Evolution of Block chain Technology

Eesha Goyal[1], Angela Gilhotra[2]

[1,2]*MCA, IT department, Indira Gandhi Delhi Technical University for Women, New Delhi, India*

Abstract- **When bitcoin was unleashed on the world it filled a specific need for a digital currency. It wasn't long before people realised the technology behind Bitcoin i.e.-the blockchain could do much more than just record monetary transactions. This realisation has developed into an array of startup companies, initiatives, corporate alliances, and research projects.**

This survey paper aims to provide an insight into the origin of blockchain technology and also sheds light upon how the technology has evolved with time. It mentions the modern day applications of blockchain using some present day use cases.

I. INTRODUCTION

The blockchain was first devised by a person/ group of people known by the pseudonym, Satoshi Nakamoto for the digital currency Bitcoin [1] but the roots of the Blockchain can be traced back much further back. A 1976 paper on New Directions in Cryptography [2] discussed the idea of a mutual distributed ledger, a type of data structure which resides across multiple computer devices spread out over the globe. This was later used in the 1990s in a paper entitled How to Time-Stamp a Digital Document [3] along with David Chaum's digital cash [4]. These preexisting technologies and research is what formed the basis of this technology.

But bit coin was just the tip of the iceberg and people soon realised the wide range of possibilities that were unlocked with this technology. Since then the technology has been employed in various other industries like healthcare, banking, IoT, finance etc.

On a very basic level, Blockchain is a type of database that takes a number of records and puts them in a block. Each block is then linked ('chained') to the next block using a cryptographic signature.

A regular database uses a centralized server to store information while a blockchain stores information on a public ledger. This ledger is duplicated across all the nodes in the network. Traditionally, transactions require a middle man like the bank but while working on a public ledger, transactions are automatically verified by multiple nodes. This makes it extremely difficult to falsify information or tamper with transaction history. It can be said that blockchain is a way of ruling out the middleman in transactions while ensuring security, privacy and transparency.

II. BEFORE THE BITCOIN

A. DigiCash

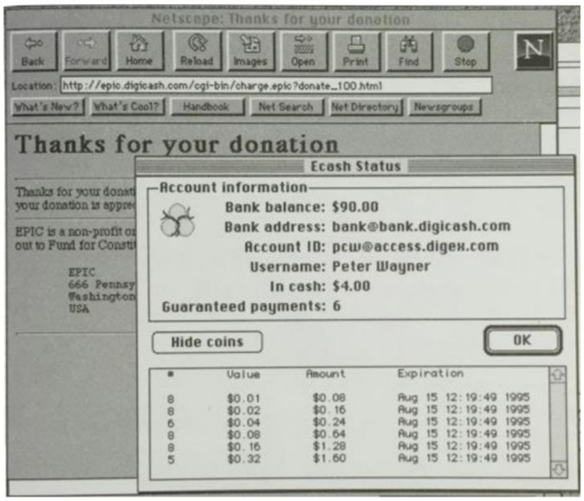
A fundamentally new kind of cryptography was introduced by David Chaum in 1983. This Digital Cash on preventing double spending. The new crypto system was called 'Blind signature', which provided a means of de-linking from the central server and yet allowing a central authority to prevent double spending. Before Chaum's, in any electronic cash system a central authority issued serial numbers and did the signing and record-keeping of these serial numbers It was not cash but was not anonymous either. A note issued from the central authority could be attached to the receivers identity and could be made to track all the places where the person has spent the money. The goal Chaum wished to accomplish with *blind signature* was to create a system that was anonymous *and* prevented double spending. The system of Digital Cash did the following:

1. A sender creates his own serial number and keeps it known only to himself (private key) as opposed to a serial number being provided by a central authority - the serial number here is trusted to be completely unique, such that there is no other way it could be regenerated
2. The central authority *signs* the serial number (not knowing it)

Digital cash was based on the concept of a vulnerable central server. Even though this single point of failure can be distributed by substituting the central server's signature with a threshold signature of several signers, it still remains important for auditing that the signers be unique and identifiable. The system is prone to failure, as each signer can fail, or be made to fail, one by one.

Then, in 1988, Chaum in collaboration with two other cryptographers Fiat and Naor proposed offline electronic cash. With this, the focus shifted from *prevention* of double spending to *detection* of double spending. The payment is delayed to the time the merchant reconnects to the server, and if a problem has been detected, the payment fails. At a high level, what it achieved was this: only the owner can decode the identity of the digital coin. Every time the coin is spent, the recipient will require the sender to decode a random subset of the encoding. This decoding isn't enough to allow the recipient to decipher the identity of the sender. But if the coin is ever double spent, both recipients will go to the bank to redeem their notes eventually, and then there is a high probability that the bank can decipher the original identity by putting the two subsets together.

David Chaum commercialised the idea into a company called DigiCash. The cash in DigiCash's system was called Ecash. The clients in the system were anonymous while the merchants were not. The banks could not trace where a particular individual was spending his money but the merchants had to report their earnings.



Location: http://epic.digicash.com/cgi-bin/charge.epic?donate_100.html

Thanks for your donation

Thanks for your donat
your donation is appre

EPIC is a non-profit or
out to Fund for Constit

EPIC
666 Pennsy
Washington
USA

Ecash Status

Account information

Bank balance: $90.00
Bank address: bank@bank.digicash.com
Account ID: pcw@access.digex.com
Username: Peter Wayner
In cash: $4.00
Guaranteed payments: 6

#	Value	Amount	Expiration
8	$0.01	$0.08	Aug 15 12:19:49 1995
8	$0.02	$0.16	Aug 15 12:19:49 1995
6	$0.04	$0.24	Aug 15 12:19:49 1995
8	$0.08	$0.64	Aug 15 12:19:49 1995
8	$0.16	$1.28	Aug 15 12:19:49 1995
5	$0.32	$1.60	Aug 15 12:19:49 1995

Figure 2: Screenshot of DigiCash

However the DigiCash failed because :

1. The banks and merchants proved hard to persuade to adopt it.
2. Since merchants didn't want Ecash, users didn't want it either.
3. The system did not support user-to-user transactions

Many ideas followed the inception of DigiCash. Some that improved upon the system and devised a work around its shortcomings were CAFE, Mondex, VisaCash. Some systems created new possibilities altogether. They were NetCash, eGold, DigiGold. But ultimately they all aimed to peg the value of digital cash to that of a dollar or a commodity. Where the value of digital money is directly proportional to the value of dollar or the commodity. To ensure that digital currency amounts to real value it is necessary that it is scarce by design so that an effort is needed in order to acquire that value.This is made possible by minting money by solving problems (or "puzzle") that takes a while to crack.

In 1992 Dwork and Naor [5] proposed this concept of solving computational puzzles to create a digital object of some value as a potential solution to email spam. A similar idea was later discovered by Adam Back [6] in 1997.

The concept put forward by Dwork and Naor as a solution to email spam can be broken down as follows:

1. The sender solves a computational puzzle each time before sending an email
2. The recipient's email program would simply ignore the email if it does not have a solution to the puzzle attached

The puzzle should be sufficiently difficult to solve by any average user and also computationally costly for a automated spam bot. The puzzle should be as per the details of the E-mail -sender, receiver, message. Also, the receiver should be able to check the solution easily and each puzzle should be independent of the other. These properties can be achieved by using cryptographic hash functions to design the puzzles.

B. Time-stamping

Time stamping as proposed by Stuart Haber and W Scott Stornetta [7] in their first paper is a method of determining the creation history of a particular document. It is easy to determine the sequence of creation of a particular document when it is created by hand, but in the digital realm, there is no concept of time. Haber and Stornetta proposed a method of *time-stamping* which certified when a particular document was *first created* or *last modified*. In basic terms, time-stamping is a 'little something' added to the document which proves that the document has been issued before or after a certain time.

What Haber and Stornetta proposed was to send the documents to a time-stamping service (central authority). The sole purpose of the server was to *sign* the document together with the current time. An additional function of the server was to *link* the document to the previous document, thus making it possible to determine that a particular document was issued before another. The pointer is question is a hash function that depends on the data of the previous document. What this means is if the data of previous document changes, the pointer becomes invalid.

This method achieved more than just certification as certificate of each document ensured the integrity of all the previous documents. And not just the document, it also ensured the integrity of their contents. It formed a *chain*. Each certificate fixed the entire history of the documents up till that point in time.

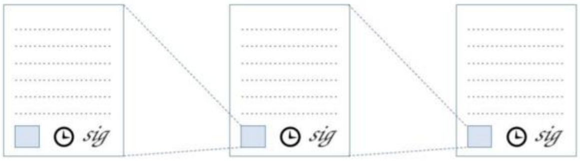


Figure 4: linked timestamping. To create a certificate for a document, the timestamp server includes a hash pointer to the previous document's certificate, the current time, and signs these three data elements together.

An efficiency improvement was later proposed, which did not link the documents individually but collected them into blocks, and then linked the blocks together into a chain. Within each block, documents formed a tree of blocks instead of linear links. The term coined by Haber and Stornetta for what was formed was *Blockchain*.This significantly reduced the amount of checking needed to verify where a particular document appears in the history of the system.

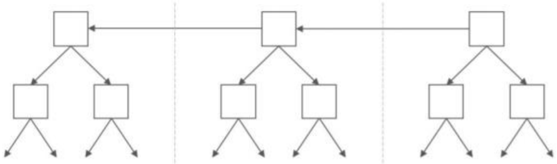


Figure 5: efficient linked timestamping. Arrows represent hash pointers and dotted vertical lines indicate time intervals.

III. WHAT IS A BLOCKCHAIN

According to hyperledger.org,"A blockchain is a peer-to-peer distributed ledger forged by consensus, combined with a system for "smart contracts" and other assistive technologies."

C. How it works

As the name suggests the blockchain is a continuous chain of blocks such that each block contains the following:

1. data according to the application of blockchain
2. a unique hash code which acts like a fingerprint
3. Unique hash code of the previous block. i.e.- a link to the previous data block

The hash code is calculated dynamically after the formation of a block. Any change in the data of the block will change its hash code. If this code changes the block will not be considered to be the same block anymore and it will make all subsequent blocks invalid as they will loose the connection with the tampered block. However, this is not the only thing ensuring security in a blockchain as computers can be programmed to calculate thousand of hash codes per second.

You may effectively tamper with a block and work out all the hashes of alternative blocks. To solve this problem blockchains have an inbuilt mechanism called the proof of work. It slows down the creation of new blocks. for example, it takes 10 minutes to calculate specific proof of work and add a block to the blockchain in a Bitcoin.

Tampering with one block will require calculating the Proof of Work of all adjacent blocks making it a very exhausting process.

Another added security in a blockchain is that it is distributed. Instead of employing a central entity to manage the chain, blockchains use a peer-to-peer network. If a new block is created every node in the network has to verify that the new node hasn't been tampered with. Every node in the network then adds this new node to their blockchain and once again verifies that the entire network is on the same page.

D. Sidechain

Bitcoin's transactions are stored in an all-encompassing ledger - network called the blockchain, secured by a powerful hashing algorithm. A sidechain is a separate blockchain attached to its parent blockchain using a two-way peg. This technology enables interoperability between the two different chains referring to the parent chain as 'main chain' and all additional blockchains as 'side chains'. The way it works is as follow:

1. The user who wishes to transfer his coins (or digital assets) to the side chain sends the amount to a wallet address that renders those coins unusable.
2. Once the transaction is complete, a confirmation is broadcasted across chains followed by a waiting period for extra security.
3. After the waiting period, the equivalent coins are released on the sidechain allowing the user to access and spend them there. The reverse happens when the user wishes to move back to the main chain.

The applications and uses of sidechains are as follows:

1. Sidechains allow interoperability
2. Allow beta releases of Altcoins or software updates before pushing them on the main chain
3. Issuing and tracking of ownership (traditional banking functions) can be first tested on sidechains before moving them to main chains

IV. MODERN DAY APPLICATIONS OF BLOCKCHAIN

A. Supply Chain

Supply chain management is the management of flow of goods, services, products and resources from the suppliers, wholesalers, retailers and to consumers. This movement usually occurs among various companies. This movement among various companies causes major weak points in the system. The reason is no interoperability amongst the ERP Systems of these companies. As a result, data does not flow well through the interface points. The problem that is put forth here can be boiled down to sharing of data. Blockchains are employed such that, each node contains a copy of all the transactions. Each node would know what the present state of the system is and each node having the ability to either accept or reject a change. The examination of products at each stage in the supply chain could be replaced with simply querying the blockchain for the state of the product which was recorded at a particular time in history.

B. Banking/ Finance

The Bitcoin blockchain was created as a "peer-to-peer electronic cash system" (Satoshi Nakamoto, Bitcoin). Therefore, the first blockchain use case in existence was payments. However, Bitcoin proved to be quite slow to process payments, "somewhere in the region of 7 transactions per second" (Guy Brandon, due.com, February 2017), when compared to Visa, which "averages around 2,000 transactions per second, with peak capacity of perhaps 50,000 transactions per second" (Guy Brandon, due.com, February 2017). Developers are actively working to increase the throughput capacity of Bitcoin and other blockchain payment systems.

Blockchain technologies plan to decrease the costs associated with payments, by allowing parties to interact directly, instead of transferring through an intermediary, such as a bank. In addition, having a record of all past payments is useful to auditors and regulators. Financial institutions have heavily researched blockchain payment systems because a universally recorded world state of payment information can decrease the number of payment disputes among institutions.

Bitcoin permits anyone to send cash across borders virtually instantly and with comparatively low fees."Abra" is one startup that's functioning on a bitcoin-based remitment service.

C. Internet of Things

Originally IoT relied on the centralised client-server architecture. This incurred a high infrastructure and maintenance cost. This cost increases substantially when tens of thousands of devices start communicating with each other simultaneously in an IoT network.

Allowing the blockchain technology to replace the traditional IoT architecture gives it a new decentralised approach eliminating single points-of-failure and creating a more resilient and reliable network of devices.

The cryptographic algorithm used in blockchain makes the consumer data more private and secure. It also eliminates the possibilities of man-in-the-middle attacks as there is no single chain for communication between devices.

Some Use cases for blockchain in IoT are :-

1. Samsung and IBM are currently working on a concept called ADEPT which aims to create a decentralised network of IoT devices.

2. The use of E-wallets can allow car owners to automatically pay for parking, highway tolls, and electricity top-ups for their vehicle. Some of the companies working on blockchain e wallets are UBS, ZF and Innogy.
3. the IOTA project (https://iota.org/) is a new-generation cryptographic token that has been specifically designed to meet the needs of the IoT industry.

D. Forecasting

Augur, an online platform is currently working on global decentralised prediction markets.

E. Healthcare

Another industry that depends upon unreliable single server database solutions is the healthcare industry.

Hospitals are at high risk of data tampering and privacy breach. Blockchain technology can revolutionise this field and maintain a secure medical record of patients to be shared with the staff as well as provide a level of transparency with the patient. this can even help in accuracy and speed of diagnosis.

Two companies currently working on this are Gem and Tierion.

F. Provenance

Provenance is a ownership record used as a guide to authenticity or quality. There is a lot of overhead involved in generating provenance records and therefore it is only available for very large systems. With advancement in blockchain provenance records can be made available for a wider variety of things. This information can help the consumer make better and informed purchasing decisions.

To verify the authenticity or quality of a product the consumer can either refer a trusted third party or rely on a transparent record of every transaction associated with that product throughout its life. This is where Blockchain comes into play.

Alternatively, these trusted third parties can use blockchains for recording their audits and inspections. This would reduce the overhead needed to certify the products.

G. Energy Management

Energy management has always been based on central server systems. Energy can not be bought directly from producers and users. It goes through a public grid system or a trusted private intermediary. This field too is gradually making a move to the decentralising technology. Currently, TransactiveGrid is a startup that is using Ethereum to allow customers to buy and sell energy from each other in a peer-to-peer way.

H. Voting and Elections

Electronic Voting Machines (EVMs) and their software security have in the past been the targets of hacks and fraud, and blockchain is a simple and effective solution to the traditional electronic voting methods.

Blockchain technology can be used for voter registration and identity verification, and electronic vote counting to ensure that only legitimate votes are counted, and no votes are changed or removed. This publicly-viewable ledger of recorded votes would prove to be a massive step toward making elections more fair and democratic. Democracy Earth and Follow My Vote are two startups working on creating blockchain-based online voting systems for governments.

A current example of this is :-

In march, 2018 an African country, Sierra Leone, authorised Agora, a Swiss company offering digital voting solutions, to use blockchains to tally the votes in the country's most populous district. Agora stored over 400,000 ballots on its blockchain-based voting system, which also lets registered voters see the vote tally. They aim to improve transparency and reduce suspicion of corruption in a democratic election.

I. Government and Public Sector

Government systems are infamous for being slow, opaque, and prone to corruption. Implementing the blockchain technology on this sector can significantly reduce bureaucracy and increase security, efficiency, and transparency of government operations.

Some present day examples of this are :-

1. Dubai is going to put all its government documents on the blockchain by 2020.
2. The government of Indian state of Andhra Pradesh is working with Swedish startup ChromaWay to set up a blockchain-based land registry system that allows people to collateralise property, get loans, and invest against that asset.

V. CONCLUDING REMARKS

The above survey provides a comprehensive and concise description for blockchain and its features. Moreover, application of blockchain in several industries has been discussed, such as healthcare, finance, internet of technologies, etc. The discussion has proved the importance of this technology which is bound to witness an exponential growth in the future. Proper research, management and experience are required to completely understand the applications of this technology and the business domains where the technology may be applied.

REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" -www.bitcoin.org

[2] WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE, "New Directions in Cryptography",IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] David Chaum "Blind Signature for Untraceable Payments", 1998

[5] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Proceedings of Crypto, 1992. Also available as http://www.wisdom.weizmann.ac.il:81/Dienst/UI /2.0/Describe/ ncstrl.weizmann_il/CS95-20.

[6] Adam Back ,"Hashcash - A Denial of Service Counter-Measure",1st August 2002, http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[8] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[9] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.