An Empirical Review of Blockchain Algorithms for Cryptocurrency Mining

Jiangda Zhao (jiangdazhao1@gmail.com)

Abstract— Blockchain and its first implementation Bitcoin have gained widespread attention in the past few years, and the blockchain system today is comparable to the internet in its early years. Blockchain has many similarities to the internet: both are decentralized networks, without a single point of control. For example, in the Bitcoin system, anyone can download a Bitcoin program and start participating in the system–no authentication needed. Additionally, both are emergent technologies, with companies investing heavily in the technologies' initial years of development: Ethereum has been endorsed by over thirty large firms. [5] Lastly, both have the potential for a myriad number of uses. Blockchain system have been studied for use in the sharing economy [7], as well as being considered by the US government. [4] Blockchain technology presents an exciting future due to it being an emergent, rapidly developing technology, being decentralized, and having many diverse uses.

Index Terms— blockchain, Byzantine fault tolerance, cryptocurrency, cryptography, distributed systems, hashing, mining, networks, nodes

1 Introduction

Just as how the internet revolutionized communications in the 1990s, blockchain has the potential to improve upon the storage and access of important information. In 1989, Tim Berners-Lee proposed a new framework, called the World Wide Web, by which computers could be linked together under a common protocol. The source code which computers operated by was released to the public, spawning rapid development of online services. The transparent framework that is the blockchain was proposed by the entity Nakamoto in an anonymous white paper in 2008. [6] Similar to the early days of the World Wide Web, the public nature of blockchain applications today is helping businesses and individuals create myriad uses. Proposed uses of blockchain technology encompass the business, law, and communication sectors. [8]

There are three main types of blockchains: public blockchains, which are open to anyone to participate in, consortium blockchains, which are led by a select group, and private blockchains, internal blockchains run by a company. Examples of public blockchains are Bitcoin and other cryptocurrencies, while private blockchains include IBM's Hyperledger.

The genesis of the blockchain wave that we see today began with the publishing of Nakamoto's whitepaper, which itself was influenced by Adam Back's Hashcash. [3] The blockchain concept, along with its first use Bitcoin, were created at the same time in 2008. Nakamoto himself may have been the first to use the Bitcoin system when it was first proposed. Throughout 2009, the Bitcoin system remained largely unbeknownst to the general public.

In late 2010, the first Bitcoin market exchanges emerged, enabling anyone to buy and sell Bitcoins for fiat currencies. These cryptocurrency exchanges behave similar to, but on a smaller scale than conventional publicly traded exchanges. The first of these exchanges was Mt. Gox, which kept its position as the largest Bitcoin exchange through 2013. Mt. Gox was the first cryptocurrency exchange that allowed anyone to buy and sell Bitcoins for USD. Around this time, other Bitcoin exchanges started gaining increasing popularity and increased market shares. Up until April of 2013, Mt. Gox controlled seventy percent of the total Bitcoin market share.

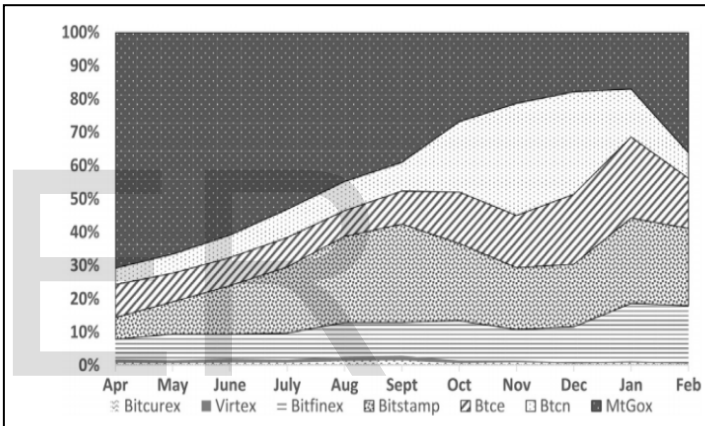

Fig. 1. Trading volumes of cryptocurrency trading platforms in the wake of the Mt. Gox hackings.

During these first few years that Bitcoin's blockchain made its entrance, the price of Bitcoin underwent several rapid surges. The first surge occurred in January 2011, and the price of Bitcoin reached parity with USD in February of 2011. Later in spring of that year, the price of Bitcoin underwent another dramatic surge, increasing from $1 to $10. Bitcoin's price underwent another surge in the first quarter of 2013, increasing from $10 to $100. Lastly, Bitcoin's price surged from $100 to roughly $1000 in September and October of 2013. This, until recently, was the peak of Bitcoin's price.

In May 2013, Mt. Gox was indicted of monetary fraud. Thereafter, the US government seized funds that Mt. Gox held at Dwolla, an online payment service, and Wells Fargo, after accusations of illegal money service. Nevertheless, Mt. Gox continued to remain the largest Bitcoin trading platform. It was not until February of 2014 that Mt. Gox suspended Bitcoin with-

drawals, effectively stopping all trade on the platform. Soon after, Mt. Gox declared bankruptcy, and revealed to the public that it had lost some 700,000 Bitcoins to online hacking.

Recently, other cryptocurrency trading exchanges have enjoyed increased attention due to the failure of Mt. Gox. In the aftermath of Mt. Gox's bankruptcy, the price of Bitcoin suffered a dramatic decline to about $100. The failure of Mt. Gox taught other cryptocurrency exchanges to implement stricter procedures, such as KYC (Know Your Customer) and AML (Anti Money Laundering) laws. In addition, the overall market behavior changed dramatically. In the early market before the Mt. Gox failure, the BTC to USD price was driven primarily by speculative investment. The price showed limited correlation with economic fundamentals such as US interest rates. In the later market, speculative investment had limited impact and economic fundamentals heavily influenced the Bitcoin price, indicating that investors had become more rational

Technology in Bitcoin mining, which forms the backbone of the Bitcoin system, have become progressively advanced and efficient as miners enter into an arms race. In the Bitcoin system, miners with more computing power get a bigger share of profits earned by the network. In 2009, Bitcoin was dominated by CPU mining, but in late 2010, miners switched to faster graphics cards (GPU) mining. Field programmable gate arrays, offering the ability to be custom-programmed and thousands of times more computing power, appeared in mid 2011. FPGAs were quickly replaced by the even faster application specific integrated circuits (ASIC) in early 2013. Today, all Bitcoin miners use ASICs and the total mining power is concentrated in the hands of a few individuals, leading to an oligopolistic market. The top five miners, all based in China, reap eighty-five percent of the profits, leading to concerns about the security of the system.

Along with the Bitcoin system, other cryptocurrencies such as Ethereum and Ripple have emerged, promising alternative and better systems to Bitcoin. Ethereum uses smart contracts that are hard-coded into the Ethereum network and protect against default by one of the agreeing parties. An example would be escrow payments without a third party, in which the developers' code handles all payment logic. Ethereum is a new cryptocurrency but has seen astronomical growth in 2017, increasing 3,000 percent in price. Ethereum was developed and came online in 2016 as an improvement to Bitcoin, and its founder is Vitalik Buterin.

Ripple, the third largest cryptocurrency behind Bitcoin and Ethereum is a decentralized, friend-based payment system. Newer cryptocurrencies such as these seek to reduce the technological arms race seen in Bitcoin and to place money under control of financial institutions. Financial institutions will be better equipped to implement AML and KYC, providing a source of consumer protection.

2 Theory and Mechanics of the Bitcoin Blockchain System

The basic principles of the Bitcoin blockchain system are outlined in Nakamoto's seminal whitepaper titled Bitcoin: A Peer-to-Peer Electronic Cash System. At the core of Bitcoin's blockchain is a digital ledger—the blockchain—replicated across a network of computers. A digital ledger is simply a database which can hold data such as text, numbers, and images. In this case, the ledger, or blockchain, holds records of financial transactions that occur throughout the peer-to-peer network. Comparable to a physical accounting book, the ledger timestamps each transaction. Ledgers are synced between all members of the network to ensure that if the data on one node is corrupted, such as by hacking, the integrity of the data on other nodes is preserved. Thus, the digital ledger is kept intact using a fault-tolerant peer-to-peer system.

When a person joins the Bitcoin network via a computer, their computer links up with other computers and becomes a network node. The person's computer then communicates over this meshed network, listening and storing transactions that it hears about, as well as adding newly created blocks to its blockchain. Nodes operate independently, acting as transmitters of information. In some cases, a node becomes a miner if it has substantial computing power and can help verify the validity of transactions.

The blockchain itself uses cryptographic mechanisms to make Bitcoin secure across a web of interconnected nodes, with each node independently processing and organizing transactions that it hears about into blocks of transactions. Blockchain thus makes it difficult for an attacker to forge or alter transactions stored. This security is accomplished through encryptions, a pseudo anonymous identity verification system, and incentivized competition between nodes.

The blockchain system ensures security through hashing algorithms. Hashing algorithms are secure, difficult to reverse-engineer, and fast, making them ideal to secure blockchain systems. A hashing algorithm, such as the Secure Hash Algorithm (SHA256), which is used in the Bitcoin network, takes a data input of an arbitrary length and compresses it down to two hundred and fifty-six bits. The output of a hash is a mixed string of letters and numbers. SHA256 has the property of being collision-free, meaning that no two different inputs to the SHA256 that generate identical outputs have been found. Keep in mind that while a hash collision has never been found, it is entirely possible for two hashes to collide if the numbers are large enough. However, for practical purposes, it is safe to assume that no two hashes of different inputs will realistically produce the same output. In Bitcoin, hash pointers—data that tells where the hash was stored and what the last value of that has was—utilize the collision-free nature of hashes to improve security.

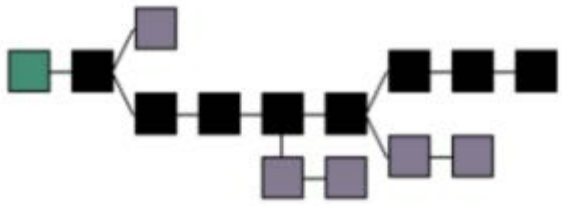

Fig. 2. Architecture of a blockchain system, showing a main branch and side branches.

In Bitcoin's blockchain system, there are two types of hash pointers used to safeguard against tampering by an adversary. The digital ledger that comprises the Bitcoin system is made up of many thousands of transactions that are heard over the Bitcoin network. These transactions are grouped by time—all transactions occurring within ten minutes are lumped into one block—and the blocks are connected by hash pointers, forming a long, almost-linear chain. The chain extends back to the genesis block—the first block on the blockchain—on which other successive blocks are linked. Along the way, because of block-creation dynamics which we shall later discuss, there are orphan blocks—blocks connected sideways to the main blockchain. The first hash pointer used is a hash of certain key information in the previous block—the previous block header. Starting with the genesis block, the hash of the current block header is stored in the next block. When the second block is ready, its block header, including the first hash, are hashed and stored in the third block header. The cycle continues, forming a tamper evident chain.

The second type of hash deals with the individual transactions stored inside the block. The accumulated transactions that each node listens for are organized in a data structure called a Merkle Tree. Inside a block header, there is another hash called the Merkle Root. This is included in the block header and hashed. The Merkle Root is a hash pointer that forms the base of the Merkle tree and is the culmination of a series of other hashes. These other hashes are not included within the block header but are still included in the total block. As a node accumulates transactions over the network, the transactions are hashed, producing the first generation of hash pointers. A second generation of hash pointers is then produced; these hashes are hashes of the first generation. It is possible for hashing algorithms to take any string as input, including other hashes. The number of second generation hashes is half the number of first generation ones since each second-generation hash covers the contents of two first generation hashes. The generations continue up with the number of hashes successively reducing until there is one hash—the Merkle Root.

These two interlocking hash systems form a giant data structure—the blockchain—wherein all data elements inside are protected against tampering. If an adversary tries to tamper with an individual transaction, that transaction's hash pointer will no longer be valid, and users will become aware of the activity by running periodic hash checks on the blockchain. Similarly, if he or she tries to alter the merkle root, the block header hash pointer will no longer be valid. If an adversary decides to change data, the hashes will not match up and the location of the change can easily be found.

Whereas hash algorithms serve to prove that the data in the blockchain system has not been tampered with, devices called digital signatures and keys verify the sender and receiver of transactions in the Bitcoin network. There are two types of keys—public and private—as well as numerous commands that one can execute with digital signatures, such as the verify and sign commands. By digitally signing a transaction, a sender of Bitcoins indicates consent for Bitcoins to be withdrawn from his or her account and deposited in another's. By verifying a signature, a receiver of Bitcoins confirms that the Bitcoins came from the sender and is a valid transaction.

When a user creates a Bitcoin account, he or she is assigned a public key and a corresponding private key. Both keys are lengthy alphanumeric strings and visually similar, but they differ in function. An example of a public key starts with 0x… and are fifty-one characters. The public key serves as the identity of the user and the address to which other can pay Bitcoins. Public keys are visible to anyone; on the other hand, private keys are closely guarded. The private key serves as a user' authentication device by which he or she authorizes payments to others. Private keys are fifty-two characters and are stored in cold storage—offline and away from prying eyes.

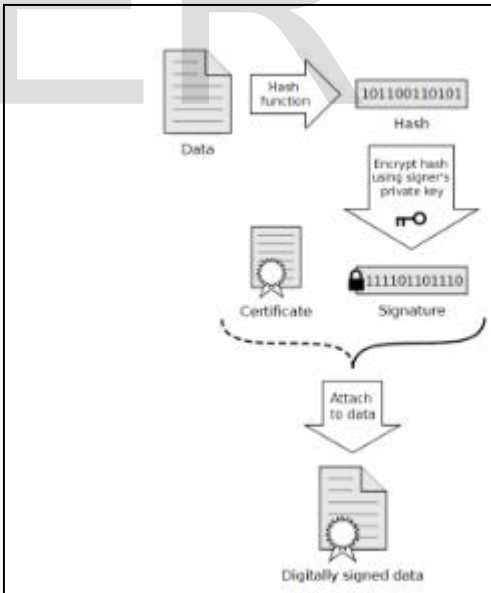

Fig. 3. The verification process in which data becomes digitally signed through a redundant hashing system.

There are two cryptographic functions that a user can perform with public and private keys. One is the sign function; users use this to indicate that they have agreed to pay to someone else. This function takes as input the user's private key and the message that they are signing; "Pay five BTC to Bob" could be a mes-

sage that user Alice signs. The output is a data value—the signature. For a recipient of a transaction to confirm that a signature is valid, he or she uses the verify function. The user's public key, signature, and the message received are fed into the function; the output is a simple true/false.

Some nodes in the system will choose to become miners if they have enough computing power. Miners are nodes that dedicate their computing power to solve difficult cryptographic puzzles. In doing so, they contribute to the system's security. Miners spend their time computing nonces—random numbers that are the input of a block's hash, along with the rest of the block header—to solve a hash puzzle. The process goes as follows: miners accumulate transactions broadcast over the network and organize them into a prospective block. As they are accumulating, miners also work on solving the block's hash puzzle by varying the nonce value and executing hashes millions or billions of times per second. The puzzle is structured so that there is no better strategy than trying random nonce values. Usually, the hash output fails to meet the solution criteria and the miner must repeat. In the rare event that a miner finds a solution, the miner adds the block to its blockchain. It then broadcasts the solved block to the rest of the network to be verified and added to other nodes' blockchains.

The time intervals between which blocks are added to network are carefully controlled to be approximately ten minutes. Thus, one can expect about six blocks to be added to the blockchain per hour. The mechanism by which this is enforced is the mining puzzle difficulty. The difficulty is related to the number of leading zeros that a hash contains; a hash puzzle gets progressively harder the number of leading zeros required increases. The difficulty is adjusted to respond to the total computing power available, also known as the total hashrate, at regular intervals. As the difficulty increases, miners will have to execute more hashes to arrive at a solution, thus increasing the time interval between solved blocks.

After a miner solves a block, the public key associated with the miner receives a Bitcoin reward, and a service bonus voluntarily donated by users of the Bitcoin system. The Bitcoin that the miner receives is a newly minted coin; mining is the only way in which new coins are created. The creators of Bitcoin posited that the block reward halves from its previous amount every 210,000 blocks created, or roughly every four years. Currently, 12.5 BTC are rewarded per block. It is expected that as block reward decreases, service fees by users will increase to maintain the same quality of service.

Bitcoin and many other cryptocurrencies operate on a PoW (Proof of Work) system. PoW miners are compensated for their effort in proportion to the amount of computing power that they dedicate to mining. The aforementioned mining process is how the PoW system works; miners with higher hashrates have a higher chance of receiving BTC.

The blockchain system ensures that all newly created blocks are synced between all nodes, or peers, via a consensus procedure. Miners listen for any newly created blocks and evaluate whether they should be added to the blockchain. A miner checks if all the transactions within a block are valid and if the hash pointers are correct, among other criteria. This consensus procedure is described below by Bitcoin blockchain dynamics and is run every time a node hears of a block

3 PROCEDURE

1. Reject the new block if a duplicate of the block is present
2. Compute the double SHA-256 hash of the new block according to (1) and check that the hash has the required number
   of leading zeros.
3. Check the timestamp of the new block.
4. Compute and verify the merkle hash of the new block.
5. Check if the predecessor block (that is, the block matching the previous hash) is in the main branch or a side branch.
    1. If it is in neither then query the peer that sent the new block to ask it to send the predecessor block and abandon the
       blockchain update.
6. Add the new block to the blockchain if the predecessor block is in the main branch or a side branch. There are three cases.
    1. The new block extends the main branch: add the new block to the main branch. If the new block is mined locally, relay the block to the node's peers.
    2. The new block extends a side branch but does not add enough difficulty to cause it to become the new main branch add the new block to the side branch.
    3. The new block extends a side branch which becomes the new main branch: add the new block to the side branch
7. Run all these steps (including this one) recursively, for each block for which the new block is its previous block

4 CONCLUSION

This empirical review concludes that the blockchain is a sustainable long-term revolutionary new technology with myriad applications in banking, commerce, internal record keeping, and personal privacy. Moveover, blockchain systems are remarkably resilient and exhibit great Byzantine fault tolerance. The author predicts a myriad of blockchain technologies which will revolutionize a plethora of industries in the future.

REFERENCES

[1] Acdx, "Digital Signature diagram," 2008
[2] Brandvold, M., Molnár, P., Vagstad, K., Valstad, O.C.A. , 2015. Price discovery on bitcoin exchanges. J. Int. Financ. Markets Inst. Money 36, 18–35.
[3] Back, Adam Hashcash – A Denial of Service Counter-Measure (August 1, 2002) Available at http://www.hashcash.org/papers/hashcash.pdf
[4] Disrupter Series, The: Digital Currency and Blockchain Technology — A Hearing Before the Subcommittee on Commerce, Manufacturing, and Trade (March 16, 2016)
[5] Irrera, Anna, JPMorgan, Microsoft, BP, UBS, Credit Suisse, Intel, and more are forming a new blockchain alliance (February 22, 2017) Available at http://www.businessinsider.com/r-jpmorgan-microsoft-intel-and-others-form-new-blockchain-alliance-2017-2
[6] Nakamoto, Satoshi; Bitcoin: A Peer-to-Peer Electronic Cash System. Available at https://bitcoin.org/bitcoin.pdf
[7] Pazaitis, Alex; De Filippi, Primavera; and Kostakis, Vasilis; Blockchain and value systems in the sharing economy: The illustrative case of Backfeed (May 22, 2017)
[8] Wright, Aaron and De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015). Available at: https://ssrn.com/abstract=2580664