create excessive number of miners to ensure that a mining majority of nodes/individuals does not exist. A majority attack or 51% attack can be possible only if majority of the computing needs of a network come from a single/singular group of providers, who then control the hashrate of the blockchain. This could give them the power to indulge in unlawful mining which would eventually lead to unsolicited double spends.

What this means in simple terms for blockchain is that if the price of electricity were to drastically increase in the years to come, very few companies or groups would be able to afford mining. This would put them at the risk of being controlled and dominated by said groups and open themselves up to the possibility of majority attacks and double spends on a regular basis.

Open To External Attacks:

Blockchain is based on a large network of nodes. These nodes have the same information stored on them. This would mean that the information, even if

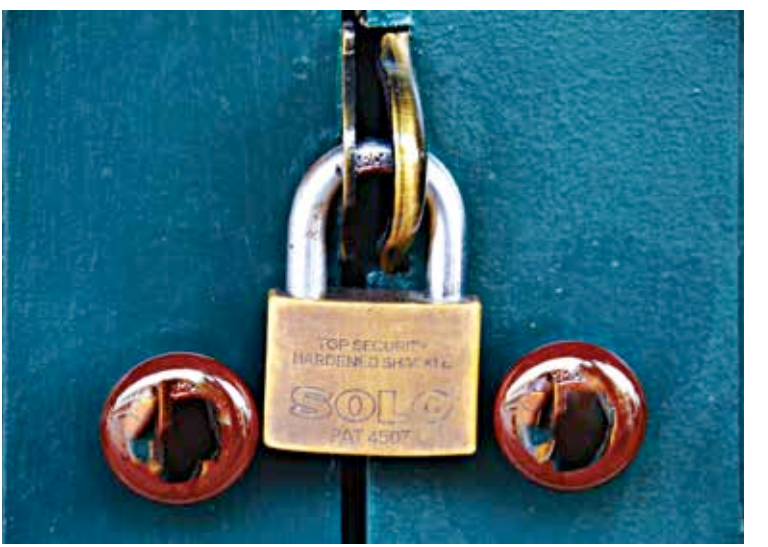
Having open nodes also leaves room for hackers to infiltrate networks

wiped out from one server would stay safeguarded because it has so many other copies. But what about control on these nodes? If you were to look at the top 20 mining groups, you would notice that the top earners are situated in close geographical boundaries. This could leave them susceptible to external attacks. Gaining control over computers from 4 or 5 top mining groups could give a terror group the chance of carrying out a majority attack on the miners and blockchains of the world.

Too Much Financial Transparency:

The anonymity and financial transparency of blockchains are being celebrated by users and trade pundits alike across the world. But how much is too much? Picture a world where cryptocurrency and blockchains have weeded out traditional currency. You are now using digital money to buy anything from toothpicks to a new television set. In such a scenario, if you were to send money to say your parents, they would get access to your previous and future transactions. They will now know of the hotel room you booked and the amount you lost gambling at a casino - not exactly the kind of information you want to discuss with them!

The issue with this much financial transparency would be lack of privacy. Your private life is now available for friends or family members to comb



Having your private financial information out there has far reaching effects

through once they are linked to your blockchain. While this kind of transparency is more of a cosmetic problem for individuals, the repercussions it has on the ledgers of larger companies is very real. They could be sending out information with regards to tenders and other such sensitive data to anyone linked to their blockchains. While private blockchains seem to have solutions for these issues, a public blockchain like Bitcoin is not very useful for companies with big bank balances and multiple financial transactions.

Regulating blockchain technology is going to be a nightmare

Customer Protection Isn't Foolproof:

Eventually any business will do well only if the end user is happy with the product. When the product in question is blockchain technology, the customer along with feeling bouts of happiness should also feel secure given that his/her money and data is also being protected. But are all transactions on a blockchain really secure?

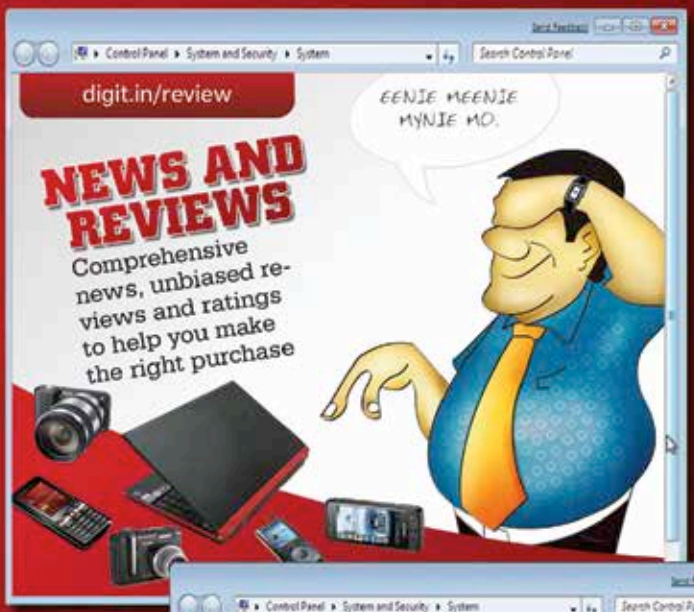
When it comes to blockchains, individuals have the right to determine how much information they want to verify and add to the blockchain. They could choose to add everything from land titles to medical records or even cryptocurrency. The biggest problem with this arrangement is that once a transaction is verified, it is difficult or close to impossible for it to be rolled

back. Picture this, you enter a transaction into the blockchain, only to realise a while later that the deal with the other party has gone sour and has fallen through. By this time, the transaction is linked to the blockchain and proof of ownership has been transferred to the name of the other party. The only way to remedy this is if both (or in some cases many/all) parties involved are willing to verify that the transaction has to be made null and void.

Some trade technologies that are based on blockchains have started suggesting multiple signature transactions or having a clause in the contract that allows for the use of an arbitrator to settle such disputes.

In Conclusion:

Creating federal laws to regulate blockchain technology is going to be a logistical nightmare for regulators. That being said, for the technology to be implemented, there is an immediate need for effectively laws that cater specifically to it. Industries like supply chain management or financial services are more likely to start using blockchain on a regular basis in the near future. It might take longer for other industries to follow suit. People need to be educated about blockchains and how it can help them and change the way they do business or even everyday transactions. It's only when they are aware that they will open up their minds to the possibility of adopting a system so radically different from the one they are currently using.



All this and more in the
world of Technology

VISIT NOW digit.in

RNI REGN. NO. DELENG/2001/03791