Analysis and Comparison of Cryptocurrency Transaction and Verification Methodologies

Grant Gittes

INFSCI2170: Cryptography

Introduction

Cryptocurrencies began in 2008 as a theoretical method for the development of a decentralized network of independent users to process and verify transactions. Since Bitcoin launched in 2009, these cryptocurrencies have exponentially increased in value and usability, causing many to reevaluate the importance of traditional currencies (dollar, euro, etc.) and stores of value (gold, silver, etc.). While there are many cryptographical, economic, and technological aspects to analyze about various cryptocurrencies, this paper will focus on the transactions and verification of selected, popular cryptocurrencies. While Bitcoin was revolutionary in creating a distributed ledger through a blockchain and verifying transactions through independent machines using proof of work, many other currencies have been designed to address perceived “flaws” in Bitcoin, either by changing hashing algorithms or by verifying though a different mechanism. First, Bitcoin’s transaction methodology will be explained and then the differences between other popular “coins” will be discussed.

A Simple Bitcoin Transaction

Bitcoin and most other cryptocurrencies use asymmetric encryption to authorize and perform transactions. Most cryptocurrencies use a type of elliptic-curve cryptography, as the private keys are relatively short at 256-bits. The specific curve for most cryptocurrencies is secp256k1, which has the equivalent of 128-bit strength, but has certain properties that make calculation faster.[1] The public key and private key uses are similar to that of network encryption, as in, anyone who owns currency can send that currency to any public key, but only those with the private key can “receive” the currency and subsequently “spend” it by sending it to another public key address. The recipient (and observers) can verify the “sender” used a valid private key for the public key address sent from by using the elliptic curve digital signature algorithm.[2] The transaction details are hashed and combined with the private key and other mathematical transformations, which becomes the digital signature. The receiver decrypts the digital signature with the public key of the sender, then compares the hash of the transaction data. If the values are identical, the receiver and everyone in the network knows the sender authorized the transaction with a valid private key for the public key address.[3] The hash algorithm used for Bitcoin is SHA-256, but other currencies use different hashing algorithms.

The receiver can verify the sender did authorize the payment, and the receiver can analyze the prior transactions in the blockchain through the Merkle root to determine that the sender did, in fact, own the sent amount of Bitcoin. However, the receiver has no way of knowing if the sender "double spent", meaning, send the same Bitcoin to 2 or more recipients. This is where transaction verification comes into play. While the "transaction" is instantaneous, the recipient will likely want confirmation that the Bitcoin was validly sent and not double-spent.

Transaction Verification – Bitcoin Mining and Proof of Work

Bitcoin mining is the process by which the totality of Bitcoin transactions is verified by the network via consensus and a methodology called proof of work. The term "proof of work" was coined in 1999 as a way to prove that a certain level of computational effort has been expended, in contrast to a typical cryptographic scenario where one party wants to prove knowledge to another.[4] The concept applies to cryptocurrency by requiring "miners" to expend much computational effort to verify valid Bitcoin transactions. Bitcoin uses the hashcash proof of work function using SHA-256.[5] The idea of hashcash is to modify a message, that when hashed, yields a certain kind of result. For example, in Bitcoin, "miners" must determine a what value, when added to a message results in a hash of the message starting with n number of zeros, or in other words, that the 256-bits are less than or equal to a certain value less than 2^256. The maximum target for Bitcoin (meaning easiest to calculate) is defined as 2^224, meaning that on average, it can be expected to take 2^32 hashes to calculate that target.[6] However, as current computers and mining technology specifically have evolved, the current target hovers around 2^180 (quoted as a difficulty of 2^44),[7] taking on average 2^76 hashes to calculate correctly, which has been enabled by specialized computers called ASICs or application-specific integrated circuits that are designed to hash values incredibly quickly and in parallel versus a normal computer.

Getting to the target hash value, however, is only one part of the mining process. The main purpose of mining is to verify the transactions, thus creating a block to add to the blockchain. Each block contains the timestamp, a record of recent transactions the miner has included, a reference to the prior block and the number used to solve the hashing puzzle (called a nonce).[8] The miner must verify the transactions by making sure no Bitcoin is double spent, so the onus is on the miner to go back in the blockchain to verify all the transactions are valid and if multiple transactions come in that would result in double spending, to only include the most recent per the timestamp in the transaction ledger. The miner is held to this standard because a consensus is required on the network to accept a block. Other computers on the network can quickly verify every transaction in the block and check that the hash puzzle is solved (since verifying the hash takes 1 hash, while finding the correct nonce takes on average 2^76 hashes).[9] This is where the “proof of work” concept comes in. A miner is greatly incentivized to ensure adherence to the protocol because if the block is not accepted by network consensus, all the “work” the miner has put into solving the puzzle is lost, and the miner will not be entitled to a reward and forfeits the transaction fees collected.

The blockchain also provides integrity through its chained difficulty and exponential work required to alter prior blocks. If an adversary, Oscar, wants to change a large transaction 5 or 10 blocks back that went from Alice to Bob and reroute it to himself, he would not only need to change that block and resolve its hashing puzzle, but would also need to resolve each subsequent block and its respective hashing problem since each block references the hash of the prior block (creating a chain), which will be affected if Oscar tries to alter the destination address of a singular transaction. Thus, as the network as a whole is solving the current block, Oscar must solve the block from the changed transaction and all subsequent blocks, and eventually overtake the network and aim to form a consensus based on his new block chain. Since the overall computing power of the network dwarfs Oscar's personal computing power, this is extremely unlikely, and practically impossible if Oscar is behind by more than a few blocks.[10]

For this reason, many vendors and currency markets will require a certain number of blocks to be added to the blockchain after a transaction has been recorded in a block to ensure that the transaction is validated. The Bitcoin algorithm automatically adjusts difficulty of its puzzle to target 1 block added every 10 minutes, as this is a tradeoff between network latency of the distribution of the latest block, and the desire for transactions to be quickly approved.[11]

Practical Issues with Bitcoin's Proof of Work Blockchain

While Bitcoin pioneered proof of work cryptocurrency, there has been much discussion around the specifics of its blockchain, and how it could be improved. As Bitcoin evolved from its launch in 2010, the world of finance and technology has evolved and limitations have been discovered that prevent Bitcoin from being widely used as a currency.

One area for concern is the volume of transactions. Previously, Bitcoin blocks were capped at 1MB in size (which later was updated to up to 4MB), and based on the average data in a transaction, and the time between blocks, the Bitcoin network could only handle 7 transactions per second, while a payment processor like Visa can handle 45,000+ transactions per second. This clearly results in a problem if Bitcoin is hoped to be adopted as a "currency" to be used for day-to-day transactions, and not simply a store of value that is seldom exchanged.[12]

Another area for concern with regards to transactions is confirmation time. Because blocks are only added every ~10 minutes, it may take a while for a transaction to be "confirmed" by the blockchain. Due to the double spending problem, a vendor would likely wait until a few blocks were added to the blockchain to be assured from consensus that the transaction was valid and approved from the blockchain. Coinbase, the largest cryptocurrency trading platform, requires 3 confirmations (~30 minutes) to consider a transaction final.[13] While this may be fine for large transactions or currency trades, it is not suitable for day-to-day spending at in-person vendors. However, it may be acceptable for online transactions as those are typically processed and shipped over the course of hours or days, in contrast to a retail establishment where one would expect to collect all purchased goods/services and simply leave the store.

An additional problem regarding confirmations is how transactions get included in the blockchain. Miners determine which transactions to include based on transaction fees offered (which the miner directly receives if the block is successful), and the number of transactions included is limited by the block size. Because a $10 transaction and a $1 million transaction take the same amount of computational effort (with differences depending on the number of addresses per transaction), miners are incentivized to process transactions that include higher absolute fees (meaning a smaller percentage on large transactions, and a higher percentage on small transactions).[14] If someone wants to make a small purchase, that purchase will probably have higher fees as a percentage of transaction value, if it is desired to be included quickly on the blockchain.

In addition to the issues with transactions, there are also concerns about the mining proof of work methodology. Due to Bitcoin's meteoric rise in value, there has been much investment in mining hardware, resulting in the development of specialized computers called ASICs that perform the hashing algorithm extremely quickly. Due to competition over solving a block, there has been an "arms race" in terms of faster and more specialized computers being used.[15] This results in the problem where the difficulty of the block solving increases exponentially, and makes it infeasible for individual users to mine using standard hardware. The result has been that most blocks are mined by one of a handful of mining pools, which is antithetical to the vision for Bitcoin to be a truly decentralized network.

Overall, the multiple transaction and mining issues have led to many “altcoins” that modify parts of Bitcoin’s functionality to improve one or more of these transaction or mining problems. Some of these alternative coins and their properties that differ from Bitcoin will be discussed.

Litecoin and the Scrypt Hashing Algorithm

Litecoin was launched in 2011 as an alternative to Bitcoin. Its main selling point was faster block generation (targeting 2.5 minutes vs. 10 minutes for Bitcoin), and a more decentralized hashing algorithm: Scrypt.[16] It maintains the same elliptic-curve cryptography, in addition to digital signing, and the general concept of proof of work, but differs in hashing algorithm. The Scrypt algorithm was created to combat the Bitcoin ASICs, and reduce the centralization of computing power. While it uses a similar computational algorithm to SHA-256 used in Bitcoin, Scrypt requires much more stored data in memory (RAM) which theoretically makes it harder for ASICs, which have lots of parallel processing, but little memory, to dominate the system.[17] While originally designed for CPUs, eventually GPUs were able to mine, and even some ASICs were created specifically for the Scrypt algorithm.

Due to a lack of popularity relating to transaction time and the fact that the Scrypt algorithm ultimately proved not to protect against centralized computing, Litecoin’s market capitalization is well below Bitcoin’s ~$1+trillion, at ~$18 billion.[18]

Ethereum and Ethash

Ethereum, and its associated cryptocurrency, Ether, is the second-best known cryptocurrency. Ethereum is a network that was designed to decentralize certain financial transactions and contracts with a blockchain network of "smart contracts." One recent example is the concept of Non-fungible Tokens (NFTs), in which artists, athletes, and even everyday people, can sell digital art, digital screenshots, or even tweets in a one-time transaction that cannot be replicated. Thus, artists can create digital art and sell the rights to a single owner, who will be verified on the blockchain.[19] While this is just one example of the potential use of the Ethereum network, this paper will focus on the currency, Ether, which is rewarded for "mining" in a similar manner to Bitcoin.

The Ethereum network, similar to Bitcoin and Litecoin, uses elliptic-curve cryptography (including digital signatures) and a hashing algorithm for proof of work, but it uses an algorithm called Ethash, which was specifically designed for the Ethereum network. Ethash, like Scrypt, was designed to be resistant to ASIC mining. The Ethash algorithm is descendent of Dagger, an algorithm that utilizes directed acyclic graphs, and Hashimoto, which adds transaction and other information to those acyclic graphs to generate a hash. The Ethash algorithm built on those two algorithms, and added Keccak-256 and Keccak-512 functions similar to SHA-3. Each hash requires up to 4 GB of data for the graph, thus making it complex for ASIC devices, while very efficient for GPU devices.[20]

In terms of blocks, Ethereum adds blocks much more quickly than Bitcoin or Litecoin, but includes fewer transactions in each block. The average block time hovers around 13 seconds, but those blocks include both smart contracts and transactions.[21] Similar to Bitcoin, this can result in slow execution time if transaction fees are insufficient. Ether is the 2nd largest cryptocurrency by market cap, worth ~$290 billion.[22] While the Ethereum network has faster execution time than Bitcoin, it still lags behind traditional payment processors (like Visa).

Ethereum 2.0 and Proof of Stake

One recent and exciting development for cryptocurrencies is Eth2 – sometimes referred to as Ethereum 2.0 which will replace Ether on the Ethereum network. Eth2 will switch from a "proof of work" model employed by the currencies discussed in this paper to a "proof of stake" model, with the goal of enhancing transaction speed, reducing transaction costs, improving security, and becoming more environmentally friendly.[23] Proof of stake allows users to "stake" some Ether tokens as a type of collateral for accurately verifying transactions and preventing double spending. In a proof of work structure, miners lose out on transaction rewards and all the energy spent computing if they verify an incorrect transaction or try to deliberately change the blockchain.

In proof of stake however, "stakers" lose some or all of their "staked" Ether tokens if they incorrectly verify blocks or try to verify malicious blocks.[24] This process allows passive holders of Ether tokens to earn a type of "interest" without investing $1,000-10,000+ on mining computers.

This process increases transaction speeds and reduces costs because more transactions can be verified per second, since the machines only need to "attest" to the block's correctness, and are not required to expend extreme amounts of energy and computing power to solve the hash puzzle at a given difficulty level. This methodology addresses one of the key criticisms of cryptocurrency: the fact that they use too much energy through their difficulty-adjusting algorithms, thus contribute to climate change. While Bitcoin proponents have pushed back on that assertion, it is interesting that Ether is touting this benefit, and is trying to brand itself as the "green" cryptocurrency.

Overall, Eth2 will launch in stages, as the first step has already launched, the Beacon Chain, and next steps are estimated in 2021, finishing in 2022. Ether has outperformed Bitcoin +230% vs. +90% year to date, causing it to have a market cap of ~$290 billion vs ~$1 trillion for Bitcoin, so it be fascinating to see if the transition to Eth2 results in even more demand.[25]

Conclusion

Overall, the world of cryptocurrency is extremely complex and evolving quickly as valuations climb. Bitcoin, especially, has exponentially grown in value, threatening existing stores of value like gold and silver. All popular cryptocurrencies facilitate transactions with public-key cryptography, using elliptic curves to send currency, and verifying the transaction on the blockchain through digital signatures. The blockchain, started by Bitcoin, was designed to create a fully-decentralized network in which transactions could be verified and processed without a traditional intermediary like a bank. Its proof of work implementation provided confidence about the integrity of the blockchain, allowing for elimination of fraud within the system (however, there have been many instances of fraud surrounding the exchanges on which most currency is traded).

However, it still seems like there are barriers to the scaling of the transaction and verification of most popular cryptocurrencies that make use as a day-to-day medium of exchange unlikely in the near term. Some companies and investors view Bitcoin as a hedge against inflation, as there will only be 21 million Bitcoins ever in the world. Due to this fact and its immense current popularity, Bitcoin seems likely to at least maintain its worth as a revolutionary store of value, but it probably will mainly be bought and held, or exchanged for large transactions (for example, Tesla accepts Bitcoin for its vehicles). Ether, especially Eth2, seems more likely to be used more frequently as a currency, given its rapid transaction speed, the improvements from moving to proof of stake, and the more integrated smart contract network. Overall, cryptocurrencies have revolutionized how currency and stores of value are viewed, but likely will not be replacing any government-issued currencies anytime soon as a medium of exchange.

Bibliography

[1] Brown, D. R. L. (2010, January 27). *SEC 2: Recommended Elliptic Curve Domain Parameters. Standards for Efficient Cryptography.* https://www.secg.org/sec2-v2.pdf

[2] Bitcoin Developer. (n.d.). *Transactions.* https://developer.Bitcoin.org/devguide/transactions.html

[3] Marshall, B. (2018, January 31). *How does a bitcoin transaction actually work?* Medium. https://medium.com/@blairlmarshall/how-does-a-bitcoin-transaction-actually-work-1c44818c3996

[4] Jakobsson M., Juels A. (1999) *Proofs of Work and Bread Pudding Protocols(Extended Abstract).* In: Preneel B. (eds) Secure Information Networks. IFIP — The International Federation for Information Processing, vol 23. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35568-9_18

[5] Bitcoin Official Wiki – Community Maintained. (n.d.) *Hashcash.* https://en.Bitcoin.it/wiki/Hashcash

[6] Bitcoin Official Wiki – Community Maintained. (n.d.) *Difficulty.* https://en.bitcoin.it/wiki/Difficulty

[7] Blockchain.com (n.d.) *Bitcoin Explorer.* https://www.blockchain.com/btc/block/00000000000000000006a5d5fe2d341d4e555a9bf7533d6c2b8abd45896391a4

[8] Bitcoin Official Wiki – Community Maintained. (n.d.) *Block hashing algorithm.* https://en.bitcoin.it/wiki/Block_hashing_algorithm

[9] Reiff, N. (2020, January 24) *How does a block chain prevent double-spending of Bitcoins?* Investopedia. https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-Bitcoins.asp

[10] Bitpay.com (n.d.) *How do Bitcoin block confirmations work?* https://support.bitpay.com/hc/en-us/articles/115004832203-How-do-Bitcoin-block-confirmations-work-

[11] Kenton, W. (2020, October 1). Bitcoin Mining. https://www.investopedia.com/terms/b/Bitcoin-mining.asp

[12] Investerest by Vontobel. (2019, August 8). *Bitcoin Explained - Chapter 7: Bitcoins Scalability.* https://investerest.vontobel.com/en-dk/articles/13323/Bitcoin-explained---chapter-7-Bitcoins-scalability/

[13] Coinbase (n.d.) *Why is my transaction "pending"?* https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/why-is-my-transaction-pending

[14] Blockchain.com (2021, April 11). *Explaining Bitcoin transaction fees. https://support.blockchain.com/hc/en-us/articles/360000939883-Explaining-Bitcoin-transaction-fees*

[15] Reiff, N. (2021, March 10) *Why Centralized Cryptocurrency Mining Is a Growing Problem?* Investopedia. https://www.investopedia.com/investing/why-centralized-crypto-mining-growing-problem/

[16] Kenton, W. (2021, March 10). *Litecoin (LTC).* Investopedia. https://www.investopedia.com/terms/l/litecoin.asp

[17] Mycryptopedia. (2018, December 18). *Litecoin Scrypt Algorithm Explained* https://www.mycryptopedia.com/litecoin-scrypt-algorithm-explained/

[18] CoinMarketCap (Accessed 2021, April 22). *Today's Cryptocurrency Prices by Market Cap* https://coinmarketcap.com/

[19] Clark, M. (2021, March 11). *NFTs, explained*. The Verge. https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq

[20] Bit2me Academy (n.d.) *What is the Ethash mining algorithm?* https://academy.bit2me.com/en/what-is-the-algorithm-of-ethash-mining/

[21] Etherscan. (Accessed 2021, April 22) *Ethereum Average Block Time Chart.* https://etherscan.io/chart/blocktime

[22] CoinMarketCap (Accessed 2021, April 22). *Today's Cryptocurrency Prices by Market Cap* https://coinmarketcap.com/

[23] Ethereum.org (n.d.) *The Eth2 Vision.* https://ethereum.org/en/eth2/vision/

[24] Ethereum.org (n.d.) *PROOF-OF-STAKE (POS).* https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[25] CoinMarketCap (Accessed 2021, April 22). *Today's Cryptocurrency Prices by Market Cap* https://coinmarketcap.com/