

Kevin A. Gutierrez

IT 104 – 005

September 19, 2018

The Block Chain Technology

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on <https://oai.gmu.edu/mason-honor-code/> and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Introduction

The Blockchain Technology has many facets to consider, some are potentially positive and other are not. We are going to explore some background of the technology, explore the law implications, ethical considerations, privacy concerns, and some of the social consequence of the application of Blockchain Technology. The Blockchain technology at its simplest descriptions is an immutable and decentralized public ledger of transactions between individuals and the transactions are verified to be unique and thus cannot be duplicated in the system.

Background information

The technology behind Blockchain exhibits the following set of characteristics: relies on a peer to peer network, uses public-private key cryptography, and it uses consensus mechanisms. Relying in a peer to peer network allows for everyone on the network to have a copy of the public ledger and all the transaction that were recorded in it, thus not needing to have a central database with a single point of failure. Using Public-Private cryptography allows for secure transaction to take place placed between individuals. The consensus mechanisms assembled within the blockchain support a tamper resistant data structure in which the system foundation is based on “[m]ost if not all blockchain-based networks feature market-based or game-theoretical mechanism for reaching consensus” (De Pilippi, P., & Wright, A. 2018). These blockchain features explain why this technology is so powerful and the impact is having on today society. The aspects of Blockchain Technology we are going to explore are: the potential benefits, the legal and ethical issues, Security concerns, and Social Effects.

Potential Benefits

The most important benefits of blockchain technology are data assurance authentication, data redundancy, transparency of transactions on the network, and the ability to create smart contracts.

Blockchains store data in a unique manner as compare to other technologies. Data is store with each of the peers in the network so no one person has the ability to edit the electronic ledger this secures the redundancy of the data. In an example of the power of this electronic ledger. “[i]n war-torn Syria, Iranian-Backed Shia settlers have invaded the country, claiming lands where former Sunni residents once resided. To prevent displaced Sunni residents from reclaiming their land, Shia settles have systematically torched land registry offices across the country. Had Syria implemented a blockchain-based land registry on a widely supported blockchain – such as bitcoin – before the conflict erupted, the torching would have had little effect. Because of the resilient nature of the blockchain, even if flames engulfed Syria’s traditional land registry system—and even if Syrian data centers were destroyed—copies of ownership records would remain safely stored on the computers of miners scattered across the globe who support the Bitcoin network. Because a blockchain is resistant to change, had Shia settlers taken control of the Syrian land registry directly and illegitimately assigned land to new Shia residents, displaced Syrians could still prove their previous ownership claims once the conflict subsided. By relying on the sequentially ordered records maintained in the Bitcoin blockchain, any displaced Syrian resident could use a blockchain to support a legal action to reclaim their land” (De Pilippi, P., & Wright, A. 2018) because there would be not one centralized point of attack on the blockchain the data is safe from being remove or edited by malicious actors.

Data inside a blockchain network is verify using Private-Public key encryptions and digital signatures. Here is the process as “[b]efore engaging in a transaction with a smart contract or another member of a blockchain-based network, a party must sign the transaction with their private key. The digital signature serves as evidence that an account initiated a transaction, narrowing the ability of the holder of a blockchain-based

account to refute the fact that a transaction occurred, unless a party can prove that the private key associated with the account was somehow compromised” as described in *Characteristics of Blockchains* (De Pilippi, P., & Wright, A. 2018), authentication of a transaction is one of the features of blockchain technology that is key to its extensive use and confidence on the system. Being able to verify a transaction and the transparency in which this is done is a major feature of the blockchain technology, take for instance the following situation. A known party had received multiple payments in the form of bitcoin to a known address, later this party was suspected to have died and disappear due to the lack of activity on the network. The party in question in order to verify that he was alive use the network to send out a series of transaction origination from this well known address with a note stating he was well, “the blockchain provided the necessary infrastructure to prove the integrity of the message and the authenticity of its source in a way that could not be repudiated” (De Pilippi, P., & Wright, A. 2018).

With smart contracts we can reduce the burden or verification from public and private entities by encoding legal and contractual provisions “into simple and deterministic code-base rules that will automatically execute by the underlying blockchain network” (De Pilippi, P., & Wright, A. 2018). Using code to enforce the law and contracts can help reduce the burden of record keeping from our private and public entities. Tax collection for example could be streamline into a simple process. Sales tax could be collected and remitted to directly to the government after each transaction, a smart contract can be set to submit the percentage allocated after each completed transaction by the store to the government.

Legal and Ethical Issues

Blockchain with all its bells and whistles comes with legal and ethical implication which are cause by the implementation and adoption of the technology. The main issues we are going to

focus on are: current legal view of virtual currencies, letter of the law vs intent of the law, supporting terrorism and money laundering, and the lack of privacy in the blockchain.

Using the blockchain technology as a medium of exchange was first introduced in 2009 “following the publication of a white paper by Satoshi Nakamoto in 2008” (William J Luther), at first Bitcoin was nothing more than an extravagant piece of code being traded for pennies between collector and aficionados. According to William J Luther in Bitcoin and the Future of Digital Payments Bitcoins’ value “climbed to roughly \$1.00 by February 2011 and then to nearly \$30.00 four months later before settling down to an average of just \$8.16 from July 2011 to February 2012”, this is not the first nor the only time that Bitcoin as a medium of exchange has fluctuated wildly up and down in value. Bitcoin is not money according to the Department of the Treasury and the Internal Revenue Service “virtual currency is treated as property” (IRS, Notice 2014-21), like a vehicle, real state, or a computer. This is because currency is issued by governments to finance its operations and thus having the power regulate, print, and tax the currency. Bitcoin is a decentralized peer to peer currency without the backing of any government and thus it cannot be controlled by any one government. Bitcoin cannot add more currency to its numbers thus making this a deflationary currency; a Government is able to print more money to meet its obligation, which usually causes inflation within the economy. Taxes are collected with the currency issued by the government, as is written on each bill we use “This note is legal tender for all debts public and private” if you wished to do business with the government you must use its currency, governments can’t tax bitcoin within the program, as this is not a feature of bitcoin. Regulation and case law will ultimately define and shape how virtual currencies will be treated. Natural language is how law are written, however smart contract relies on strict language to execute. When using blockchain to enact and process smart contracts we must be aware of the restrictions of trying to turn law into code. Natural language is flexible and ambiguous, while

computer code is strict and clear. When using code to turn certain laws with specific outcomes blockchain should help with the burden of record keeping and processing of transactions.

However when we turn open-ended laws into computer code we face the unescapable reality that by turning them into code we maybe be making these laws less flexible and could distort the meaning of these laws since blindly applying the wording of the law would violate the law's original intent. Consider how is not possible to come up with every possible contingency to a given situation, translating law into code will not work without a process to correct any possible misuse of the technology.

Terrorism and money laundering have been at the forefront of the blockchain technology.

Bitcoin along with other technologies that allow for the anonymity of those transacting with it has led to the creation of illegal marketplaces where the illegal sale of prescription drugs, weapons, child pornography, and drugs. Because bitcoin allows for the easy of transferring value anywhere in the world this has facilitated much of the dark market transaction thus supporting money laundering and possible terrorist activities.

Privacy in the blockchain although anonymity is one of the selling features of the technology, however it really is not very anonymous. Transactions are kept in a chronological order and cryptographic signatures link blocks thus enabling block-chain to form, these in turn provide an auditable trail of transactions, significantly increasing the probability of detecting patterns that could disclose who is on the other side of the transaction.

Security concerns

One of the security concerns that we are most aware of is called the "51% Attack" because of the blockchain it is a peer to peer distributed ledger the information is distributed and shared amongst everyone on the network, making changes to it would require that 51% of the network agree on the changes. So, in order to perform a 51% attack one party would have to have control

of 51% or more of the network resources in order to force a change in the data store on the chain. However, performing a 51% attack is very costly and sophisticated. Currently the ability of anyone to perform such attack is not possible, however as more resources are placed on a blockchain, an incentive for malicious parties will eventually make it worth it for a party of even a foreign government backed effort could come to be.

The lack of privacy in the system is one concern, the blockchain “provides an auditable trail of transaction, significantly increase the probability of detecting criminal activity” (Killian J McCarthy, 2018), although we want to root out criminal activity from any system the cost at which the blockchain does this, for some the cost might be too high. Using statistical analysis of the data in the chain, a person, government, corporation can disclose enough information about one person to create a mosaic view of an individual thus violating any privacy right that people believed to have.

Social Problems

As with any revolutionary technology blockchain will bring about social problems that must be addressed on a proactive or reactive manner. With improvement in performance in the private sector due to the use and integration of blockchain technology certain jobs in the economy will no longer be relevant. Blockchain systems are subject to malicious 3rd party actions that must be accounted and planned for. The loss of security of the government over the medium of exchange could cause economy wide issues. The loss of anonymity while performing everyday transaction could be dangerous and discriminatory.

Further required research

Blockchain technology is the new kid in the block and with such status the information is still being developed. Continue monitoring and research on this subject help understand the use

and long-term implications of the technology. Further research current uses of the technology and understanding how government regulation affect the current technology.

Conclusion

Block chain technology is a powerful new way to handle data, however, with its implementation chaos will be cause amongst our society systems that are use today to handle everyday transaction. I believe that it's benefits will outweigh its downfalls and the technology will be used to make Governments more transparent make the ability of people to identify themselves easier. With the proper laws and regulation privacy could be protect and allow the full of the blockchain technology.

References

- De Fillipi, P., & Wright, A. (2018). Tamper-Resistant, Certified, and Authenticated Data. In *Blockchain and the Law*. Harvard University Press. Retrieved September 20, 2014, from <https://www.jstor.org/stable/j.ctv2867sp.9>.
- De Pilippi, P., & Wright, A. (2018). Characteristics of Blockchains. In *Blockchain and the Law*. Harvard univeristy press. Retrieved September 20, 2018, from <https://www.jstor.org/stable/j.ctv2867sp.5>.
- Dove, T. (2018). Career Outlook It's not rocket science. It's FINTECH. *Career Communications Group*, 33(1), spring, 39-43. Retrieved September 20, 2018, from <https://www.jstor.org/stable/26448985>.
- Middlebrook, S. T. (2014). Bitcoin for Merchants: Legal Consideration for Businesses Wishing to Accept Bitcoin as a Form of Payment. *Business Law Today*, 2014(11), 1-4. Retrieved September 20, 2018, from <https://www.jstor.org/stable/businesslawtoday.2014.11.03>.
- Steinmetz, F. (2018). USING BLOCKCHAIN TECHNOLOGY FOR THE PREVENTION OF CRIMINAL ACTIVITY. In K. J. McCarthy (Ed.), *The Money Laundering Market*. Agenda Publishing. Retrieved September 20, 2018, from <https://www.jstor.org/stable/j.ctv5cg8z1.11>.
- Turner, W. J. (2016). Bitcoin and the Future of Digital Payments. *Independent Institute*, 20(3), winter, 397-404. Retrieved September 19, 2018, from <https://www.jstor.org/stable/24562161>.
- USA, Department of the Treasury, Internal Revenue Service. (n.d.). *Virtual Currencies*. Retrieved September 25, 2018, from <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>