Blockchain Technology Beyond Bitcoin

Mausam Kumar
Student, Department of Information Science and Engineering, Nagarjuna College of Engineering and Technology, Bangalore, India

***Abstract*: Blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer to peer digital currency, is the most popular example that uses Blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying Blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world. The main hypothesis is that the Blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun.**

***Keywords*: Blockchain technology.**

1. Introduction

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easy to steal a cookie from a cookie jar, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since

It helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions. However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the Blockchain distributed consensus model as the most important invention since the Internet itself. Johann Polychaeta from BNP Paribas wrote in the Quintessence magazine that bitcoin's Blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond.

2. How does it works?

We explain the concept of the Blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin.

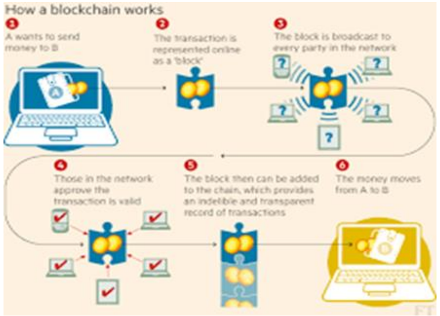

How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
FT

Fig. 1. Financial transactions using the Blockchain technology

However, the blockchain technology is applicable to any digital asset transaction exchanged online Internet commerce is exclusively tied to the financial institutions serving as the trusted third party who process and mediate any electronic transaction. The role of trusted third party is to validate, safeguard and preserve transactions. A certain percentage of fraud is unavoidable in online transactions and that needs mediation by financial transactions. This results in high transaction costs. Bitcoin uses cryptographic proof instead of the trust in the third party for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to spend money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency verifies the digital signature –thus ownership of corresponding "private key" on the transaction using the "public key" of the sender. Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity.

3. Transaction order protected by race

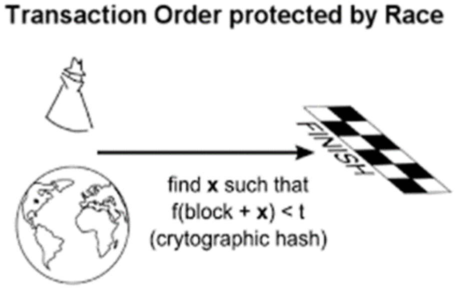


Fig. 2. Mathematical race to protect transactions

This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a node in the Bitcoin network to make a right guess and generate a block. There is very small probability that more than one block will be generated in the system at a given time. First node, to solve the problem, broadcasts the block to rest of the network. Occasionally, however, more than one block will be solved at the same time, leading to several possible branches. However, the math of solving is very complicated and hence the blockchain quickly stabilizes, meaning that every node is in agreement about the ordering of blocks a few back from the end of the chain. The nodes donating their computing resources to solve the puzzle and generate block are called "miner" nodes" and are financially awarded for their efforts.

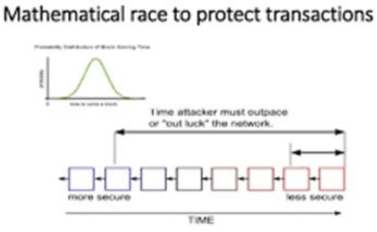

Mathematical race to protect transactions
Time attacker must outpace
or "out luck" the network.
more secure
less secure
TIME

Fig. 3. Mathematical race to protect transactions

4. Existing market

There are a number of blockchains in existence to support wide range of applications--not just cryptocurrency. Currently there are three approaches in Industry to support other applications and also to overcome perceived limitations of Bitcoin Blockchain.

Alternative blockchain is a system of using the Blockchain algorithm to achieve distributed consensus on a particular digital asset. They may share miners with a parent network such as Bitcoin's--this is called merged mining. They have been suggested to implement applications such as DNS, SSL certification authority, file storage and voting.

Colored Coins is an open source protocol that describes class of methods for developers to create digital assets on top of Bitcoin Blockchain by using its functionalities beyond digital currency.

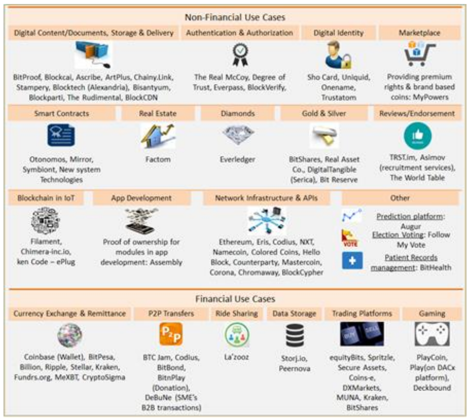
Sidechains are alternative blockchain which are backed by Bitcoins via Bitcoin contract--just as dollars and pounds used to be backed by Gold. One can possibly have a thousands of sidechains "pegged" to Bitcoin, all with different characteristics and purposes--all of them taking advantage of scarcity and resilience guaranteed by the Bitcoin blockchain. The Bitcoin blockchain can in turn iterate to support additional features for the experimental sidechains--once they have been tried and tested.

5. Application

The focus of a new generation of the blockchain applications is not on the transfer of money via transactions on the blockchain but on carrying out serious computation on a decentralized network of computers. Despite the fact that the use of the blockchain as a ledger for decentralized applications offers a seemingly unlimited amount of potential, many concerns regarding the use of the blockchain exist. One of the largest problems with blockchain is the issue of scalability. As for now the use of the blockchain for applications requires every full network node to perform every calculation to reach consensus.

Blockchain shows potential to be used in many different fields and some of them are:

- Domain registration (Namecoin)
- Trading Assets (Colored Coin)
- Cloud Storage
- Voting
- Crowdfunding
- Car sharing
- Gambling and prediction markets
- Internet of Things



Non-Financial Use Cases

Digital Content/Documents, Storage & Delivery: BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN

Authentication & Authorization: The Real McCoy, Degree of Trust, Everpass, BlockVerify,

Digital Identity: Sho Card, Uniquid, Onename, Trustatom

Marketplace: Providing premium rights & brand based coins: MyPowers

Smart Contracts: Otonomos, Mirror, Symbiont, New system Technologies

Real Estate: Factom

Diamonds: Everledger

Gold & Silver: BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve

Reviews/Endorsement: TRST.im, Asimov (recruitment services), The World Table

Blockchain in IoT: Filament, Chimera-inc.io, ken Code – ePlug

App Development: Proof of ownership for modules in app development: Assembly

Network Infrastructure & APIs: Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher

Other: Prediction platform: Augur; Election Voting: Follow My Vote; Patient Records management: BitHealth

Financial Use Cases

Currency Exchange & Remittance: Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma

P2P Transfers: BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)

Ride Sharing: La'zooz

Data Storage: Storj.io, Peernova

Trading Platforms: equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares

Gaming: PlayCoin, Play(on DACx platform), Deckbound

Fig. 4. A few block chain applications with their respective domains

Maybe the most prominent blockchain application that has a purpose outside of sending money from one party to another is Namecoin. Namecoin is the first fork of the Bitcoin protocol ever published and it aims to work as a decentralized domain name registration service and database. Without such a system (centralized or not) services like Tor use pseudorandom hashes to identify accounts. Technically there is no problem with this approach but users would prefer to use more meaningful names to identify the accounts they interact with. Of course systems like Tor would not work if the names identifying the users were not unique. Namecoin ensures the uniqueness of the names chosen by the users. The consensus protocol used by the Bitcoin is perfectly suited to ensure that the first user that gives himself a certain name gets this name and that all users trying to register a name that is already taken will fail to do so.

6. Risk for adoption

- *Blockchain is a promising breakthrough technology*. As we described before, there are vast array of applications or problems that can be solved using blockchain based technology. That spans from Financial (remittance to investment banking) to non-financial applications like Notary services. Most of these are radical innovations. As it happens with adoption with radical innovations, there are significant risks of adoption.
- *Behavior change:* Change is constant, but there is resistance to change. In the world of a non-tangible trusted third party, that blockchain presents, customers need to get used to the fact that their electronic transactions are safe, secured and complete. The present day intermediaries like Visa or Mastercard (in case of a credit cards) will also go through change roles and responsibility. We envision that they will also invest and move their platforms to be blockchain-based. They will continue to provide the customer relationship kind of services.
- *Scaling:* Scaling of the current nascent services based on blockchain presents a challenge. Imagine yourself executing a blockchain transaction for the first time. You will have to go through downloading the entire set of existing blockchains and validate before executing your first transaction. This may take hours or longer as the number of blocks increase exponentially.
- *Bootstrapping:* Moving the existing contracts or business documents/frameworks to the new blockchain based methodology presents a significant set of migration tasks that need to be executed. For example, in case of Real Estate ownerships/liens, the existing documents lying in County or Escrow companies need to be migrated to the equivalent blockchain form. This may involve time and cost.
- *Government Regulations:* In the new world of blockchain-based transactions, Government agencies like FTC, SEC etc. may slow down the adoption by introducing new laws to monitor and regulate the industry for compliance. In USA, this may in a way help adoption as these agencies carry customer trust. In more controlled economies like in China, the adoption will face significant headwind.
- *Fraudulent Activities:* Given the pseudonymous nature of blockchain transactions, coupled with ease of moving valuables, the bad guys may misuse this for fraudulent activities like money trafficking. That said, with enough regulations and technology support law enforcement agencies will be able to monitor and prosecute them.
- *Quantum Computing:* The basis of blockchain technology relies on the very fact that 8 it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the advent of Quantum Computers (in future), the cryptographic keys may be easy enough to crack through sheer brute force approach within a reasonable time. This will bring the whole system to its knee. The counter-argument would be for keys to become even stronger so that they may not be easy to crack.

7. Conclusion

To conclude, blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of blockchain, makes it very attractive technology to solve the current Financial as well as non-financial business problems. As far as the technology is concerned, the cryptocurrency based tech is either in the downward slope of inflated expectations or in trough of disillusionment as shown in Figure 5 below.

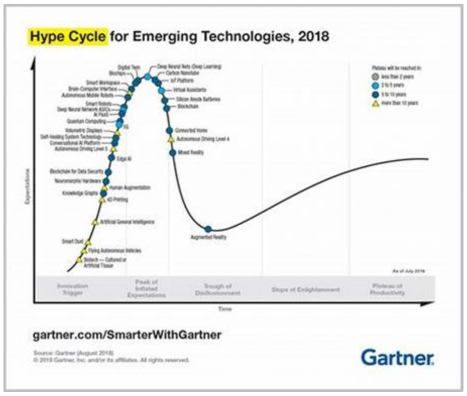


Fig. 5. Showing cryptocurrencies in the trough of disillusionment in gartner's hype cycle

There is enormous interest in blockchain based business applications and hence numerous Start-ups working on them. The adoption definitely faces strong headwind as described before. The large financial institutions like Visa, MasterCard, Banks, NASDAQ, etc., are investing in exploring application of current business models on blockchain. In fact, some of them are searching for the new business models in the world of blockchain. Some would like to stay ahead of the curve in terms of transformed regulatory environments of blockchain.

References

[1] https://hbla.com/blockchain-technology-beyond-bitcoin/