International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume V, Issue X, October - 2018

A STUDY ON BLOCKCHAIN TECHNOLOGY AND ITS IMPACT ON THE E-COMMERCE

Lt Col C Preveen, BSc,BTech,MS,MBA,MIETE

Abstract

Digital transaction of a crypto asset always involved a third party, mostly a trusted financial institution who verifies and authenticates the parties involved and the transaction. This not only entailed time for verification and money in the form of a financial fee to the institution, but also made the transaction recorded and monitored, seriously affecting the privacy of the parties involved. Also a purely peer to peer transaction was only possible with an inherent risk of fraud being encountered, without a monitoring and regulating agency. Even though Digital signature mitigated this problem to some extent, could not circumvent the requirement of a third party, to check double spending. The issue was finally addressed in the Blockchain technology invented by Satoshi Nakama to in 2008 for implementation of the crypto currency called bitcoin. Bitcoin is a crypto currency which can be exchanged online through peer to peer transitions without a separate institutionalised regulator or monitor. The technology consists of usage of distributed continuous records replicated across a host of users in a worldwide network. The trust factor which was being assured by an institutionalised and trusted third party who verifies and acknowledges the participating parties is being fulfilled by distributed ledger algorithms in the Blockchain technology. Blockchain technology gave rise to various other crypto coins like Litecoin, Etherium, Ripple Etc. The underlying technology is used for various other areas which demands secure record keeping in public domain, and has influenced E-Commerce in a constructive and revolutionary way.

Introduction

Commercial transaction almost invariably require a payment, which was done through fiat money authenticated and guaranteed by a financial institution like a Reserve Bank, or a letter of credit by a banking institution trusted by both parties. Payment using fiat money has its own advantages as it is universally accepted and acknowledges and is handed over in material form, which can be inspected and verified. When the internet become popular the advantages of online payment was understood to be manifolds than the fiat money in terms of bulk carriage and geospatial constraints.

However dependency on financial institutions serving astrusted third parties to process electronic payments could not be avoided in the initial model. The problems were escalated by the need to have reversible transactions, which is a requirement of financial institutions to recover from fraud and mistakes, and the cost of dispute resolutions and meditative interventions. Trust was still a serious issue in these scenarios. Satoshi Nakama to proposed a solution to the double-spending problem using a peer-to-peer distributedtimestamp server to generate computational proof of the chronological order of transactions in 2008, which by design built in a cryptographic proof of transaction instead of trust,allowing any two willing parties to carry out a peer to peer online transaction without the need for a trustedthird party. Transactions were made computationally impractical to reverse, to protect sellersfrom fraud, and routine escrow mechanisms were implemented to protect buyers. The system has caught wind hence and is being implemented not only for monetary transactions, but for various other purposes by governments, private firms etc for recording of sensitive information.

Blockchain

A Block is a just a database in a particular format, akin to a distributed ledger. The database has a number akin to a page number in a book. A Blockchain is simply a sequence of such numbered databases. Just like a book is numbered sequentially, the block chain has a unique number and the reference number of the previous block. The number of a block is the hash of the contents of that block. This effectively works as a security mechanism against hackers, since if a hacker changed the

content of a block he has to change all the further block, which is not feasible without alerting the network. A block has two parts viz header and content. The header contains metadata like the time block was created, unique block reference number, and the reference number of the previous block. The content will contain the transaction details of the digitals assets like the address of the parties, amount transacted and time etc. if a particular block is given, one can reference all the previous blocks in the Blockchain giving out the complete history of asset transmutations to the very first one. Hence the entire block chain data is rendered verifiable and auditable. Hence when a Blockchain becomes huge, it becomes more and more difficult for attackers to bypass or overcome the verification activities of the genuine majority stakeholders. Hence such Blockchain can be used not only in crypto currency transactions, but in record keeping of all sensitive assets and database.

Characteristics of Blockchain

Most of the Blockchains have certain common elements which essentially provide them with the characteristics which make them robust ad secure, as given under.

- Decentralised and Distributed: A Blockchain is decentralised and a copy of the same is digitally distributed across a number of computers is near real time. This means that a copy of the entire records are available with each of the participants of the peer to peer networks. This element pre-empts the requirement of monitoring and regulating intermediaries in the network and makes it a true trusted peer to peer network.

- Consensus instead of Authentication: All participants use their respective nodes to verify and authenticate any new transaction carried out in the network. The consensus of majority constitute the approval of the network for that transaction. This effectively counters double spending and manipulation by hackers.

- Identity through cryptography and Digital Signature: even though the network values privacy and use of anonymous identities based on cryptography for routine transactions, it is still possible to find out the real life identity if the person through his available crypto credentials and digital signature records

- The operative philosophy makes changing of records very difficult: The records can be read by anyone in the system and new e=records can be created by the persons who are authorised by the b=network. However it is very difficult ot change existing records as it needs consensus of the majority of the peers in the network and hence is considered near impossible, unless desired by majority stake holders in the network.

- Time stamp for /tracking: All transactions in the Blockchain are time stamped for tracking and verification.

- Programmability: A Blockchain can be programmed for conditional access and operation by the network. A new entrant can be forced to do the legitimate operations and made to follow the ground rules by means of this conditional programming.

Important Crypto Currencies using Blockchain

Most crypto currencies use Blockchain technology for carrying out storage and transmutation of the asset value of their respective currencies, with variations in the components technologies as per their need for security, speed and ease of operation. Certain prominent crypto currencies using this technology are as under:-

- Bitcoin: Bitcoin is the first decentralized crypto currency and worldwide payment

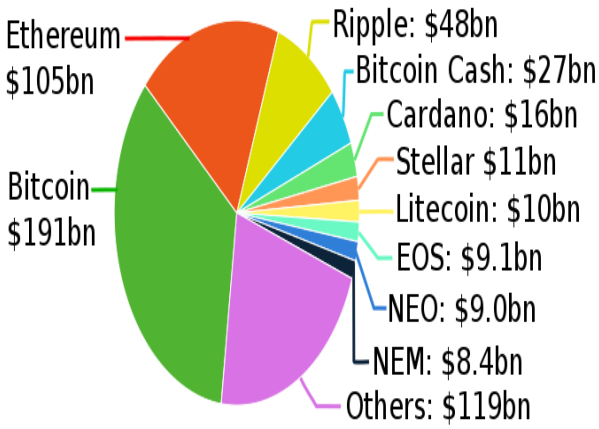
system and works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a Blockchain. Bitcoin was invented by an unknown person or group of people under the name Satoshi Nakamoto and released as open-source software in 2009.Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services. Over 200,000 merchants and vendors accept bitcoin as payment worldwide. Research produced by the University of Cambridge estimates that in 2017, there were 2.9 to 5.8 million unique users using a crypto currency wallet, most of them using bitcoin. As on date bitcoin remains most costly, valuable and preferred crypto currency in the world.

- Litecoin :Litecoin (LTC or Ł) is a peer-to-peer crypto currency and open source software project released under the MIT/X11 license. Creation and transfer of coins is based on an open source cryptographic protocol and is not managed by any central authority. The coin was inspired by, and in technical details is nearly identical to, Bitcoin (BTC).Litecoin was released via an open-source client on GitHub on October 7, 2011 by Charlie Lee, a former Google employee. The Litecoin network went live on October 13, 2011. It was a fork of the Bitcoin Core client, differing primarily by having a decreased block generation time (2.5 minutes), increased maximum number of coins, different hashing algorithm and a slightly modified GUI. During the month of November 2013, the aggregate value of Litecoin experienced massive growth which included a 100% leap within 24 hours. Litecoin reached a $1 billion market capitalization in November 2013. In May 2017, Litecoin became the first of the top 5 (by market cap) crypto currencies to adopt Segregated Witness.Later in May of the same year, the first Lightning Network transaction was completed through Litecoin, transferring 0.00000001 LTC from Zürich to San Francisco in under one second.

- Ethereum:Ethereum is an open-source, public, Blockchain-based distributed computing platform and operating system featuring smart contract functionality. It supports a modified version of Nakamoto consensus via transaction based state transitions. In popular discourse, the term Ethereum is often used interchangeably with Ether to refer to the crypto currency that is generated on the Ethereum platform. Ether is a crypto currency whose Blockchain is generated by the Ethereum platform. Ether can be transferred between accounts and used to compensate participant mining nodes for computations performed. Ethereum provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network. Ethereum was proposed in late 2013 by VitalikButerin, a crypto currency researcher and programmer. Development was funded by an online crowdsale that took place between July and August 2014. The system went live on 30 July 2015, with 11.9 million coins "premined" for the crowdsale. This accounts for approximately 13 percent of the total circulating supply. In 2016, as a result of the collapse of The DAO project, Ethereum was split into two separate Blockchains – the new separate version became Ethereum (ETH), and the original continued as Ethereum Classic (ETC). The value of the Ethereum currency grew over 13,000 percent in 2017.

Market Capitalisation

There are many crypto coins whose total number will run into more than 200 and their total market capitalisation is $379,110,440,913 as on dateThe following chart shows market capitalisation as on 28 Jan 2018.



Market capitalisation of Bitcoin alone is $156,947,150,608 as on date. That of Litecoin is $10,462,242,889 and Etherium is $70,173,568,036. Ripple, a crypto contract based online currency has market capitalisation of $31,962,756,562. There are thousands of companies including Paypal and Microsoft who accepts crypto currencies for their business transaction.

Blockchain in Ecommerce

Blockchain technology has already entered Ecommerce scenario. This technology offers a host of benefit to the E commerce transactions right from acceptance of payment through crypto currencies to maintenance of merchandise details in various showrooms across a city ot country or Globe, to entering into a smart contract by parties who may be sitting virtually across the globe. Some key points are discussed below.

-Complete Transparency: Integrating Blockchain into the payment processing system gives the benefit of absolute transparency. Blockchain based transmutation of money offer visibility, security, faster processing speed and traceability through the decentralized register and Digital Signature. Each and every transaction is recorded in the decentralised ledger and can be seen by the public if desired so. The transparency off Blockchain will also help in automating the implementation of agreements and eliminate counterfeit goods from your supply chain. Fraudulent goods are always an issue in online commerce and Blockchain offers an ideal solution for this problem Alibaba has successfully used Blockchain technology in tracking counterfeit products.

-Cost-Effectiveness & Trust: Based onBlockchain, store owners can accept crypto currencies with zero or very low transaction fees. The concept of cost-effectiveness beats the conventional digital payment methods as it removes the middlemen/payment processors that require a cut in exchange for security and guarantee for the transaction. PayPal, for instance secures a buyer's payment up until the goods are delivered. Using Blockchain, a merchant can guarantee a similar level of security to its buyers. This way, your customers have the peace of mind that until the exact delivery is fulfilled, money will not be transferred to the merchant's wallet.

- integration with the Management Systems: Blockchain can be can easily integrated into various management systems. A very probable use case is the integration of blockchain with warehouse management systems. This integration is crucial for avoiding the supply of fraudulent items. At the same time, this integration also allows for the automation of inventory control and streamlines the distribution processes – The possibilities are endless.

Another use case is the market strategy that involves democratization of content and its use in the daily business functions, such as the sharing and monetization of 3D images. Using the blockchain technology, creators and online retailers can share and sell content through P2P networks. An example of this solution is Cappasity, a cloud based platform, which leverages blockchain infrastructure to easily create and embed 3D content into their websites.

Conclusion

Blockchain technology is one of the greatest disruptive technologies invented in this century and is becoming viral not only in the financial scenario but in the e commerce, government, military and business scenarios also. We can expect a torrent of new applications and technologies using the Blockchain technology in the times to come.

References

1. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
2. https://bitcoin.org/bitcoin.pdf
3. Bitcoin and Beyond:A Technical Survey on Decentralized Digital CurrenciesbyFlorian TschorschBjörnScheuermann
4. BITCOIN:A Primer for Policymakers byJERRY BRITO AND ANDREA CASTILLO
5. https://coinmarketcap.com/
6. Chaum, David; Fiat, Amos; Naor, Moni. "Untraceable Electronic Cash"