Blockchain

Mashallah Behbehani

Jesse Cox

Kartik Chavan

Ashwini Vishwanath Hosmani

Salman Mohammed

Tapan Patel

The University of Texas at Arlington

**Abstract**

In 2009 an IT worker in the U.K. named James Howell created software files called Bitcoins on his laptop, using a technique called “Bitcoin mining”. Bitcoin is a form of digital currency based on a concept called a Blockchain. A few years later in 2013, James threw out the hard drive his Bitcoins were sitting on. As Bitcoin became more popular, his hard drive became increasingly valuable and unsuccessful requests were made to local officials to approve an excavation. (Kobie, n.d.) When Bitcoin’s price recently spiked to $19,783 in December 2016, the hard drive buried within the dump contained 7,500 coins with an approximate value of $148.37 million. (“Bitcoin Price Drops Below $15k, Down 25% from All-Time High,” 2017)

Another blockchain-based platform named Ethereum recently experienced a rush of popularity due to a trading app called Cryptokitties. The creators of Cryptokitties earned over $12 million, with some Cryptokitties trading for over $80,000. (Liao, 2017) The FBI shut down an illegal online drug marketplace which relied on Bitcoin its payments and sold the seized Bitcoins for $48 million. (“The U.S. sold over 144,000 Bitcoins at an Average Price of $334,” n.d.) In the midst of a cryptocurrency goldrush, the Securities and Exchange Commission has begun filing complaints in federal court over initial coin offerings for new cryptocurrencies (“SEC.gov | SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds,” n.d.) The trigger for all of this activity is the introduction of Blockchain.

Bitcoin.org defines Blockchain as: “a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. The integrity and the chronological order of the block chain are enforced with cryptography.” (“How does Bitcoin work?” n.d.) Satoshi Nakamoto published the initial paper on Bitcoin, describing use of a blockchain to process transactions without the need for a central authority. (Nakamoto, n.d.) Since then, blockchain has expanded too many additional implementations. In addition to Bitcoin, trading websites such as Coinbase offer blockchain-based currencies like Litecoin, Ethereum and a Bitcoin Cash, with Coinbase claiming over 10M users and $50B in completed transactions. (“Coinbase - Buy/Sell Digital Currency,” n.d.)

1. **Why does it matter?**

Blockchain provides several advantages such as transparency and integrity of transactions, anti-theft encryptions, increased efficiency and low costs (Nowiński & Kozma, 2017, p. 174). Blockchain technology is less costly than physical transactions leading to cross-over network effects which increase the use of electronic transactions. Bitcoin is said to continue to function as “niche monies” even with the rise of similar other cryptocurrencies. Cryptocurrency is facilitated by trust which increases with the number of users of the cryptocurrency. Blockchain’s bitcoin is a first step towards decentralization of the currency. Bitcoin can single handedly bring minorities and many unbanked people within the purview of the economic system.

Blockchain technology enables trustworthy transactions in a trustless world. The blockchain technology provides a platform for the exchange of digital assets, like bitcoin, anonymously. One of the best things about blockchain is that it eliminates the norm, which is the requirement of a centralized authority to verify each transaction and then transfer the value. Also, the power and control are transferred from the big boys to numerous small ones.

· It’s potential to impact virtually every industry. Blockchain technology has the potential to drastically impact the world and change the way it currently works. The way people live, work, consume and interact is going to be completely changed. It will affect virtually all the industries – Finance, Insurance, supply chain, government, education, to name just a few. It’s potential to have exponential improvements in business value .So, people who have a good grasp of the blockchain technology and understand its benefits believe that the technology enables great improvements in business value. We are talking huge increases in performance here. (10x, 50x, 100x, and 1000x.) Gartner, a management consulting firm predicts that by 2030, blockchain will be generating business value of $3.1 trillion, which could still be a low estimate if all the ancillary effects are included.

It’s infinite potential – we are still in early stages. Blockchain technology is still in its nascent stage and is slowly maturing. But the numerous advantages of the technology such as transparency, strong cryptographic foundation, integrity of transactions, etc. have attracted a lot of investors from different industries to invest in the technology. Companies have already started building new innovative applications on their own custom blockchains. For instance, Gridcoin is an application that is built on blockchain and is used to crowdsource scientific projects. It uses its own protocols which leads to much more economical requirements of computing power and electricity for it to operate compared to the traditional bitcoin networks.

Just like the internet, people have no idea and cannot predict the new ancillary technologies that could and would spawn based on blockchain technology. The potential of blockchain technology is just being explored. As more and more people start understanding the potential and application of the technology, many new and revolutionary applications will be developed.

1. **How does it work?**

The blockchain allows exchange of value, by eliminating the need for trust or for a central authority. Let us consider an example of a transaction occurring between two parties, now there can be three options to conduct this transaction:

1) Trust.

Both parties can trust each other to fulfil their part of the transaction, but any party can easily back out under dire circumstances.

2) Contract.

Due to the contract both the parties will be more inclined toward fulfilling their part of the transaction, but if any one decides not to pay the other party will have to bear the additional burden of paying legal expenses and getting the verdict might be time consuming.

3) Neutral Intermediary.

We can always involve a neutral third party that can make sure the transaction goes smoothly but there are always chances of bias and default by the third party.

All the options don’t seem like optimal solutions, but block chain technology offers us an option which is quick secure and cheap. In simple words Blockchain allows to write a few lines of code, a program that is running on blockchain, to which both parties fulfil their obligations within the contract. This program will check the contract logic and perform the transaction accordingly and once it is running on the blockchain it cannot be halted or altered.

Let us try to understand the concept of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin.

A transaction that takes place with a blockchain technology such as with bitcoin is described with a unique hash called the hash-function, a nonce and a hash from a prior book. A hash-function is a string combination of alphanumeric elements which is in turn is generated through data coding with a cryptographic; whereas a nonce is a unique number belonging to the block. Thus, an effort to hack or imitate a block would require a preceding step of imitating preceding blocks. This mechanism ensures safety to the blockchain transactions from wrongful attempts or simply changing the transactions (Nowiński & Kozma, 2017). Blockchain is the digitizing of the central exchange system where it aims to replace the formal institutions. Bitcoins cannot be transferred without the account holder’s permission. Miners determine an elliptic curve digital signature algorithm (ECDSA) which is arithmetically converted into a data string of 256 bits in length. The data string is the payload through which transactions are encrypted and encrypted by the senders and receivers respectively. Once this match is made, the data block is ready to be added to the ledgers which contains record every network miner and the ledger host machine. The decrypted message by the receiver is sent to the miner for cross-verification. Once the blockchain block is complete, the said contents are sealed, and the payload becomes incorruptible. Thus, to hack into or corrupt a transaction would mean to attack an entire network. If the network suffers a connectivity issue the recourse is to pass the data blocks to a single miner (Alcazar, V. 2017).

Bitcoin addresses are synonymous with that of bank accounts but are different in the sense that other users are aware of the amount available but not the identity of the holder of that account. The addresses are assigned cryptographic keys which authorize the transactions. All bitcoin transactions are collected into blocks and each block has a hash of the previous block hence the name blockchain. The frequency of finding a specific transaction in a block occurs every 10 minutes. Transactions are traced via the IP address of the computer that generated them although anonymous mining is also possible (Polasik, M., Piotrowska, A. I., Wisniewski, T. P., Kotkowski, R., & Lightfoot, G., 2015).

Blockchain and Bitcoin are different things – blockchain technology is what bitcoin is based on, blockchain technology can be used for many other applications other than crypto currency. The term blockchain comprises of a combination combination of a multiple technologies, including:

Ø The blockchain data structure.

Ø Public key cryptography.

Ø Distributed ledgers.

Ø Consensus mechanisms.

The blockchain data structure - A blockchain is a unique type of data structure, the data is set and built on successive blocks. Every block consists of a small piece of data that verifies the content of the previous one. Thus, a change in the predecessor leads to a mismatch all the subsequent blocks. The system that manages the block chain is capable detecting and rejecting the attempted modifications and this is what makes block-chain tamper proof.

Public key cryptography -Public key cryptography allows each participant to be identified uniquely within the system and can be used to validate if any modifications to the blockchain using a cryptographically secure private key. Although public key cryptography has wide uses, it plays an important role in underlying blockchain technology ensuring security, making sure only authorized participants can make changes to blockchain. It can also be used to restrict access only by those with the decryption key.

Distributed ledgers - There are two ways in which ledger systems operate. The first is the adoption of a decentralized ledger where the transaction costs are high, and the maintenance of records becomes cumbersome. Decentralized ledgers are not secure because it may be difficult to track the history of changes made to the ledger or the transactions. The second way to main ledge systems is to trust a centralized ledger where parties to the transaction rely on a formal and central institution to avoid vulnerability. The downside of such a centralized form of ledger maintenance is that the system is easy to hack or can be easily deleted. Comparing the two forms of ledger maintenance, the former decentralized form of ledger allows all participants to maintain complete records of all transactions where each participant or node’s approval is required to make a substantial change to the ledger.

Consensus mechanisms - This mechanism entrusts the participants or nodes in a ledger with the function of gate-keeping. As gate-keepers of the ledger, every substantial change made to the ledger is pre-approved by the nodes. Once the approval, permission and consensus from all nodes or participants to the transaction has been retrieved, the change will be implemented. This change is implemented uniformly across all participants via the validation of new data entry reflected in the consensus of the parties. Based on pre-set rules and versions, the changes in the blockchain will reflect identically in all the participants’ ledgers. The reliance for security on a network of users than a single, centralized authority reduces the propensity of loss of important data.

1. **How is it being used by others?**

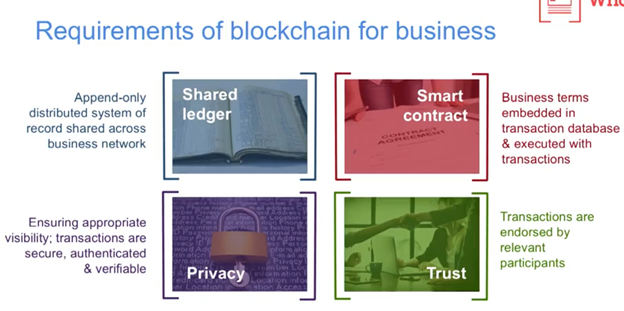
In the legal world, Blockchain technology is being used to build smart contracts which are self-executing digital contracts that are essentially decision rules coded into a computer that are used to ensure that both parties involved in the contract are held accountable and that the terms of the agreement are complete only when both the parties have honored their end of the bargain. The terms of the deal, once finalized, cannot be rewritten by either of the parties.

Blockchain technology has also been successfully used in the social work area. Over 10,000 Syrian refugees received cryptocurrency-based vouchers from United Nations World Food Programme (UNWFP). These vouchers were used by them to purchase food. Some of the leading personalities and companies in the blockchain world helped make this application of the platform a reality by helping thousands of refugees purchase food. The growing global refugee crisis is becoming an unmanageable situation and the countries and agencies deeply involved in it are looking toward new, innovative solutions to solve some of the problems.

1. **What are the requirements?**

**Enterprise requirements**

Fully secure and Authenticated Transactions; associated with FinTech, (economic generation) and the commercial agreement of financial transactions.

Mass Updates of Asset Registers; associated with IoT endpoints facts transfers and associated micropayments.

Regardless of the requirements of FinTech or Blockchain or dispensed Ledger there are 4 commonplace primary abilities required in a commercially acceptable solution, and the challenge is to achieve this whilst enabling the other specialized requirements.

Permanent unbreakable relationship between some the Asset and the mathematic Authentication; a widespread and unacceptable risk lies within the being separate entities that can be exploited and mixed one at a time.

State-of-the-art identity management; able to resource whole identity authentication to the direct player’s in individual transactions, at the same time as making sure the character transactions updating the dispensed Asset Registers are genuinely anonymous.

Complicated Transaction control: successful in making sure the form of transaction is standardized, apparent, and allotted to all Ledgers in the determined time frame.

Consensus primarily based agree with model; to make sure that each one members together can verify all transactions through not unusual evaluation in their Asset Ledgers.

Examining simply the handiest basic requirements for FinTech Transactions versus Mass update of Asset Registers illustrates just how one-of-a-kind the commercial enterprise answers and resulting the technology development are;

|  |  |  |
| --- | --- | --- |
| Core Requirement | FinTech | Mass Update Asset Mgmt |
| Principle use | Auditable financial payment transactions | IoT Device updates with micro payments |
| Volumes/ Transaction sizes | Low volumes with relatively large transaction data | Massive volumes with exceeding small transaction data |
| Security/Reliability | Absolute, both transaction and end devices must not be accessible to hackers | Functional, acceptable as individual transactions low value, & dumb end devices |
| Cost | Transactions are each of high importance/value and higher cost is acceptable. | Transactions are individually of low value and cost must match |

1. **What are the downsides?**

Bootstrapping- Bootstrapping the Blockchain includes downloading of bootstrap file, closing of the wallet, overriding of the Blockchain files, & restarting of the wallet. This is high level idea of bootstrapping, but it varies in every case. Entire set of existing Blockchains must be downloaded & verified for the first time. Blockchain being a new technology requires engineering of a lot of migration tasks. Migration from existing business framework demands both cost and time.

* Costs of Transactions- In attempt of selling Bitcoin started off as ‘nearly free’ in the initial years of its existence. But Nolan Bauerle highlighted in 2016 that each transaction in Bitcoin costed about $0.20 allowing only 80 bytes of data storage and can process 7 transactions/ second only.
* 51% Attack- There appears to be an unavoidable flaw in Blockchains: The risk of 51% attack. Satoshi Nakamoto, developer of bitcoin, highlighted during launching of bitcoin: if more than half power of computing being used for mining is controlled by someone or more than half the computer nodes make a false verification, then it gets accepted to update in the ledger. Unlike traditional payment systems, blockchains are not immune to 51% attack, making it prisoner of its own ideology.
* Scalability, The Everlasting Myth-Considering 7 transactions/second processing speed of a Blockchain network, scalability appears to be an issue with exponentially growing network. According to the blog, “Six Myths about Blockchain & Bitcoin” by Alexey Malanov, Kaspersky Lab, and entire transaction history is being stored by every high-grade bitcoin, & it has already crossed 100 GB storage. With the current trend of number of transactions, it will go beyond the capacity of commodity computer systems.

1. **Conclusions**

Blockchain is a very promising technological transformation in digital world. Although it is still in its nascent stage of development, it packs high potential to make a huge impact in financial, retail, manufacturing, real estate, politics and many more sectors. Its high potential to generate exponential increase in business value has already attracted a lot of interest from the corporate sector. And, also, the numerous benefits it offers has attracted a lot of people – both technical and non-technical, to come together to innovate and create new, innovative and transformative applications.

Even though the blockchain technology has attracted a lot of interest from different sectors and has a multitude of real world use cases, one factor that is going to have a big part to play in the evolution of blockchain technology is the regulations around it. A lot of work is required in developing better regulatory policies that allow the technology the freedom to evolve at a steady pace and reach its full potential.

1. **Bibliography**

Bitcoin Price Drops Below $15k, Down 25% from All-Time High. (2017, December 22). Retrieved April 29, 2018, from<https://www.coindesk.com/bitcoin-dropped-22-5-to-weekly-low-from-all-time-high/>

Coinbase - Buy/Sell Digital Currency. (n.d.). Retrieved April 29, 2018, from<https://www.coinbase.com/>

Kobie, N. (n.d.). This man’s lost bitcoin is now worth $75m – and under 200,000 tons of garbage. Retrieved April 29, 2018, from<http://www.wired.co.uk/article/bitcoin-lost-newport-landfill>

Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System, 9.

SEC.gov | SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds. (n.d.). Retrieved April 28, 2018, from<https://www.sec.gov/news/press-release/2017-185-0>

The U.S. sold over 144,000 Bitcoins at an Average Price of $334. (n.d.). Retrieved April 28, 2018, from

<http://fortune.com/2017/10/02/bitcoin-sale-silk-road/>

Bauerle, N. What are Blockchain's Issues and Limitations? Retrieved from <https://www.coindesk.com/information/blockchains-issues-limitations/>

Malanov, A. (2017, August 18). Six myths about blockchain and Bitcoin: Debunking the effectiveness of the technology. Retrieved from <https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/>

(2015, October 16). BlockChain Technology Beyond Bitcoin. Retrieved from <http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>

Mulholland, A. (2017, July 12). Constellation Research. Retrieved from<https://www.constellationr.com/blog-news/blockchain-or-distributed-ledger-defining-requirement-not-technology-0>

Requirements for a blockchain in a business environment - Welcome to this course. (n.d.). Retrieved April 28, 2018, from <https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers/lecture/nTsVE/requirements-for-a-blockchain-in-a-business-environment> [Graphic depicting requirements for blockchain for business]

(Nicholas, Advancing blockchain cybersecurity: Policy recommendations for growth and innovation, Mar 7th,2018)