Revolutionizing Technology, One Block at a Time

Jake Derkowski
Department of Computer Science
Cyber Forensics Intelligence Center
Sam Houston State University
Huntsville, TX, USA
jad084@shsu.edu

Narasimha Shashidhar
Department of Computer Science
Cyber Forensics Intelligence Center
Sam Houston State University
Huntsville, TX, USA
cxv007@shsu.edu

***Abstract*—When people hear the word *cryptocurrency*, Bitcoin is typically the first thing they think of. However, there are hundreds of active cryptocurrencies (or altcoins) all designed for a specific purpose, whether it be to fix the shortcomings of Bitcoin or to place more emphasis on a particular aspect of the blockchain–the technology in which they are built. This paper is meant to inform the reader about the blockchain technology and the potential that is had to revolutionize the way in which data is used, transferred, shared and stored. At the least, we wish to rid any prejudice that one may have because of Bitcoin's infamous call to "glory".**

Bitcoin and other blockchain technologies are not inherently bad, created for cyber-gangsters for cyber-gangsters. In fact, the blockchain applications and technologies have the power to secure data more efficiently in ieiu of the stabilization of quantum computers. This technology has the power to directly save the lives of various types of patients. The biggest obstacle we face: close-mindedness.

***Index Terms*—blockchain, bitcoin, decentralization, mining, ledger**

I. Introduction

In recent years, Bitcoin's popularity has grown significantly; it is no longer only known to computer nerds and cyber criminals but has become family table talk. Bitcoin is a cryptocurrency that was developed with the intention to create a monetary system that is not controlled by the governments of the world, placing the power into the users' hands. At a high-level, Bitcoin is a "digital cash that is transacted via the Internet in a decentralized trustless system using a public ledger called the *blockchain*" [1]. At a high-level bitcoin is a new form of money that uses the BitTorrent peer-to-peer file sharing plus utilizes a public-key infrastructure for its security [1].

As Bitcoin's popularity increased, more alternative coins, called *altcoins*, surfaced trying to overcome the shortcomings that were found with Bitcoin. This was done by placing more emphasis on various aspects of the blockchain technology resulting in many different coins. In understanding what cryptocurrencies are and how they are able to achieve these goals, we must turn towards the technology upon which it is built: the ***blockchain***.

[2] defines blockchain as a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus among peers. This section we will break down these characteristics and show how they are made possible. Firstly, *peer-to-peer* simply means transactions are made directly from the sender and the receiver. There is no intermediary such as a bank or government agency.

Blockchain is a *distributed ledger* which is defined by [2] as a ledger that is spread across the network among all peers in the network, with each peer holding a copy of the complete ledger. This assists each peer in their role when deciding on the validation of a node by looking for anomalies and the like.

Blockchain's ability to be *cryptographically-secure* is pivotal in its likelihood of its success, especially in the dawn of the age of quantum computing where all current encryption will render themselves useless. This topic deserves its own paper, but when this time comes, and it will because the technology already exists, it is imperative that we already have a different cryptographic system in place. The effects of not being prepared can only be speculated–if an adversary developed one first the effects would be devastating.

The Blockchain ledger is always *append-only* meaning that records or transactions cannot be inserted between two already existing blocks but rather a new block must fit at the end of the current ledger. This reiterates the immutability of the ledger and of course it's security. It is possible to change data in completed blocks, but it is very difficult and requires the consent of the other peers within and around that node.

The rest of this paper will investigate more into what can be built upon these characteristics that we have defined above. First we will look at cryptocurrencies other than Bitcoin, their benefits plus their potential. Then we will try to see if we can think of ways this potential can be pushed into reality, finally we will look at some use cases attempting to do just this.

II. Literature Review

Let us take a look at a few "altcoins" and identify the differences between them and Bitcoin. As mentioned, the goal of a cryptocurrency will determine the way it "looks" and behaves. The first altcoin we will examine will be XRP, a coin created by Ripple Labs.

A. Ripple and Litigation

The appeal of the blockchain extends far outside the realm of wanting independence from government regulation and

monitoring, one of the major appeals is the quick transaction speed regardless where and who the involved parties are, these attributes are exceptionally true with the cryptocurrency XRP made by Ripple Labs [3]. In recent cryptocurrency news, the SEC has shut down Ripple for the threat that they impose by claiming that they have inaccurately described their agenda–based on their actions they should be labeled as a security.

Ripple Labs has now been shut down for well over a year. Although the case was initially set to be closed Summer 2021 experts think it could go another year, maybe even into the 2023 year. Even though production of the coin has been required to be paused and major coin trading platforms have suspended trading, the price of XRP has continued to rise. It reached its ceiling around $3.00 USD where it stayed for only a couple of days. Currently it has dropped below $1.00 USD but a lot of this can be attributed to the massive bull rise beginning summer 2021. This legal case certainly has posed a grave threat to Ripple but it has also brought it publicity and is still recognized as a likely contender as the cryptocurrency to become universal due to its quick and extremely cheap transactions.

It is apparent that the increased popularity of Bitcoin and other cryptocurrencies have created a threat against governments around the world and they have begun to formulate possible methods of regulating its use or refused to acknowledge the circumstances and resorted to banning its use. Banning its use, as one would expect, has failed miserably so this response has almost been thrown out altogether. Then there are the cases where governments were able to acknowledge this trend in digital payments and have tried to jump out in front of it all. Iran, for example, has backed the development of its own cryptocurrency and plans to continue its support until it takes over as the nation's currency [4].

B. Etherum

Not all applications built upon blockchain are meant to shutout government involvement in economics. The second most popular cryptocurrency (to date) called Ethereum was built to serve as a huge platform from which applications can be built on [5]. This is also the reason why there have been so many cryptocurrencies created, especially those " meme coins " like Dogecoin.

Etherum introduced a new feature into cryptocurrencies called a *smart contract* which are essentially just logic apps. A smart contract is basically like a trigger for a given code to be executed automatically [5]. However it may not be apparent initially, this furthermore eradicates the need for a third-party. This is even true for more complicated transactions like buying an United States bond, payment for a utility (wate, gas, electricity) through the use of *tokens*–a legal representation of a given unit of a given good. For example one electrical token which is equivalent to 1 kilowatt. These applications are called *dApps*.

1) dApps: Decentralized applications [6] are taking advantage of Ethereum by systematically beginning to revolutionize the financial and banking industry by providing a medium in which is used for asset registry, inventory, and exchange. This, at least from a digital standpoint, has the power to eliminate theft on the digital front which could also very well be transposed in the physical. This may sound ridiculous, but when machines are instructed to use their owners inventory to make a product it is given an item that is not supposed to be there errors will begin. If these errors are able to be overridden, then there will exist a log of this activity. Proof of the manual override will guarantee that the operator knew that they were about to do something that was against protool–will be found guilty without a doubt.

Other dApps may include things like keeping a database of votes, ideas, reputation, intention, health data, and information. If votes were to be cast using blockchain then there would be no way any entity could go back and alter the actual ballots.

Last example of a dApp could be a registry of digital rights to art [6]. With the increase of this category of art counterfeiting would become impossible because of the immutability of the block chain!

C. Data Security and the Medical Field

Using blockchains within the medical field has already been touched upon in the preceding sections. We know that a lot of the benefits that we have discussed is a result of the immutability of blockchains. So for this section, let us take a quick look at an instance where blockchains have already been implemented.

III. Cryptocurrencies on the Blockchain

IV. Some Considerations

It has been stated why the adoption of blockchain technologies would be benefical on nunerous fronts, but with that being said there are still some precautions that should be taken as we go about this process.

- Inform the public

  We need the public to understand what the technology is and why it will benefit them
- Dissolve Predujice

  We assume from our own experience, that there is a large percentage of people who have the wrong perspective of blockchain technologies because of the shaky debut of Bitcoin and its use in illegal markets on the dark net. This may be initially difficult just because of the unwillingness to listen, but when the technology is explained it will be shown that it can be trusted–that we are not trying to hide away from the government. We are only trying to take advantage of technology that will improve our lives.
- Develop for yourself!

  Lead by example

Last consideration that we feel necessary to share on the cybersecurity regarding the blockchain. As stated by the National Institure of Standards and Technology (NIST) almost entire involves that of human error [7]. So long as the other

standards and principles are followed then there should be nothing new (policy or procedure) that has to be learned.

This will make the integration less intimidating because unlike most new technologies comes new terminology and ways of doing things that will discourage the average person. The reality is that their time can be spent in a more efficient way like doing things to directly grow their company. There will be some work initially, but once integrated then it can essentially be business as usual!

V. Conclusion

It has been shown that there is much more to the *blockchain* than Bitcoin and other cryptocurrencies because it has applicable uses in nearly every field imaginable.If we can take advantage of the Ethereum platform and begin developing our own solutions others will see the simplicity, reliability, and attractiveness of blockchain. With the security that it can provide us in spite of quantum machines and the great advantages and certainty gives us in the medical field, this is a technology that at least deserves to be further investigated– but by everyone!

References

[1] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of economic Perspectives*, vol. 29, no. 2, pp. 213–38, 2015.

[2] I. Bashir, *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing Ltd, 2018.

[3] L. Martin, "Ripple effects: How in re ripple labs inc. litigation could signal the beginning of the end of the payment platform," *Duke L. & Tech. Rev.*, vol. 19, p. 1, 2021.

[4] "View of bitcoin and future of cryptocurrency." https://journals.christuniversity.in/index.php/ushus/article/view/2112/1717. (Accessed on 07/31/2021).

[5] "Various types of cryptocurrency: How many cryptocurrencies are there?." https://www.bitdegree.org/crypto/tutorials/types-of-cryptocurrency. (Accessed on 07/31/2021).

[6] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[7] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.