Cryptocurrencies, Blockchain & Consensus

Jason Ballantyne & Jonathan Farrell

COMP30660: Computer Architecture & Organisation

UCD School of Computer Science

10/05/2021

Underlying technology and Architecture

Both Bitcoin (BTC) and Ethereum (ETH) are built using blockchain technology. Although the concept of blockchain existed as far back as 1991, Bitcoin's creation in 2009 created a new use case for the technology and brought it to the fore. Bitcoin aimed to use blockchain technology to provide an alternative to national currencies (Simply Explained, 2017).

A blockchain is a ledger database, with no central authority, that is distributed amongst a network of peers. The ledger is a record of all historical transactions and ownership. All peers hold a replica of the ledger, and each peer plays a role in the authentication of the chain, and blocks on the chain (Selbold, Samman, 2016). In their article *The Truth About Blockchain*, Marco Iansiti and Karim R. Lakhani, write that blockchains can record every transaction with a unique, permanent, and traceable ID (2017). The process by which they do this is called "hashing." The combination of this hashing process, and the Peer-to-Peer distribution structure are a large part of what makes blockchains so effective.

The decentralised distribution is a key component of both Bitcoin and Ethereum. This means that they do not have a single point of control such as a bank or government controlling them and allows it to be both secure and anonymous. This anonymity is a by-product of the decentralized nature of Bitcoin where each transaction can be seen as a unique id sending bitcoin credits to another unique id. The use of a peer-to-peer network means that computers that participate in the network are all equal and share the burden of providing network services, of verifying the authenticity of others' actions, and removing any hierarchy within the network.

Ethereum is also a decentralized peer-to-peer (P2P) network of Ethereum clients, representing network nodes. These peer-to-peer apps on Ethereum are known as decentralized apps (dApps) and can provide trust-less products and services. As the native currency on the Ethereum platform, ETH is the gas that is needed to run dApps on the platform.

Both Ethereum and Bitcoin currently use a proof-of-work consensus mechanism. This means that to add new blocks to the chain, requires solving a difficult puzzle that requires a lot of computing power. Solving the puzzle "proves" that you have spent the computational resources. This brute force and energy intensive computation process, known as "mining", creates a "hash". The "miner" transmits this hash to the Peer-to-Peer network, which then uses it to add a new block to the chain (Computerphile, 2018). Successfully adding a block is rewarded in ETH (Richards, 2021) or BTC.

A hash key is a unique key that is computed based on the contents of the data that an algorithm is provided. For a hashing algorithm to be effective, it must have several very important properties. For example, the hashes should be reasonably cryptographically complex, they must always provide the same output for the same input, and they must produce a significantly different hash for any small changes to the input (Blockgeeks, 2018). Each block on the chain contains data, and a hash pointer to the previous block in the chain. This hash pointer operates as an identifier for the block and, as any small change in the block's data will create a change in the hash, each block holds another accountable. Therefore, tampering with a block will cause other blocks to reject it.

Technical Comparison

To choose an investment strategy between Bitcoin and Ethereum it is important to understand the characteristics that differentiate the two cryptocurrencies. We will examine these trust-less cash systems' (Floyd, 2021) architecture, then delve into their strengths and weaknesses under the headings of security, price, scalability, and performance.

Security: A major advantage of Bitcoin is its personal data protection. There is a low risk of a user becoming victim of a cyber security attack possibly losing financial or personal data. This scenario is only possible whereby hackers have obtained access to the user's private key which is a sophisticated form of cryptography that allows access to a user's cryptocurrency.

Bitcoin's anonymous nature can also be a disadvantage. These untraceable transactions make them well-suited for a host of illegal activities such as money laundering and tax evasion. Ether's security can also be a weakness as it has suffered at least four successful 51% attacks, deteriorating trust in the network and requiring weeks for a transaction to be successfully completed and validated (Voell, 2020).

Price: Another advantage of Bitcoin is the lower transaction fees. Bitcoin users are not subject to the litany of traditional banking fees. The cost of transactions in Bitcoins is lower, reflecting the amount of data sent (Blystone, 2015). Since Bitcoin users have no intermediary, the cost of transacting is kept very low.

On the other hand, Ethereum's growing popularity has led to higher transaction costs. Ethereum transaction fees hit a record $23 per transaction in February 2021. This is because unlike Bitcoin, where the network itself rewards transaction verifiers, Ethereum requires those participating in the transaction to cover the fee. (Rodeck, 2021)

Scalability: A weakness associated with Bitcoin is that the maximum number of Bitcoins that can ever be produced is 21 million, introducing scarcity into the market. Each bitcoin will be worth more as the total number of Bitcoins edge towards capacity. Unlike Bitcoin, there is no limit to the amount of Ether that can be released, the production of Ether is continuous. This removes the perceived scarcity that may be a factor in Bitcoin's higher valuation.

Performance: Ethereum block time is faster than Bitcoin block time, transactions typically settle in seconds as opposed to minutes. Ethereum can also currently handle about 15 transactions per second (TPS) as opposed to 4.6 TPS on Bitcoin (Ethereum transactions per second chart, 2021).

The final weakness of Bitcoin is its performance problems. Bitcoin can only achieve a low throughput of 4.6 TPS, and it takes approximately 10 minutes for a transaction to get confirmed. For comparison, Visa handles an average of 1736 TPS (Muli, 2021)

Trade-off Summary: To conclude our technical comparison, it is worth highlighting that Ethereum and Bitcoin were not designed with the same purpose in mind, nor to be competitors of each other. Bitcoin was designed with the intention of replacing national currencies and it aspires to be a medium of value exchange. It holds greater reputation for stability, and a stronger position in the market, holding just under 10 times the market cap as Ethereum (Divine, 2021).

Ethereum was designed, not with the intention of solely being an exchange currency, but to provide "smart" contracts – a way for contractual transactions to be written and executed by a programming language, without the need for a centralised authority to verify them. So, while Bitcoin holds a stronger position and reputation as a financial asset, Ethereum provides a broader variety of applications and solutions to remove exchange friction.

Cardano – An Alternative

Cardano is a relatively new cryptocurrency, founded in 2017 and calling itself part of the "third generation" of cryptocurrencies, with Bitcoin being part of the first and Ethereum part of the second. The Cardano team wants to improve three longstanding problems with cryptocurrencies to date: scalability, sustainability, interoperability. These goals help address some of the issues we have observed in our discussions around Bitcoin and Ethereum.

Security: Much of the security concerns we mentioned with BTC and ETH, regarding anonymity, are also shared by contemporary banking organisations. Cardano seeks to solve the traditional banks issue, by providing users with ability to provide meta-data, if they wish. This makes up part of Cardano's goal of becoming an interoperable coin – one where transactions can be interfaced across different mediums.

Price: Cardano's fees are very low, with a typical 200-byte transaction estimated at about <$0.01 in 2019. Although Cardano's prices may rise over time, they are spared industry volatility by use of a simple transaction calculation: a + b * size, "where a and b represent special constants and the size refers to the amount of bytes in a transaction" (thecoinoffering.com, 2019). Cardano charges fees per transaction, which contribute to its treasury scheme. This treasury is used to fund development suggestions proposed by members of the network – which are then voted on and developed. The treasury model, and users' transaction fees, give solace to users that the platform will not suffer a premature end.

Scalability: First, to improve scalability issues, Cardano sought to use a proof of stake scheme, instead of Bitcoin's proof of work, like Ethereum. This means Cardano, like Ethereum, can perform much more transactions per second without the wastefulness of the proof of work methodology. Another scalability issue for cryptocurrencies is growing network bandwidth as a blockchain grows. Cardano splits up the network, using a protocol called RINA, into subnetworks. This is like the TCP/IP protocols in networking and helps Cardano create less excess traffic.

Performance: Cardano has significantly higher transactions per second over Bitcoin and Ethereum, with coinmarketcap.com reporting "When the Cardano chain was first tested in 2017, it was able to process as much as 257 transactions per second (TPS)."

Conclusion

We have examined the underlying technology and architecture of Bitcoin and Ethereum, technical comparisons were made between the two identifying the strengths and weaknesses of both under the headings of security, price, scarcity, and performance. While Ethereum and Bitcoin are considered the two most important cryptocurrencies for investment, there are obvious trade-offs that exist. We have seen from analysing Cardano using the same criteria, that there are far more projects and each one of them has its own unique specifications. This illustrates the importance of doing thorough and in-depth research before investing in cryptocurrencies in 2021.

Bibliography

Antonopoulos, A., 2017. *Mastering Bitcoin, 2nd Edition*. 2nd ed. O'Reilly Media, Inc.

Blockchair.com. 2021. *Ethereum transactions per second chart*. [online] Available at: <https://blockchair.com/ethereum/charts/transactions-per-second> [Accessed 10 May 2021].

Blockgeeks, 2018. *What is Hashing on the Blockchain?*. [online] Youtube.com. Available at: <https://www.youtube.com/watch?v=IGSB9zoSx70>.

Divine, J., 2021. Retrieved 10 May 2021, Available at: <https://money.usnews.com/investing/cryptocurrency/articles/bitcoin-vs-ethereum-which-is-a-better-buy>

Dumitrescu, G., 2017. Bitcoin – A Brief Analysis of the Advantages and Disadvantages. Global Economic Observer, 5, 63-71.

Floyd, D., 2021. *How Bitcoin Works*. [online] Investopedia. Available at: <https://www.investopedia.com/news/how-bitcoin-works/>.

Frankenfield, J., 2021. *Smart Contracts: What You Need to Know*. [online] Investopedia. Available at: <https://www.investopedia.com/terms/s/smart-contracts.asp>.

Iansiti, M. Lakhani, K.R. 2017., *The Truth About Blockchain*. Harvard Business Review. Available at: <https://hbr.org/2017/01/the-truth-about-blockchain>

Muli, K., 2021. *The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed*. [online] Medium. Available at: <https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44>.

Müller, P., Bergsträsser, S., Rizk, A., & Steinmetz, R. (2018). The Bitcoin Universe: An Architectural Overview of the Bitcoin Blockchain. DFN-Forum Kommunikationstechnologien.

New York Times, The., 2021. Cryptocurrency’s Newest Frontier. Available at: <https://www.nytimes.com/2021/04/13/podcasts/the-daily/nft-bitcoin-cryptocurrency.html>

Reiff, N., 2020. Bitcoin vs. Ethereum: What’s the Difference? <https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp>

Richards, S., 2021. *Intro to Ethereum | ethereum.org*. [online] ethereum.org. Available at: <https://ethereum.org/en/developers/docs/intro-to-ethereum/>.

Rodeck, D., 2021. *What Is Ethereum And How Does It Work?*. [online] Forbes.com. Available at: <https://www.forbes.com/advisor/investing/what-is-ethereum-ether/>.

Roth, N., 2015. An Architectural Assessment of Bitcoin. *Procedia Computer Science*, 44, pp.527-536.

Samman, G. Selbold, S. 2017., *Consensus: Immutable agreement for the Internet of value*. Available at: <https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf>

Simply Explained, 2017. *How does a blockchain work*. [online] Youtube.com. Available at: <https://www.youtube.com/watch?v=SSo_EIwHSd4>.

The Coin Offering. 2019. *Is Cardano (ADA) a better project than Ethereum (ETH)?*. [online] Available at: <https://thecoinoffering.com/learn/cardano-ada-vs-ethereum-eth>.

Voell, Z., 2020. Ethereum Classic Hit by Third 51% Attack in a Month. [online] CoinDesk. Available at: <https://www.coindesk.com/ethereum-classic-blockchain-subject-to-yet-another-51-attack>.

Werner, V., 2021. A Deep Dive Into Cardano | CoinMarketCap. Available at: <https://coinmarketcap.com/alexandria/article/a-deep-dive-into-cardano>