ABSTRACT

Blockchain (BC), the technology behind the Bitcoin crypto-currency system, is considered to be both alluring and critical for ensuring enhanced security and (in some implementations, non-traceable) privacy for diverse applications in many other domains - including in the Internet of Things (IoT) eco-system.

Intensive research is currently being conducted in both academia and industry applying the Block chain technology in multifarious applications. Proof-of-Work (PoW), a cryptographic puzzle, plays a vital rôle in ensuring BC security by maintaining a digital ledger of transactions, which is considered to be incorruptible.

Furthermore, BC uses a changeable Public Key (PK) to record the users' identity, which provides an extra layer of privacy. Not only in cryptocurrency has the successful adoption of BC been implemented but also in multifaceted non-monetary systems such as in: distributed storage systems, proof-of-location, healthcare, decentralized voting and so forth.

Recent research articles and projects/applications were surveyed to assess the implementation of BC for enhanced security, to identify associated challenges and to propose solutions for BC enabled enhanced security systems.

Issues with Current Banking System

Any existing system will have some issues. Let us look at some of the most commonly faced issues with the Banking system:

- **High Transaction Fess**

Let's look at an example to understand this issue better:

Here, Chandler is sending $100 to Joe but it must pass through a trusted third party like a Bank or Financial service company before Joe can receive it. A transaction fees of 2% is deducted from this amount and Joe only receives $98 at the end of the transaction. Now this may not seem a big amount but imagine if you were sending $100,000 instead of $100, then the transaction fees also increases to $2,000 which is a big amount. As per a report from SNL Financial and CNNMoney, JPMorgan Chase, Bank of America and Wells Fargo earned more than $6 billion from ATM and overdraft fees in 2015.

- **Double Spending**

Double-spending is an error in digital cash scheme in which the same single digital token is spent twice or more. To help you understand this problem better, let me give you an example:

Here Peter has only $500 in his account. He initiates 2 transactions simultaneously to Adam for $400 and Mary for $500. Normally this transaction would not go through as he doesn't have sufficient balance of $900 in his account. However, by duplicating or falsifying the digital token associated with every digital transaction, he can complete these transactions without the needed balance. This operation is known as Double Spending.

- **Net Frauds and Account Hacking**

In India, the number of fraud cases related to credit/debit cards and Internet banking was 14,824 for the year 2016. The net amount involved in these frauds was Rs 77.79 crore, of which Rs 21 crore was from internet frauds and Rs 41.64 crore was from ATM/debit card-related frauds.

- **Financial Crisis and Crashes**

Imagine giving all your saving to someone you trust only to know that they have gone and lost it somewhere else. That's what happened in the 2007-08 when Banks and Investment Organisations had borrowed heavily and lent it as subprime mortgages to people who could not even pay back these loans. This in turn lead to one of the greatest financial crisis ever seen and was estimated to have caused losses close to $11 Trillion ($11,000,000,000,000) worldwide. This was just one of the most popular examples, how often have we heard of Banks and Financial service companies crash due to internal frauds? The whole third-party system is something that is built on blind trust on the middle man.

We have seen some of the most common problems faced by everyone. Wouldn't it be great to have a system that overcame these problems and provided us with a That's exactly what Blockchain Technology does.

How does Blockchain solve these issues?

Below are some of the ways through which the Blockchain technology tackles the above mentioned issues:

- **Decentralized System**

The Blockchain system follows a decentralized approach when compared to banks and financial organisations which are controlled and governed by Central or Federal Authorities. Here, everyone who is part of the system becomes equally responsible for the growth and downfall of the system. Rather than one single entity holding the power, everyone who is involved with the system holds some power.

- **Public Ledgers**

The ledger which holds the details of all transactions which happen on the Blockchain, is open and completely accessible to everyone who is associated with the system. Once you join the Blockchain network, then you can download the complete list of transaction since its initiation. Even though the complete ledger is publicly accessible, the details of the people involved in the transactions remains completely anonymous.

- **Verification of Every Individual Transaction**

Every single transaction is verified by cross-checking the ledger and the validation signal of the transaction is sent after a few minutes. Through the usage of several complex encryption and hashing algorithm, the issue of double spending is eliminated.

- **Low or No Transaction Fees**

The transaction fees are usually not applicable but certain variants of Blockchain do implement certain minimal transactions fees. These transaction fees are however relatively quite less when compared to the fees implied by banks and other financial organisations. If a transaction needs to be completed on priority then an additional transaction fees can be added by the user so as to have the transaction verified on priority.

INTRODUCTION

What is Bitcoin?

Before we go on to understand what is Blockchain, it is important that you understand what is Bitcoin:

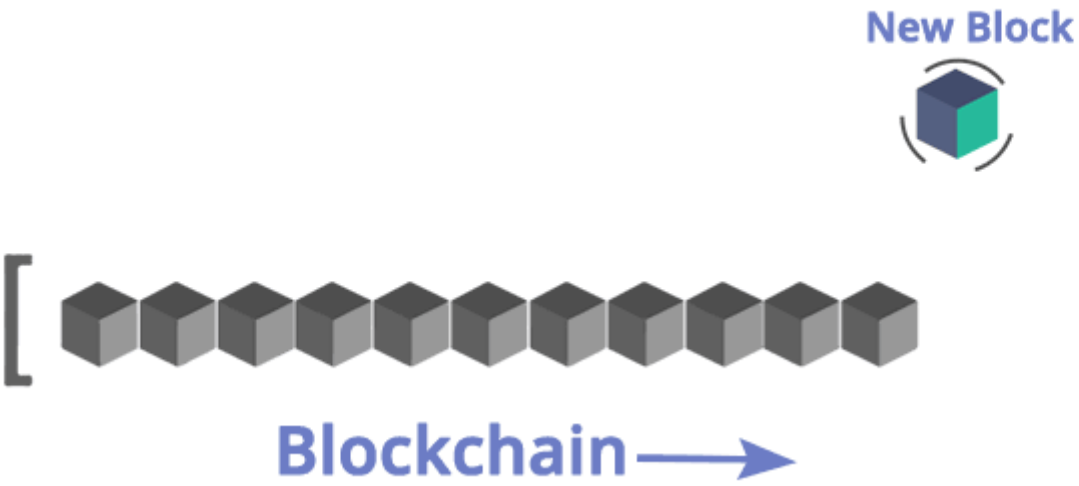
Bitcoins are a crypto-currency and digital payment system invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto. That means they can be used like a usual currency, but don't physically exist like dollar bills. They are an online currency which can be used to buy things. These are similar to "digital cash" that exist as bits on people's computers. Bitcoins exist only in the cloud, like Paypal, Citrus or Paytm. Even though they are virtual, rather than physical, they are used like cash when transferred between people through the web.

The Bitcoin system is peer-to-peer network based and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a Blockchain. Since the system works without a central repository or single administrator, Bitcoin is called the first decentralized digital currency.

Bitcoin production makes them a unique currency. Unlike normal currencies, Bitcoins cannot be created as needed. Only 21 Million Bitcoins can be created, of with 17 million have already been created. Bitcoin get created whenever a block containing valid transactions is added to the Blockchain. This is the only means for creating Bitcoins and through various

mathematical and encryption algorithms we ensure no fake Bitcoins are created or circulated. Let us now understand more Blockchain.

What is Blockchain?



Blockchain can be called the spine of the entire crypto-currency system. Blockchain technology not only helps with the users perform transactions using crypto-currencies but also ensures the security and anonymity of the users involved. It is a continuously growing list of records called blocks, which are linked and secured using cryptographic techniques. A Blockchain can serve as "an open and distributed ledger, that can record transactions between two parties in a verifiable and permanent way." This ledger that is shared among everyone in the network is public for all to view.This brings in transparency and trust into the system.

A block is the 'current' part of a Blockchain which records some or all of the recent transactions, and once completed goes into the Blockchain as permanent database. Each time a block gets completed, a new block is generated.

The Blockchain is typically managed by a peer-to-peer network, collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and a collusion of the network majority. Transactions once stored in the Blockchain are permanent. They cannot be hacked or manipulated. We will learn more about this once we get into the concepts of Blockchain.

Blockchain being relatively a new technology, a representative sample of research is presented, spanning over the last ten years, starting from the early work in this field. Different types of usage of Blockchain and other digital ledger techniques, their challenges, applications, security and privacy issues were investigated. Identifying the most propitious direction for future use of Blockchain beyond crypto-currency is the main focus of the review study. Blockchain (BC), the technology behind Bitcoin crypto-currency system, is considered to be essential for forming the backbone for ensuring enhanced security and privacy for various applications in many other domains including the Internet of Things (IoT) eco-system. International research is currently being conducted in both academia and industry applying Blockchain in varied domains.

The Proof-of-Work (PoW) mathematical challenge ensures BC security by maintaining a digital ledger of transactions that is considered to be unalterable. Furthermore, BC uses a changeable Public Key (PK) to record the users' identity that provides an extra layer of privacy. The successful adoption of BC has been implemented in diverse non-monetary systems such as in online voting, decentralized messaging, distributed cloud storage systems, proof-of-location, healthcare and so forth. Recent research articles and projects/applications were surveyed to ascertain the implementation of BC for enhanced security and to identify its associated challenges and thence to propose solutions for BC enabled enhanced security systems. The knowledge domain of the research is in the realm of the digital ledger, specifically, in Blockchain and crypto-currency.

Technology Fundamentals of Blockchain

A Blockchain comprises of two different components, as follows:

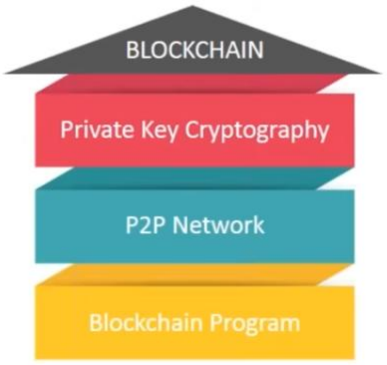
1. Transaction:

A transaction, in a Blockchain, represents the action triggered by the participant.

2. Block:

A block, in a Blockchain, is a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation, etc.

Blockchains are built from 3 technologies:



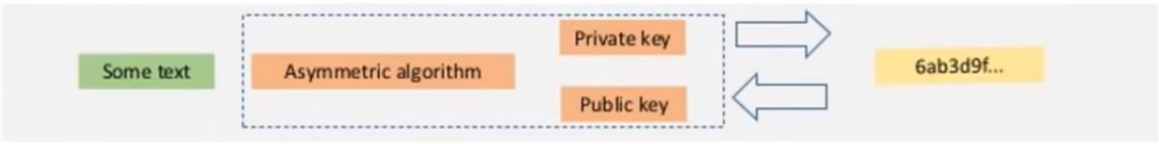
Blockchain uses Private Key Cryptography to secure identities and hash functions to make the blockchain immutable

P2P machines on the network help in maintaining the consistency of the distributed ledger

The program gives the blockchain its protocol based on the requirement

Private Key Cryptography

- Private Key Cryptography involves two different keys, private and public.
- One key is purposely kept private, the other is provided to the other party (or often the public)
- If you use private key to encrypt then the public key can decrypt and vice versa.
- This is called asymmetric encryption



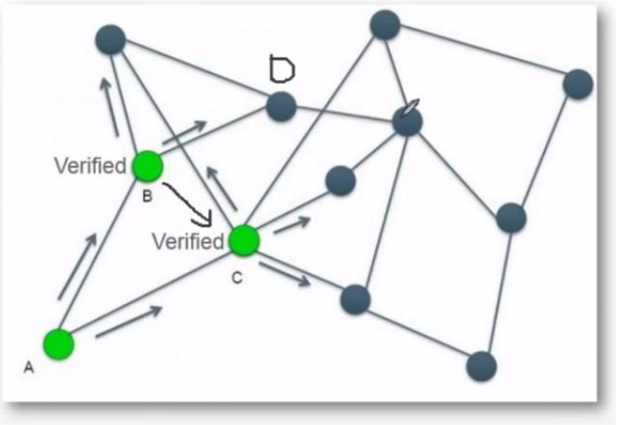
P2P Network

Suppose A finds the transaction: Bobby (B) pays 5 coins to Cindy (C)

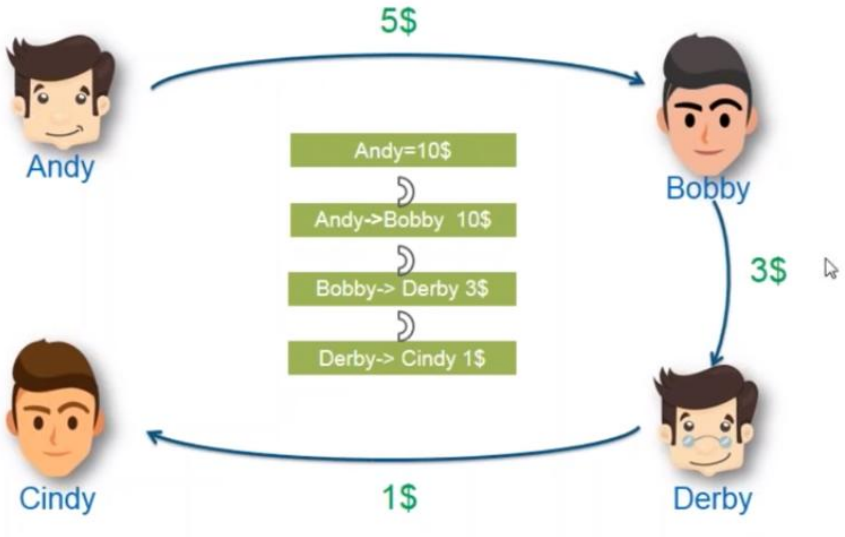
Node A broadcasts to the peers B and C in the network

If the transaction is verified, the peers (here, B & C) forward the transaction to their peers

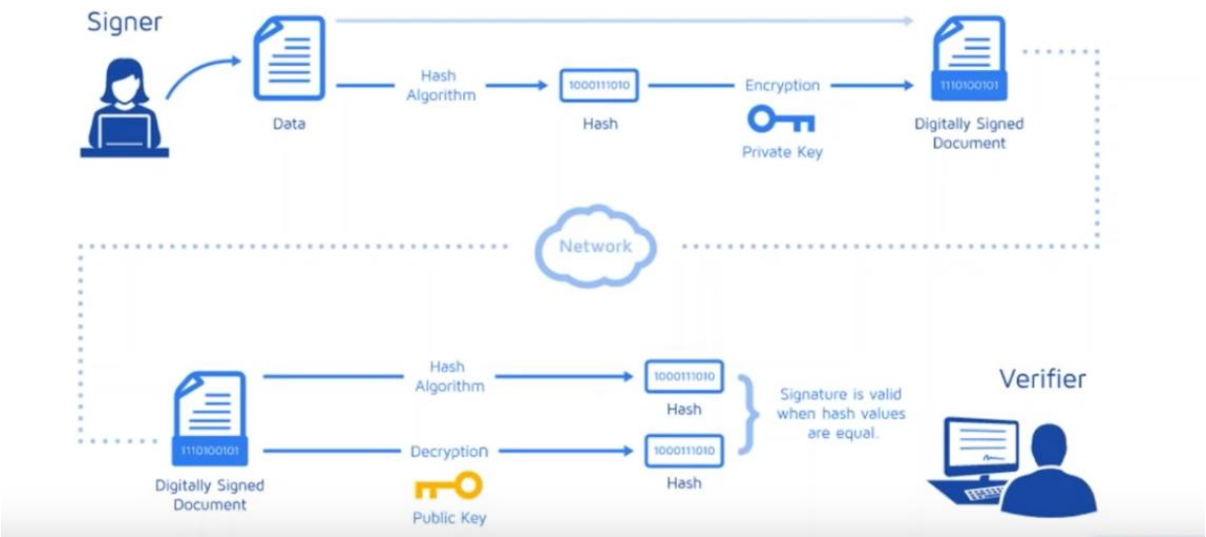
The transactions propagate rapidly across the network



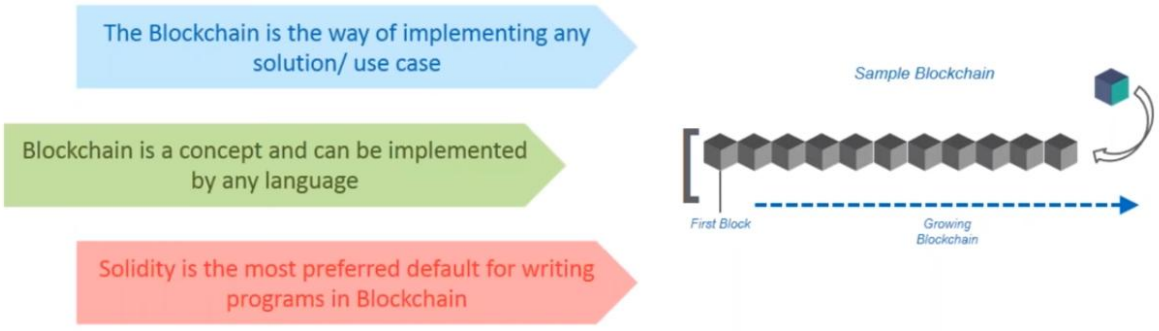
P2P Network-Distibuted Ledger



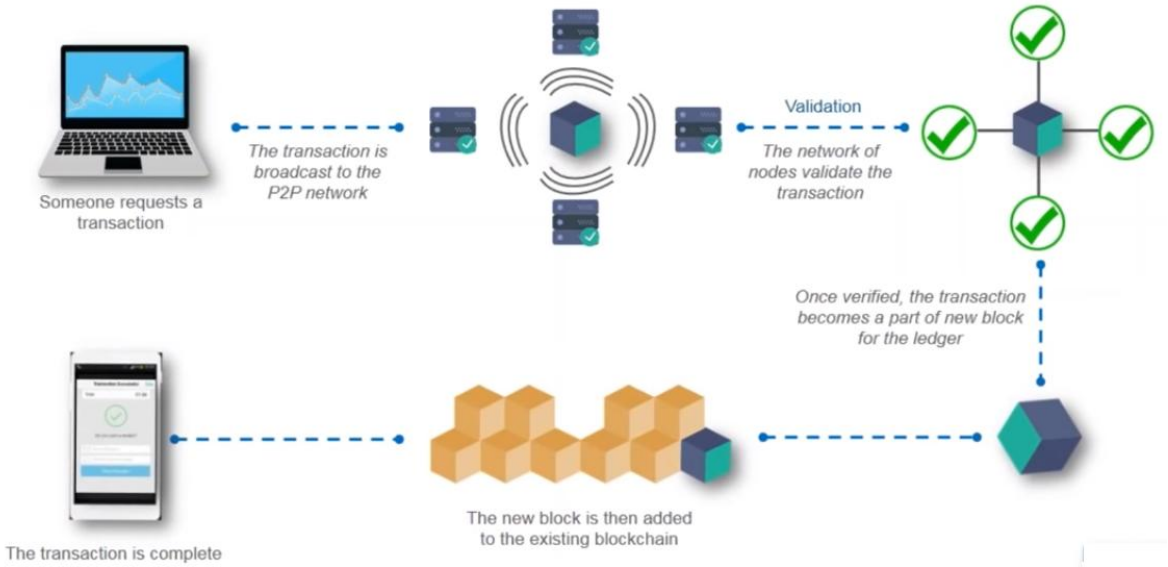
P2P Network-Digital Signature



Blockchain Program



Blockchain Flow Diagram



EVOLUTION of BLOCKCHAIN

Blockchain 1.0, Grandpa Bitcoin

Wei Dai's was one of the first noted researcher to introduce the proposal of b-money that introduced the idea of creating money through solving computational puzzles and decentralized consensus, but the proposal itself was low in implementation details. In 2005, Hal Finney introduced a concept of "reusable proofs of work", a system that used ideas from b-money together with Adam Back's computationally difficult Hashcash puzzles to create a concept for a cryptocurrency, but was also run on centralized trusted backend systems.

Blockchain finally took root with the Bitcoin whitepaper written by visionary Satoshi Nakamoto in 2009. The whitepaper outlines the details required for a protocol that establish a decentralized currency, operate it on a trustless network that is not controlled by individuals with bias towards a particular country, state or governing body.

Blockchain 2.0, Child prodigy Ethereum

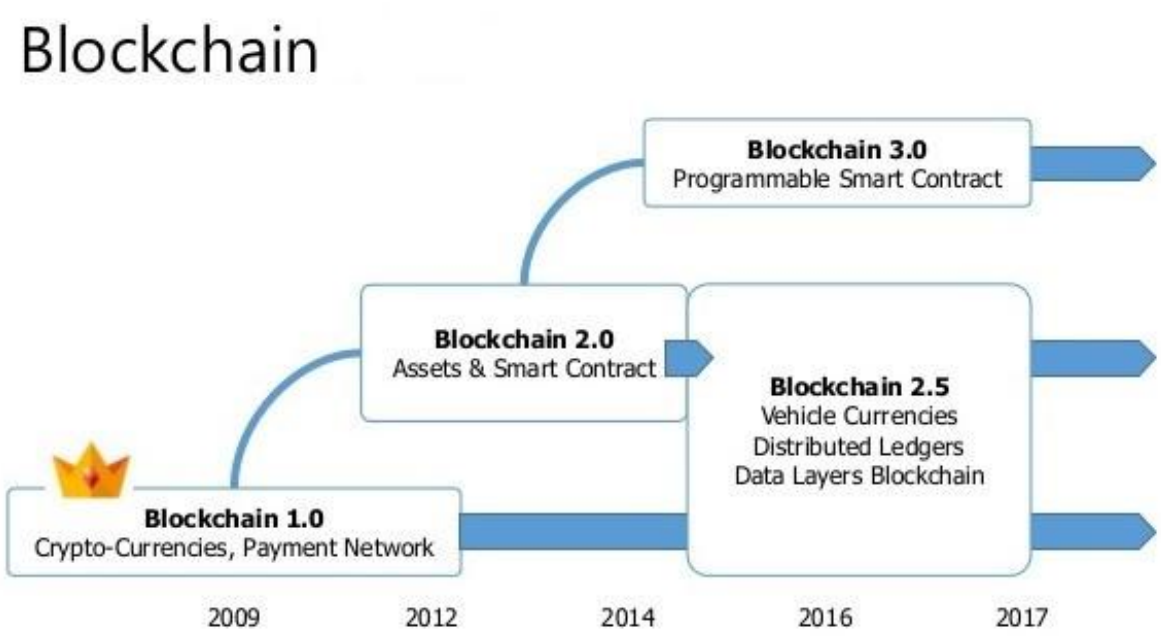
Enter Vitalik Buterin, one of the writers for Bitcoin Magazine that tried to popularize the technology in the early 2012. He witnessed first-hand the problems in the Bitcoin implementation like wasteful mining hardware, centralized mining community, and lack of network scalability. In 2013, the then 19 year old Vitalik described his vision for Ethereum by extending the concept of Bitcoin beyond just currency. He proposed a platform where developer community and entrepreneurs to build distributed application (Dapps) for the Blockchain network. He referred to this concept of trust beyond just currency as 'smart contracts' or even blockchain-based "decentralized autonomous organizations" (DAOs).

Blockchain 3.0, The Killers

The newer technologies obviously boast about the ability to improve on capabilities of Bitcoin and Ethereum networks while overcoming their limitations witnessed. We should see them deliver on their vision and differentiated ability least with regards to transaction time and scale in 2018.It would be hard for me to do justice to each of the competitors in this piece. Below is a short summary of some their key differentiators and controversial moments –

- The One, NEO—It's the first decentralized, open-source cryptocurrency and blockchain platform launched in China. Hyped as the Chinese Ethereum and backed by the Jack Ma Alibaba group it definitely has the potential to be the next Baidu equivalent (in a world dominated by Google search). Also, NEO holders get free GAS tokens and who doesn't like free dividends right?

- Blockless chain, IOTA—Was launched as a cryptocurrency platform optimized for the demanding Internet of things (IoT) ecosystem. With a twist on the traditional blockchain that the company calls Tangle, IOTA claims to provide zero-fee transactions, as well as a unique verification process that resolves many of the scalability problems associated with bitcoin. They had their DAO hack moment when MIT Technology Review's Mike Orcutt published an article entitled "A Cryptocurrency Without a Blockchain Has Been Built to Outperform Bitcoin."



APPLICATIONS

Financial Services

Traditional systems tend to be cumbersome, error-prone and maddeningly slow. Intermediaries are often needed to mediate the process and resolve conflicts. Naturally, this costs stress, time, and money. In contrast, users find the blockchain cheaper, more transparent, and more effective. Small wonder that a growing number of financial services are using this system to introduce innovations, such as smart bonds and smart contracts. The former automatically pays bondholders their coupons once certain preprogrammed terms are met. The latter are digital contracts that self-execute and self-maintain, again when terms are met.

Examples of blockchain financial services applications

- Asset Management: Trade Processing and Settlement
- Insurance: Claims processing
- Payments: Cross-Border Payments

Smart Property

A tangible or intangible property, such as cars, houses, or cookers, on the one hand, or patents, property titles, or company shares, on the other, can have smart technology embedded in them. Such registration can be stored on the ledger along with contractual details of others who are allowed ownership in this property. Smart keys could be used to facilitate access to the permitted party. The ledger stores and allows the exchange of these smart keys once the contract is verified.

Examples of Blockchain Smart Property Applications

- Unconventional money lenders/ hard money lending
- Your car/ smartphone

Blockchain Internet-of-Things (IoT)

Any material object is a ‘thing.’ It becomes an internet of things (IoT) when it has an on/ off switch that connects it to the internet and to each other. By being connected to a computer network, the object, such as a car, become more than just an object. It is now people-people, people-things, and things-things. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices. Others raise that number to over 100!

Examples of Blockchain Internet-of-Things (IoT) Applications

- Smart Appliances
- Supply Chain Sensors

Smart Contracts

Smart contracts are digital which are embedded with an if-this-then-that (IFTTT) code, which gives them self-execution. In real life, an intermediary ensures that all parties follow through on terms. The blockchain not only waives the need for third parties, but also ensures that all ledger participants know the contract details and that contractual terms implement automatically once conditions are met.

Examples of Blockchain Smart Contracts Applications

- Blockchain Healthcare
- Blockchain music

Blockchain Government

In the 2016 election, Democrats and Republicans questioned the security of the voting system. The Green Party called for a recount in Wisconsin, Pennsylvania, and Michigan. Computer scientists say hackers can rig the electronic system to manipulate votes. The ledger would prevent this since votes become encrypted. Private individuals can confirm that their votes were counted and confirm who they voted for. The system saves money, by the way, for the government, too.

Examples of Blockchain Government Applications

- Public value/ community
- Vested responsibility

Blockchain Identity

The blockchain protects your identity by encrypting it and securing it from spammers and marketing schemes.

Examples of Blockchain Identity Applications:

- Passports
- Birth, wedding, and death certificates
- Personal Identification

Blockchain Use cases

Blockchain in Banking

Blockchains could cut up to **$20 billion** in middle-man costs per year

Hacking into banking ledgers becomes close to **impossible**

Solves the **double spending** problem

Reduces bank **crises** by a large extent

Blockchain in Payments and Transfer

Payment & Transfers

Blockchains transfers are the highest in terms of security

Currently Bitcoin runs on no fixed transaction fees

No bank account required

Anonymity is maintained

Blockchain in Voting

Voting

Elections require authentication of voters' identity, secure record keeping and trusted tallies

Blockchains are the medium for casting, tracking and counting votes without voter-fraud, lost records or fowl-play.

Increases voter turnout

CONCLUSION

The application of the Blockchain concept and technology has grown beyond its use for Bitcoin generation and transactions. The properties of its security, privacy, traceability, inherent data provenance and time-stamping has seen its adoption beyond its initial application areas.

The Blockchain itself and its variants are now used to secure any type of transactions, whether it be human-to-human communications or machine-to-machine. Its adoption appears to be secure especially with the global emergence of the Internet-of-Things.

Its decentralized application across the already established global Internet is also very appealing in terms of ensuring data redundancy and hence survivability. The Blockchain has been especially identified to be suitable in developing nations where ensuring trust is of a major concern.

Thus the invention of the Blockchain can be seen to be a vital and much needed additional component of the Internet that was lacking in security and trust before. BC technology still has not reached its maturity with a prediction of five years as novel applications continue to be implemented globally.