The Future of Blockchain

Elijah N. Gartrell

Old Dominion University

COVA CCI Undergraduate Research

Mentor Rui Ning

Table of Contents *(for professional papers)*

Abstract *(for professional papers)*

Blockchain is the leading technology for cryptocurrencies, NFT's and other online marketplace transactions that go through it because of it's secure technology and how they distribute their data with Smart Contracts. This report shows how we can use Blockchain for other uses in our world and how it could advance us in the cybersecurity aspects. Showing also why we should use blockchain with basic cybersecurity concerns as in: Malware Detection, Voter Fraud, and Medical Record Security.

The Future of Blokchain

Introduction

Blockchain, a word that troubles many, some hear it and automatically brush it off because they think of cryptocurrencies in which they do not believe in. Some get intrigued, because that facet of the world and future is still up in the air, but yet many still are not sure what it really is. Most often it is just associated with cryptocurrencies and NFT's people have limited blockchain to only that, but in the future world we are living in it has so much more real world capabilities than just that. Blockchain could help with the keeping of medical data, protecting voters and their vote, even detecting malware on your computer. Blockchain is the future of the world and today I will go through what blockchain is and how it's technology works. After that I will talk about the many capabilities of blockchain and talk about three main cybersecurity/worldly issues that blockchain could truly revolutionize how we use our technology. Those three main issues include: Voter Fraud, Malware Detection, and Medical Record Security. By the end of the paper, you will have a deeper understanding of what Blockchain and how the technology works .In the world there are plenty of authoritative powers, many who hold much power over our everyday lives. For example, banks are an authoritative centralized power that runs our money, the government is another centralized power. See what those two have in common is that they are slow to process transactions, along with holding your assets in which you should have control over. Now that is where blockchain comes in, there is no authoritative power, it is decentralized and all the information is stored on everyone's system, therefore unless every single computer on that network goes down your information is still intact and going. But that begs the question: what is blockchain?

What is Blockchain?

.Blockchain is a distributed ledger that allows anyone to enter data, it is tamper resistant and tamper evident (NIST,2022). Essentially a peer-to-peer network where people can conduct transactions without needing an authoritative power conducting it, making it decentralized. What blockchain works on is called the Blockchain network, there are two categories of the blockchain network; permissioned and permissionless models, which help determine who can publish blocks on the network. Permissionless blockchain network means that anyone can publish a block of data, these are often open for anyone to download online and open source code. Permissioned blockchain networks only authorized users can publish blocks, these are used most times for businesses when you need to know exactly who is publishing data on the network. In order for blocks to be on the network they must be cryptographically secured by hash functions.

Hash functions by definition are data that is converted to alphanumeric code with no change to the data that can be easily computed by computers. Cryptographic hash functions are what is used by blockchain and has many security features such as: being collision resistant, preimage resistant, and second preimage resistant. Collision resistant means that there are no input that could give you the same output, therefore every hash will be different and no failure by the computer if it were to see the same two hashes. Preimage resistant this refers t nce given the hash function of someone's data you cannot reverse engineer it to find the input . There is no way to guess the hash with the given output and it is computationally impossible. The main cryptographic hash function that blockchain uses is the Secure Hash Algorithm and output of 256 bits(SHA-256). This is used because of how many possible digest values there are in SHA-256 making it collision resistant, because it is almost impossible to get the same two hashes.

History of Blockchain

The idea of blockchain was worked on for years throughout the late 1980s and early 1990s. In 1991 the first "blockchain" was created when several signed documents were held on an electronic ledger. Several years later in 1998 Nick Szabo worked on "bit gold" which was a decentralized digital currency. Tw years following in 2000 the idea for cryptographically secured chains came to play. Then after that arguably the most essential of them all, the paper *Bitcoin: A Peer to Peer Electronic Cash System,* pseudonymously published by Satoshi Nakamoto, in which gave the first model for blockchain and how it could be used for this new digital currency bitcoin. Then after that in 2009 the very first blockchain was used for public transactions in Bitcoin. Now of course we all know how the story went from Bitcoin, and how all of you reading this wish you would've invested even 50$ and you'd be rich right now but that's not what we are here for. Now that you have some background on it, let's get into the major components of blockchain and how the technology works.

Blockchain Transactions

A transaction on the blockchain, are interactions between two different users on the blockchain network. The most basic example of this being two users exchanging cryptocurrencies. But in order for any transactions to happen there must be an input and an output.

Inputs - This is the main list of assets being transferred to the other user on the network. In these transactions the inputs will always be referenced by the previous transaction on how they received the asset. This calls for a truly more secure trading block, along with being able to trust someone that you do not know.

Outputs - The users on the blockchain network that will be receiving the digital assets. Outputs specifically identify the specific amount of digital assets to be sent.

Figure 1 shows the basic blockchain transaction.

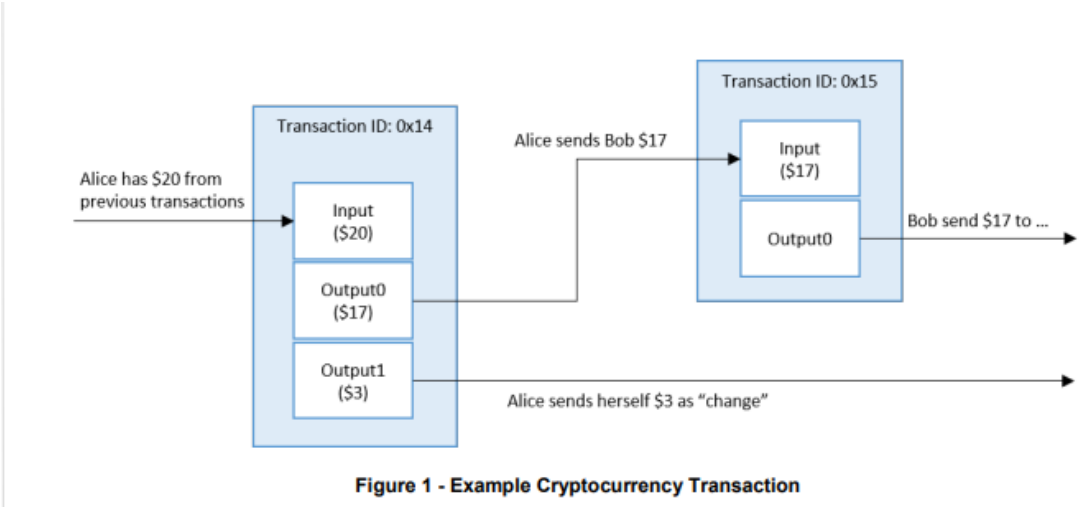


Figure 1 - Example Cryptocurrency Transaction

Here we see the basic blockchain transaction with the input and output. Alice shows the 20$ from her previous transactions, and the output is specified to be 17$. Once it is sent it now becomes Bob's input because that was his last transaction. While this was the base blockchain transaction there are many more capabilities than sending digital asset, people can also send data to each other.

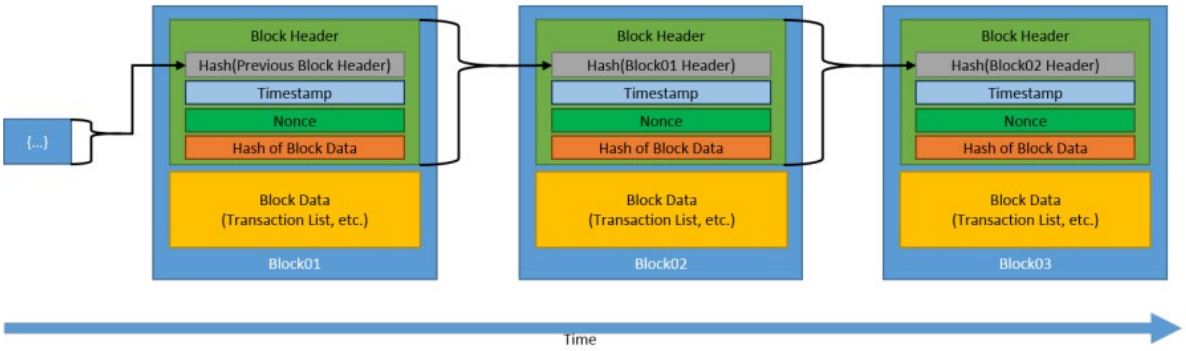
Asymmetric Key Cryptography

While a few ways that you could trust people on the network have been shown, this is one of the main ways that trust is established in the blockchain network. Blockchain uses asymmetric key cryptography which uses public and private keys in order to protect data and information. The private key use is to encrypt a transaction in such that anyone with a public key can decrypt it. Private keys are also used to digitally sign transactions. Public keys can be used to verify the signature of the private keys, and get addresses.

Blocks and Ledgers

Blocks and ledgers are the two most essential parts to a blockchain because they are what make up the blockchain. The ledger is a collection of transactions that is kept digitally now. The ownership of the ledger is distributed making it decentralized and no one authoritative power owns it or looks over it. The blockchain uploads the ledger and distributes it among plenty of computers and keeps multiple backups. The benefits of this distributed ledger is that everyone on the blockchain network can have their own copy of the ledger.

Blocks are what hold the individual data on the blockchain. Each block holds the block head and block data. Data includes previous transactions within the block and any digital assets. The block header includes the block number, the previous blocks hash value, the block's hash value, and a timestamp of the block. Each block is chained together through storing the previous block's hash value hence "BlockChain" as shown in Figure 2.



Consensus Model

So now that we have the basic principles of a blockchain now we can get a little more in-depth. One of the main points we hit would be who gets to publish the next block on the network? The way to solve the issue of multiple people trying to publish blocks at the same time is the consensus model. There are 5 consensus models that each do their own thing for permissionless and few permissioned blockchain networks. First is the Proof of Work consensus model, this is the most complex consensus model as well. Proof of work requires you to solve a

“computationally intensive puzzle.”(NIST,2018). Solving said puzzle will be proof to be able to show the publishing node that they can publish a new block. The benefits of this model are it is hard to have a DOS(Denial of Service Attack) you cannot flood the system with bad blocks. Pretty much most computers can solve the puzzle and be ready to submit the next block, Ethereum and Bitcoin are the two cryptocurrencies that implement this. Proof of stake consensus model is the next one, this consensus model essentially works off of how much “stake” you have in the blockchain. The theory is if you have more stake you are less likely to want the system to fail. Stake can be most times determined by the amount of cryptocurrencies you have. The advantages of the Proof of Stake model are stakeholders hold much of the power in this model, along with not having to do as much as the Proof of Work model. The issue with the Proof of Stake model is that the stakeholders could form to make a centralized power and try to control the blockchain network . Round Robin consensus model, this consensus model is based around the nodes taking turns and waiting your turn to publish a block, not many advantages of this model because it heavily relies on the publishing node not being compromised and allowing anyone to publish the blocks. Proof of authority, this consensus model uses your real world identity to help verify who you are. Whoever is to publish the next block must have their identity verified first. Lastly, proof of elapsed time consensus model, this you request a wait time to a computer similar to a deli clerk.

Smart Contracts

Smart contracts are code and data that are set to a specific set of rules and regulations that need to be met, once met the contract will perform what it is meant to do on the blockchain. Smart contracts became popularized with the cryptocurrency Ethereum. There are many uses for smart contracts but not all blockchain networks can run smart contracts. Smart contracts are all

final, there is no changing it once the contract is made it is going to run and if the requirements for the smart contract is not met then it will not run.

Blockchain Limitations

Blockchain is not immutable, although there are many people who say it is blockchains are not immutable.

Other Uses in Blockchain

Blockchain has a multitude of uses that we could use aside from just crypto. Voter fraud, healthcare and records, and even detecting malware could all be special uses. Implementing blockchain technology to any of these uses will advance it and reduce many cybersecurity concerns that we deal with in our everyday lives.

Election Fraud and Blockchain

2016, the year many will never forget especially those who care deeply about politics. The biggest if you can remember is the “illegal” votes that were counted in this election. Some speculate Russia, others say certain states should have their votes recounted. This continued 4 years later with the 2020 election and many of us remember the trouble it caused to recount the votes and saw how delayed the process had become. If you have ever been to a voting booth, they consist of these big clunky machines that are getting more and more outdated by the day. Some states even use voting machines that aren’t even in production anymore. The way we could solve this is by using blockchain technology in order to vote. This could be implemented by using a smart contract as well.

Malware Detection and Blockchain

Malware gets more and more destructive by the day and although our computers and firewalls are getting stronger we can never be too sure. We can implement a deep belief neutral

network as the detection method. The way that it works, new files that are added to node in the network are sent through a detection engine that produces a numeric value of the probability of how malicious the files could be. Then the numeric possibility along with the file's hash are sent to the blockchain. Other nodes in the peer to peer network has not validated it yet as it is still waiting on the validation of the peer to peer network. If the numerical value is at it's threshold it will be shown as an invalid transaction. Another way is we could implement a firewall blockchain styled network is this. After a new node is in the network a detection engine is sent it's way immediately. This will start out on just the network not the blockchain yet, after it is passed through the detection engine and given a numerical value to how malicious the node could be it is now sent to the blockchain as a transaction. After that the node can get it's final verdict on whether it can be trusted or not through the other nodes on the chain. After the trust is given it is updated after every transaction to see if the node deviates any. If the node does and any modifications happen to the file it is immediately deemed to be invalid and will be an invalid node from there on out.

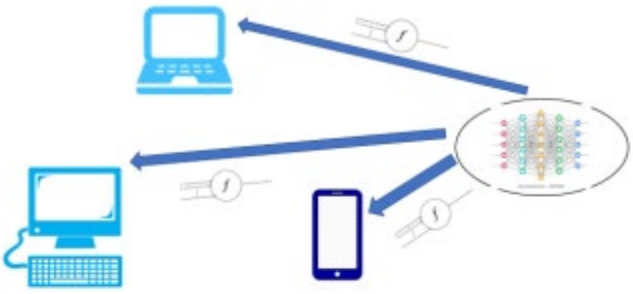
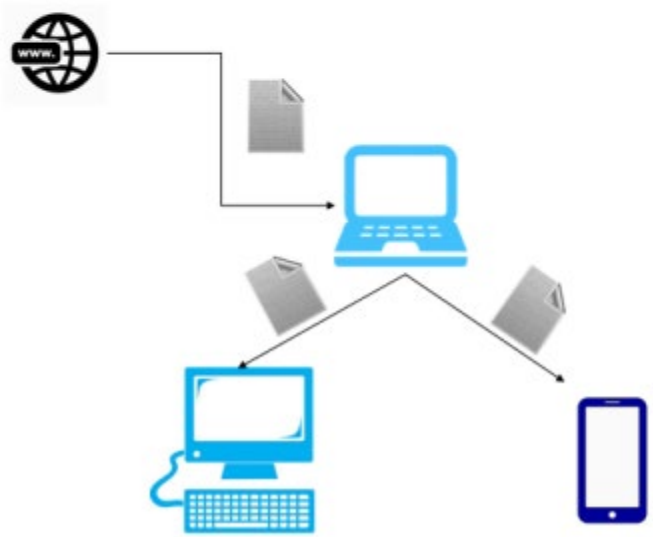


Fig. 1. Uniquely trained model shipped (by a central server) to each node in the P2P network.



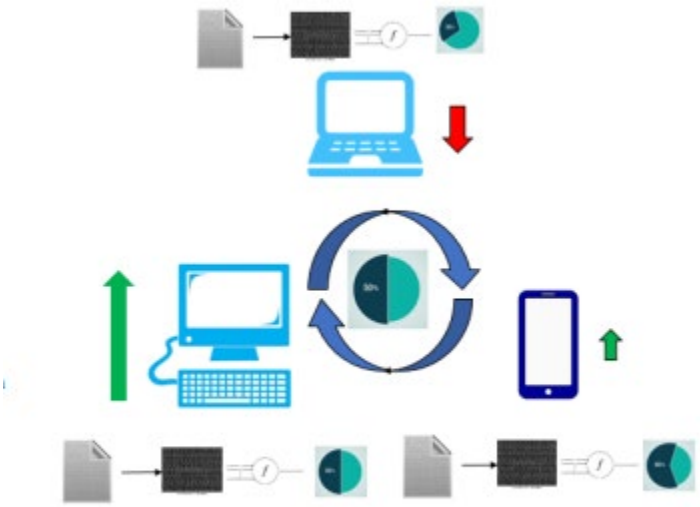


Fig. 3. Each machine processes the same file and determines the probability of the file being malicious. The network finally comes to a consensus.

Medical Record Keeping

Medical records could be safe and secured on the blockchain along with even getting alerted when your medical data is in use giving people more rights over their data and privacy. Patients can use a blockchain wallet with all their medical records and data inside, once data is pulled it will be deemed as an transaction, and patients then can get paid for their medical data being used in research or other various reasons. Your information is also much more secure with it being ran by you and not allowing the dated hospital systems to keep your records. Last year alone more than 40 million patient records have been compromised reported by the federal government.

Why We Should Implement Blockchain

Blockchain should be implemented into our everyday lives because there are fast transaction rates, it is reliable, and easy to implement. Blockchain also has great record keeping capabilities, for businesses whenever someone does something on the network and it needs to be traced you will know exactly who did what and at what time. Blockchains are secure, whether you're using it for voter registration or

Conclusion

Now that you have truly seen all that blockchain can accomplish in the world today ask yourself why not use this, or even how it could be implemented at your job or workplace. Blockchain technology could help us advance and get passed current issues we are dealing with

now and also mitigate any other that would arise. As the world becomes more and more connected we are going to need more places to store our data and make sure it is secure.

References

Yaga, D et al. (2018). NIST Blockchain Technology Overview. *NIST* , https://csrc.nist.gov/publications/detail/nistir/8202/final

Kwefati, A. (2021). HuntChain Project *A Blockchain Based Malware-Detection Tool*, *Diva*, http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1604252&dswid=-5472

101 Blockchains. (2020). *When Was Blockchain Invented?*. 101 Blockchains. Retrieved March 2nd, 2022, from https://101blockchains.com/blockchain-invented/

Rajee, S et al. (2017). *Decentralized firewall for malware protection*. Arxiv. Retrieved March 2nd, 2022, from https://arxiv.org/pdf/1711.01353.pdf

Rayamajhi, P. (2019). *Malware Detection Using Blockchain Technology*. Medium. Retrieved March 3, 2022, from https://medium.com/@parishilanrayamajhi/malware-detection-using-blockchain-technology-bca2a67f5dd

Miller, J. (2021). *How Blockchain Can Be Used for Personnel Health Record Storage and Security*. Himms. Retrieved March 18, 2022, from https://www.himss.org/resources/how-blockchain-can-be-used-personal-health-record-storage-and-security

Boring, P. (2020). *The Future of Voting is Blockchain*. The Digital Commerce. Retrieved February 25, 2022, from https://digitalchamber.org/the-future-of-voting-is-blockchain/

Singh, N. (2020). *How to Implement a Voting Smart Contract*. Dev. Retrieved February 25, 2022, from https://dev.to/niharrs/2-voting-smart-contract-2h7o

Solidity. *Solidity by Example*. Soliditylang. Retrieved March 30th, 2022, from https://docs.soliditylang.org/en/v0.8.13/solidity-by-example.html