Cryptocurrency: Minting and Distributing the Internet's Cash

Dane Rieber

Oct 2021

Cryptocurrency is an anonymous peer-to-peer system of exchange that forfeits the use of a governing body or central financial institution to carry out transactions. The most popular cryptocurrency Bitcoin -- the first of its kind -- has over $1 trillion worth of digital, unregulated, seemingly imaginary assets in circulation [8]. In the decentralized landscape of cryptocurrency, notions of ownership and value are less tangible than that of material possessions and fiat currency exchange, and the architecture of the global network that creates and transfers assets needs to be rigorously crafted to handle the myriad of new problems that arise when central authorities are eliminated. Despite decentralization, cryptocurrency designers and users argue that the system offers more integrity than traditional exchanges, since the mechanisms that verify transactions are impartial and well-distributed throughout its network of participants [1].

To achieve a reliable decentralized currency, blockchain technology has served as a fundamental pillar for peer-to-peer decentralized networking.

Blockchain Technology

Blockchains are ledgers composed of cryptographically linked blocks, or records of transactions between two or more parties. Blockchains "provide a mechanism through which mutually distrustful remote parties (nodes) can reach consensus on the state of a

ledger of information" [3]. To reach consensus, the underlying technology enforces high costs to append the ledger. These costs take any form, but the most feasible and popular forms are either computational (proof-of-work) or economic (proof-of-stake) [3].

Proof-of-Work (PoW)

PoW is a method to "achieve consensus within a permissionless blockchain", a permissionless blockchain being a public ledger with no single entity or authority granting permission to make modifications [2]. Validators utilize computational power solving cryptographic puzzles associated with blocks, and then submit blocks along with proof that computational work has been done to validate the block. The proof, a solution to a cryptographic puzzle, is costly to produce but trivial to verify, and also, through careful design choices, satisfies the requirements necessary for transaction integrity to be upheld [4].

The process of producing this proof is called "mining", and the incentive for "miners" -- anyone with computer hardware -- to contribute their resources comes from payouts for validating blocks. For common cryptocurrencies like Bitcoin, block rewards are the only avenue in which new currency enters circulation. The overall goal of PoW systems is to prevent rogue parties from creating fraudulent blocks (since influencing the consensus process requires controlling the majority of the network's computing power) and also to incentivize contribution to the PoW process through small handouts of the cryptocurrency to those who invest their resources to operate the network [2, 3].

The pitfall of PoW is its excessive use of scarce resources -- namely energy and computer hardware. Critics cite the wastefulness of using PoW only to validate transactions as unnecessary. A 2015 study on Bitcoin estimated that the power consumption from mining accounted for 173 megawatts of electricity usage, or "approximately 20 percent of an average nuclear power plant" [5]. A 2017 estimate claimed that all cryptocurrency mining could account for up to 3-6 gigawatts of electricity usage, similar to that of a "small to medium size country such as Bangladesh and Denmark" [6]. The exchange of digital currency outpacing an entire country's electricity usage is unacceptable for many, and this problem created the need for a better solution.

Proof-of-Stake (PoS)

To combat PoW's intensive resource usage (and therefore negative environmental impact), PoS was proposed and first implemented in a cryptocurrency called Peercoin. This method randomly selects stakeholders of the cryptocurrency to append blocks to the blockchain, giving rewards to those selected. A miner's chances of being chosen to write to the blockchain is proportional to the amount of cryptocurrency they own,

removing computational work altogether but still, in theory, distributing resources across the network [2].

Similar to PoW, one would need to own the majority of the resources (in the case of PoS, this means owning more than 50% of the currency) in order to affect the system's integrity. However, this turns out to be a critical issue during the creation of new PoS cryptocurrencies, during which the creator can give themselves the majority of the available stock. PoW did not face this issue because it is insurmountably more difficult to obtain a majority of assets valued independently of the cryptocurrency (computer hardware) than it is to obtain the majority of the initially unvalued cryptocurrency itself. This inherent weakness of PoS has in fact resulted in most implementations of PoS cryptocurrency to be fraudulent [4].

Hybrid PoW/PoS

To combat the unreliability during the initial growth of systems using PoS, some cryptocurrencies use PoW to distribute the currency at first and then phase out the PoW mechanism over time, replacing it with a PoS mechanism. This approach mitigates the wastefulness of PoW while addressing the initial distribution problem of PoS [4].

Bitcoin

Bitcoin is the first cryptocurrency and was released in 2009 by an anonymous group of developers. Transactions are unrestricted, processed as fast as the network can handle them, and unable to be modified once submitted, creating a near-immediate, irreversible, universally accessible method of exchanging currency.

There is a finite number of bitcoin that can ever enter circulation -- designed this way because "scarcity is a prerequisite for ascribing value to any form of money" [5]. Typically, banks and governments control the amount of currency in circulation and the amount of new currency that is produced. This is integral to preventing counterfeiting and economic crises. Bitcoin's approach, absent a governing body, is to slow the rate at which new bitcoin enters the market over time. The maximum limit of 21 billion bitcoin is not explicitly programmed into a system, but is rather a result of block rewards periodically being cut in half. Once it is impossible to continue mining bitcoin, transaction fees are the only way in which miners will receive rewards for validating the block chain. Transaction fees can be user-specified and miners will (in most cases) be incentivized to prioritize transactions that pay more fees to the miners [5].

In the early stages of bitcoin, large block rewards served to bootstrap the utility of the platform, generating large volumes of bitcoin ready for exchange and healthy sums for

miners who were willing to jump onboard early [5]. Nearly any hardware could be used at this time, but as block rewards decreased, the market for mining transitioned and created an "arms race" among ambitious miners who sought to perform computations by the most efficient means and on the largest scale [2]. One piece of hardware was discovered to be extremely well-suited for cryptocurrency mining: desktop GPUs, or graphics cards. The skyrocket in the popularity of Bitcoin caused a surge in GPU sales, resulting in a mass GPU shortage that raised prices for consumers considerably [7]. Consumers began to express much disdain for cryptocurrencies. GPUs were quite literally out of stock in nearly every store, and the thought of countless GPUs sitting in a warehouse doing nothing but chugging away on the blockchain, sucking enormous amounts of power, and potentially even facilitating illegal activities (since transactions are anonymous and irreversible) tainted cryptocurrency's reputation for some.

As Bitcoin mining stands today, block rewards have diminished to a point where "effective mining now requires specialized hardware…as well as access to low-cost electricity" [5]. Leaving the days when laptops could mine bitcoin profitably and entering a mining landscape with extreme barriers to entry has been argued to increase the centralization of Bitcoin, as less people can afford or obtain access to the necessary resources. Not only this, but groups of miners often prefer to pool their resources together, with the goal to distribute a steady stream of bitcoin to members of the pool in proportion to their processing power as opposed to independently mining and receiving block rewards intermittently (low-power users may wait months to receive a block reward). It is estimated that for PoW cryptocurrencies, "20 mining pools control 90% of the computing power" [3]. Although the largest pools often comprise tens of thousands of members, these pools are not decentralized and are operated by individual entities that organize the pool and take a fraction of the rewards. Many claim this to be counterintuitive to the original philosophies of Bitcoin, as mining pools are points of centralization [5].

Ethereum

Ethereum was launched as a decentralized network protocol built upon blockchain technology that, along with utilizing its built-in cryptocurrency called Ether, has uses beyond currency exchange, some examples being cloud computing and web hosting. The Ethereum protocol can be used to represent state changes (transactions) pertaining to "anything that can currently be represented by a computer" [1]. Today, Ether is the second-largest cryptocurrency in circulation, with a market cap of nearly half a trillion dollars [8].

It utilizes PoW mining similar to that of Bitcoin, but with key differences from Bitcoin's algorithm to address some of its caveats. Two goals are outlined in its design

specification: “it should be as accessible as possible to as many people as possible,” and “it should not be possible to make super-linear profits” (earnings should scale directly with resources, not exponentially) [1]. Both goals are achieved through the creation of a new PoW mechanism that is resistant to specialized hardware, removing the barriers to entry for consumers and also preventing unfair advantages in the mining landscape [1].

Ethereum’s accessibility and generalization for applications outside of only currency exchange made it quite popular. Ethereum’s continued development has transitioned to focus on implementing PoS, and the launch of Ethereum 2.0 (which uses PoS) is on the horizon, with the ability to stake Ether already enabled and transactions to be enabled at a later date [9].

Future

There’s no doubt that despite cryptocurrency’s success with technically proficient users, it experiences trouble reaching a large mainstream audience. This may be due to an apprehension for many to trust a system without governance, especially for governments themselves who wish to enforce stability and sustainability in their currencies. Exchange rates have proven to be highly volatile and unpredictable -- even worse so than the stock market, which is already criticized for its nonsensical patterns. Launching cryptocurrency into the mainstream may only be possible with time and growth. It may also require legitimate popular uses that justify average consumers entering the cryptocurrency landscape.

As things stand today, conventional online transactions are simple and incur no transaction fees unlike the often annoyingly high fees for cryptocurrency transactions. However, cryptocurrency transactions are essentially free from institutional overhead and don’t require any special setup for individuals or businesses to immediately start receiving payments for their goods and services. Once consumers obtain a better grasp of cryptocurrency literacy, we may see people holding small amounts of cash in crypto wallets much like digital gift cards to use on various accepting sites. Younger generations’ early exposure to the concepts of decentralized currency will likely make this transition easier. Nevertheless, cryptocurrencies should strive to simplify their systems and market to the public with an emphasis on accessibility.

Government regulation is likely one of the largest remaining inhibitors on cryptocurrency’s growth. There are inherent economic issues with cryptocurrencies that the community continues to struggle solving with only computers and mathematics at their disposal. Despite the lack of human-based verification, a large human component of cryptocurrency still remains -- the miners and the traders. As seen in the past with other economies (the U.S. stock market, the U.S. housing market, etc.), human activity

may be predictable only in its unmatched ability to completely dismantle something when left unchecked. History begs the question of whether a purely mathematical solution will ever be resilient to the tests of man. Devout pioneers of cryptocurrency technology press onward in search for the answer.

References

[1] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[2] Saleh, Fahad. "Blockchain without waste: Proof-of-stake." The Review of financial studies 34.3 (2021): 1156-1190.

[3] Sherman, Alan T., et al. "On the origins and variations of blockchain technologies." IEEE Security & Privacy 17.1 (2019): 72-77.

[4] Farell, Ryan. "An analysis of the cryptocurrency industry." (2015).

[5] Böhme, Rainer, et al. "Bitcoin: Economics, technology, and governance." Journal of economic Perspectives 29.2 (2015): 213-38.

[6] FAUZI, Muhammad Ashraf, Norazha PAIMAN, and Zarina OTHMAN. "Bitcoin and cryptocurrency: Challenges, opportunities and future works." The Journal of Asian Finance, Economics, and Business 7.8 (2020): 695-704.

[7] Hsu, Aidan, and Roger Smith. "Price Correlation Between nVidia GPUs and Bitcoin."

[8] “Cryptocurrency Prices, Charts and Market Capitalizations.” CoinMarketCap, https://coinmarketcap.com/.

[9] “Ethereum Staking.” Ethereum.org, https://ethereum.org/en/eth2/staking/.