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.

INTRODUCTION:

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.

The Blockchain can either be public or private, depending on the scope of its use. A public Blockchain enables all the users with read and write permissions such as in Bitcoin, access to it. However, there are some public Blockchains that limit the access to only either to read or to write. On the contrary, a private Blockchain limits the access to selected trusted participants only, with the aim to keep the users' details concealed.

This is particularly pertinent amongst governmental institutions and allied sister concerns or their subsidies thereof. One of the major benefits of the Blockchain is that it and its implementation technology is public. Each participating entities possesses an updated complete record of the transactions and the associated blocks.

Thus the data remains unaltered, as any changes will be publicly verifiable. However, the data in the blocks are encrypted by a private key and hence cannot be interpreted by everyone.

Another major advantage of the Blockchain technology is that it is decentralized. It is decentralized in the sense that:

• There is no single device that stores the data (transactions and associated blocks), rather they are distributed among the participants throughout the network supporting the Blockchain.

• The transactions are not subject to approval of any single authority or have to abide by a set of specific rules, thus involving substantial trust as to reach a consensus.

• The overall security of a Blockchain eco-system is another advantage. The system only allows new blocks to be appended. Since the previous blocks are public and distributed, they cannot be altered or revised.

For a new transaction to be added to the existing chain, it has to be validated by all the participants of the relevant Blockchain eco-system. For such a validation and verification process, the participants must apply a specific algorithm. The relevant Blockchain eco-system defines what is perceived as "valid", which may vary from one eco-system to another.

A number of transactions, thus approved by the validation and verification process, are bundled together in a block. The newly prepared block is then communicated to all other participating nodes to be appended to the existing chain of blocks. Each succeeding block comprises a hash, a unique digital fingerprint, of the preceding one.

Figure 1 demonstrates how Blockchain transactions takes place, using a step-by-step example. Bob is going to transfer some money to Alice. Once the monetary transaction is initiated and hence triggered by Bob, it is represented as a "transaction" and broadcast to all the involved parties in the networks. The transaction now has to get "approval" as being indeed "valid" by the Blockchain eco-system. Transaction(s) once approved as valid along with the hash of the succeeding block are then fed into a new "block" and communicated to all the participating nodes to be subsequently appended to the existing chain of blocks in the Blockchain digital ledger.

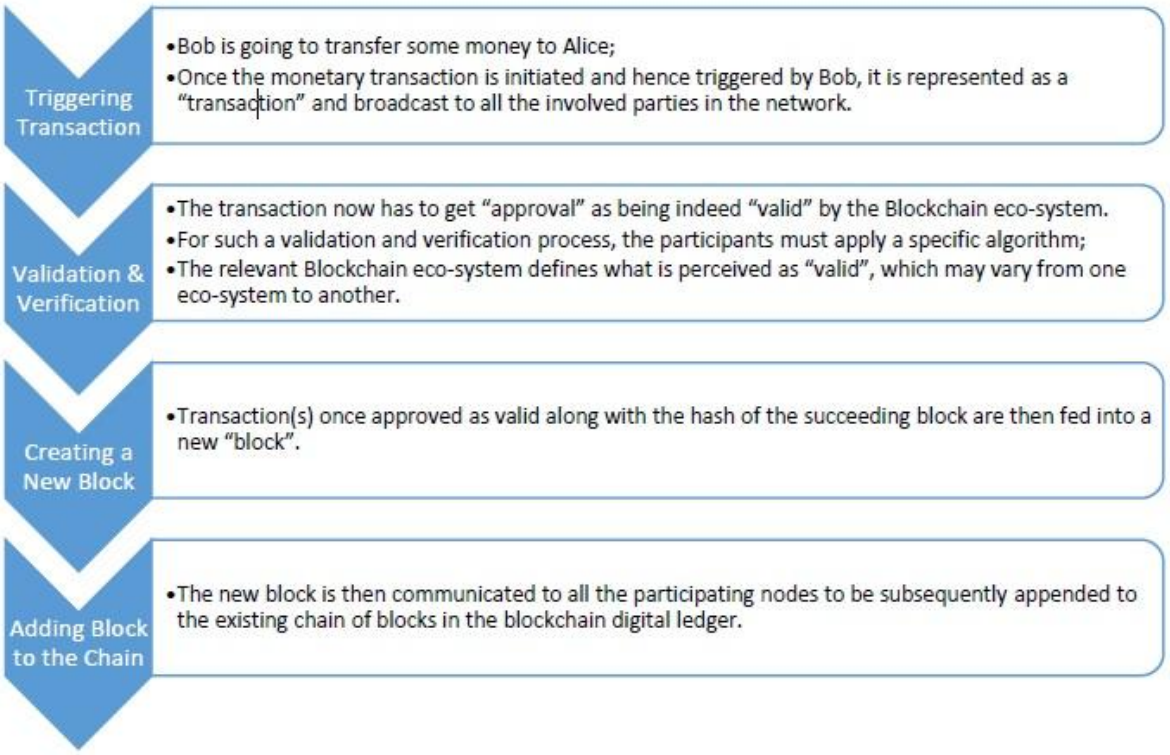


Figure 1. Operation of the Blockchain.

EVOTUTION 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.

In the initial few years it was perceived by outside the cypherphunk community as being an economic experiment. The Bitcoin market cap represented a bug bounty for hackers savvy enough to overrun it. The value of the network rose from a few thousands to over $300 billion in the peak of cryptocurrency run of 2017. The experiment clearly became massive over the years and validated the technology, now is symbolic of Blockchain itself. The technology did eventually exhibit its set of failings with regards to both people and technology. Mining, the process by which Bitcoin is created, started to get dominated in hinterlands of Inner Mongolia right next to sources of cheap hydroelectricity. Also since Satoshi chose to disappear anonymously with his stash of Bitcoins untouched, there has been emergence of people (notably Craig Wright) falsely claiming to be Satoshi. Several rebel community developers tried shepherding the community and creating their own networks with minor code changes that are referred to as forks (Litecoin and Bitcoin Cash are notable amongst the top 10 coins in terms of volume).

.

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).

Ethereum succeeded in gathering a strong developer community, enterprise support via the Enterprise Ethereum Alliance (EEA) and a establishing a true ecosystem in an extremely short time. Till date, it processes the most number of daily transactions on a public network. However by mid-2017, expectations clearly got ahead of reality. Ethereum market cap increased rapidly to 100+ billion within 3 years of existence in the market. There were countdown clocks to the Flippening — an event where the value of Ether would exceed Bitcoin. The network was unable to progress in line with expectation while being in public limelight. Projects like sharding, staking and Plasma to improve the Ethereum network need research and are at least months if not years away from main network completion.

Millions were raised by the Ethereum Dapps using the new unregulated venture capital route touted as Initial Coin Offerings (ICO). An Ethereum based ICO to create the DAO was hacked and tokens worth in excess of $70M were stolen in few hours. A network rollback to fix the hack meant that The 'Code is law' slogan associated with Ethereum immutable contracts was no longer true. There was an Ethereum fork to craft a new Ethereum Classic (ETC). Dapps like 'Status' raised 100m in 3 hours and 'BAT' raised 35m in 24 seconds. A huge market potential coupled with a low barrier to entry proved to be the perfect recipe for competitors. It wasn't long before the market realized that if applications with just whitepapers and no working product on Ethereum network could raise millions, a rival platform was guaranteed to be valued starting in Billions.

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 pre-programmed 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

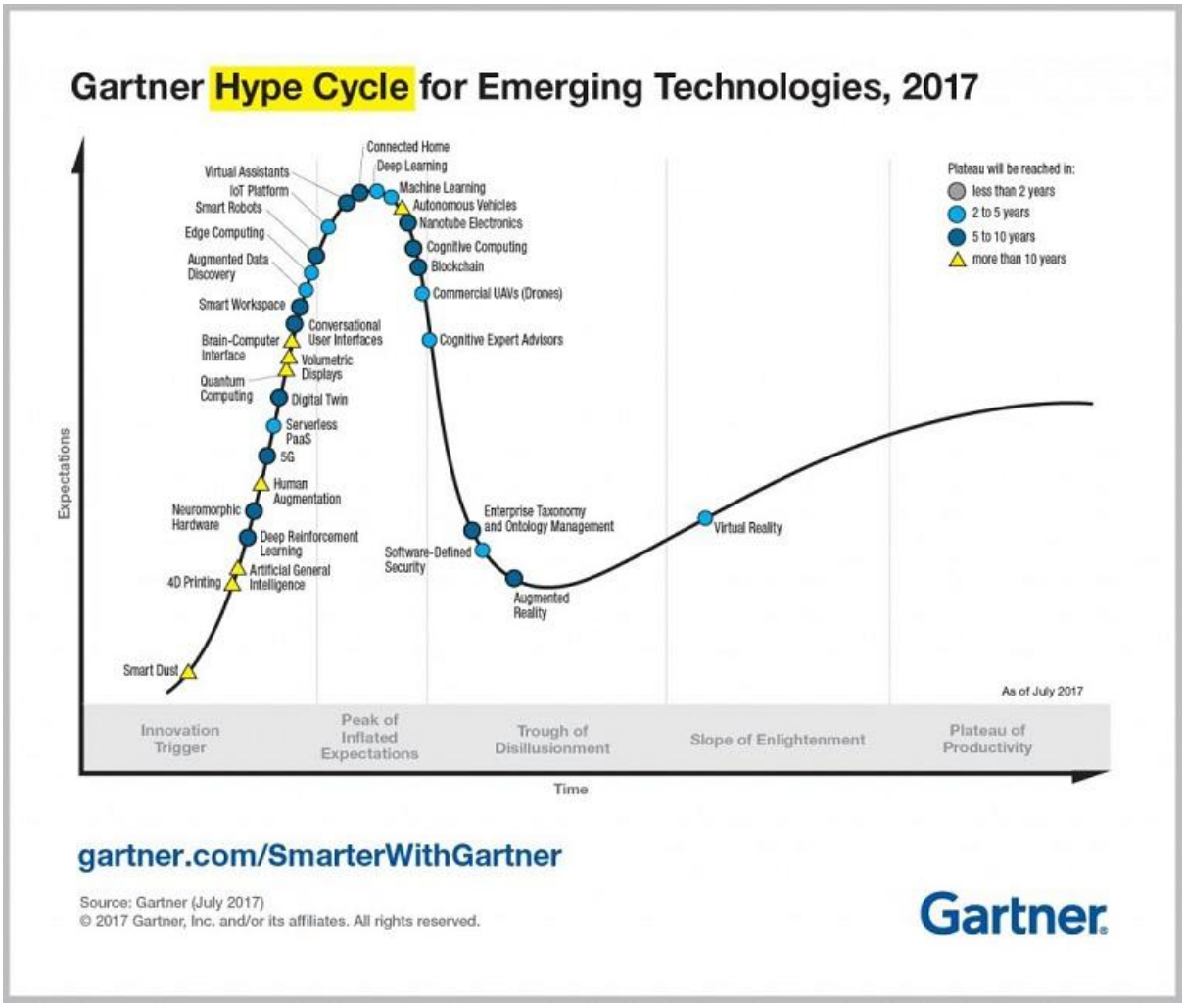
The blockchain protects your identity by encrypting it and securing it from spammers and marketing schemes.

Examples of Blockchain Identity Applications:

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

The Future of Blockchain

According to the Gartner Hype Cycle for Emerging Technologies 2017, shown in Figure 2, below, Blockchain still remains in the region of “Peak of Inflated Expectation” with forecast to reach plateau in “five to ten years”. However, this technology is shown going downhill into the region of the “Trough of Disillusionment”.



Blockchain Technology

Because of the wide adoption of the Blockchain in a wide range of applications beyond cryptocurrency, the authors of this paper are forecasting a shift in classification from “five to ten years” to “two to five years” to reach maturation. Blockchain possesses a great potential in empowering the citizens of the developing countries if widely adopted by e-governance applications for identity management, asset ownership transfer of precious commodities such as gold, silver and diamond, healthcare and other commercial uses as well as in financial inclusion. However, this will strongly depend on national political decisions.

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.