Journal of Business Theory and Practice
ISSN 2372-9759 (Print) ISSN 2329-2644 (Online)
Vol. 11, No. 2, 2023
www.scholink.org/ojs/index.php/jbtp

Original Paper

What Is Cryptocurrency?

Scott Andrew Yetmar[1]

[1] Associate Professor of Accounting, Cleveland State University, Cleveland, Ohio, United States

Received: May 12, 2023 Accepted: May 22, 2023 Online Published: May 31, 2023

doi:10.22158/jbtp.v11n2p35 URL: http://dx.doi.org/10.22158/jbtp.v11n2p35

Abstract

Cryptocurrency burst onto the scene in 2009 with Bitcoin. A person can buy almost anything with cryptocurrency. However, the thousands of cryptocurrencies are highly volatile. The majority of cryptocurrency owners are younger, highly educated males. Cryptocurrency relies on blockchain technology. To add new blocks to the blockchain, they must be mined. Non-fungible tokens represent ownership of an exclusive digital asset (e.g., a painting or a song). NFT transactions occur on the blockchain.

Keywords

cryptocurrency, blockchain, mining, non-fungible tokens, Bitcoin

1. Introduction

Cryptocurrency is continuing to evolve. Most people do not understand cryptocurrency. The use of cryptocurrency or Virtual Currency (VC) has been expanding. At least 300 million people have them. More than 21,000 different cryptocurrencies (most of which are volatile) are traded publicly, according to CoinMarketCap.com, a market research website. China is converting over to a digital yuan, and India is introducing a Central Bank Digital Currency (CBDC). This is a type of digital asset that represents a nation's fiat currency (e.g., cash) and is backed by its central bank. Not all nations issue CBDCs.

Many other countries are considering adopting or developing a digital currency (including the U.S.) that would replace fiat currency. Cryptocurrencies, or digital assets, went through a lot of turmoil in 2022. Since their high-water mark in late 2021, major assets like Bitcoin and Ethereum have seen a dramatic drop in value. These drops in value created a chain reaction in other areas of the cryptocurrency market, which ultimately led to the bankruptcy of several crypto platforms, and a crash that wiped out the value of a few large cryptocurrencies. Stablecoins are a type of cryptocurrency designed for price stability. Stablecoin prices are linked to fiat currencies, commodities, or other crypto assets. It can be used for payments, foreign exchange, and cross-border payments and transfers.

Bitcoin is the largest digital asset by market capitalization and the most well-known. It is also a digital asset enjoying the greatest adoption among institutional investors. Ethereum is the second-largest digital asset by market capitalization. The total value of all cryptocurrencies on May 25, 2023, was about $1.115 trillion, having fallen substantially from an all-time high above $2.9 trillion late in 2021.

Cryptocurrency is a type of digital asset that is intangible, digital currency that uses a very sophisticated type of encryption called cryptography to secure and verify transactions as well as to control the creation of new units of currency. It is a decentralized medium of exchange, independent of

a financial institution or any other central authority. While Bitcoin is the most well-known and the first cryptocurrency, it is not the only popular digital asset (e.g., Ethereum, Ripple, Bitcoin Cash and LiteCoin). Bitcoin became available to the public in 2009. It remained relatively unchallenged until Ethereum was introduced in 2016. All Cryptocurrencies created since then are called altcoins. Cryptocurrencies are more volatile than traditional fiat currencies. Fiat currencies are declared to be legal tender by a government and are not backed by physical commodities.

To receive or spend Cryptocurrency, users install a Cryptocurrency wallet on their personal devices or use a web wallet in the cloud. The wallet generates a key pair: the public address and a private address (a private key). The public address identifies the wallet and can be shared so the user can receive Cryptocurrency. The private key is held by the owner and used to spend or transfer the Cryptocurrency from the wallet. There are a few apps that one can download on a phone to get started investing (e.g., Coinbase, Blockfolio, and Bitstamp).

Cryptocurrency transactions are recorded on a computer file that acts as a public ledger that anyone can view using a website called a blockchain browser. The blockchain contains information on every transaction ever completed in the currency, including the value at each address at any point in history. Cryptocurrency transactions are traceable. The identities of the parties are not disclosed, but the details of the transaction are public. Every transaction is recorded publicly, so it is very difficult to copy Cryptocurrency, make fake ones, or spend ones you do not own. It is estimated that as much as $30 billion in Cryptocurrency have been lost or misplaced by miners and investors. The real loss risk revolves around not backing up your wallet. There is an important .dat file that is updated every time you receive or send Cryptocurrency. This .dat file should be copied and stored as a duplicate backup every day that a cryptocurrency transaction occurs.

Some interesting facts about cryptocurrency include:

1) The top 10 cryptocurrencies make up 88% of the total market value.
2) India has more cryptocurrency holders than any other country (more than 100 million).
3) 6% of Americans own cryptocurrency in 2022.
4) The total global revenue from mining cryptocurrency is $20+ billion annually.
5) The blockchain has grown to over 320 gigabytes in size.
6) 79% of Bitcoin investments come from males.
7) 58% of cryptocurrency holders are under 34 years of age.
8) 82% of cryptocurrency holders have a bachelor's degree or higher.

2. The Inner Workings of Cryptocurrency

Transactions are sent between peers using software called "cryptocurrency wallets". The person creating the transaction uses the wallet software to transfer balances from one account (i.e., a public address) to another. To transfer funds, knowledge of a password (i.e., a private key) associated with the account is needed. Transactions made between peers are encrypted and then sent to the cryptocurrency's network and queued up to be added to the public ledger. Transactions are then recorded on the public ledger via a process called "mining". All users of a given cryptocurrency have access to the ledger if they choose to access it, for example by downloading and running a copy of the software called a "full node" wallet (as opposed to holding their coins in a third-party wallet like Coinbase). The transaction amounts are public, but whoever sent the transaction is encrypted. Each transaction leads back to a unique set of keys. Whoever owns a set of keys, owns the amount of

cryptocurrency associated with those keys (just like whoever owns a bank account owns the money in it). Many transactions are added to a ledger at once. These "blocks" of transactions are added sequentially by miners. That is why the ledger and the technology behind it are called "block" "chain". It is a "chain" of "blocks" of transactions.

2.1 Blockchain

The blockchain is like a decentralized bank ledger (i.e., the ledger is a record of transactions and balances). When a cryptocurrency transaction is made, that transaction is sent out to all users hosting a copy of the blockchain. Specific types of users called miners then try to solve a cryptographic puzzle (using software) which lets them add a "block" of transactions to the ledger. Whoever solves the puzzle first gets a few "newly mined" coins as a reward (they also get transaction fees paid by those who created the transactions). Sometimes miners pool computing power and share the new coins. The algorithm relies on consensus. If most users trying to solve the puzzle all submit the same transaction data, then it confirms that the transactions are correct. Additionally, the security of the blockchain relies on cryptography. Each block is connected to the data in the last block via one-way cryptographic codes called hashes which are designed to make tampering with the blockchain very difficult. Offering new coins as rewards, the difficulty of cracking the cryptographic puzzles, and the amount of effort it would take to add incorrect data to the blockchain by faking consensus or tampering with the blockchain, helps to ensure against bad people.

Blockchain technology is a type of Distributed Ledger Technology (DLT) that enables peer-to-peer transactions in a secure and verifiable way without a centralized party. It is a single, incorruptible database that continuously records and timestamps transactions (blocks) chronologically. Every transaction must be verified though a process called consensus, requiring multiple-system participants to independently verify authenticity of the output of the algorithm creating the block. Once a new entry has been agreed to (i.e., verified) and made in the blockchain, it is locked and cannot be modified. It can only be updated by adding a new entry as an addendum.

Creating a new type of cryptocurrency coin requires either building a new blockchain or modifying an existing process to create a new variant (i.e., fork). Most of these altcoins are forks of the Bitcoin process. The only way more coins of an existing crypto coin can be created is through a process called mining in which the miner is awarded a transaction fee (a new coin) in exchange for contributing to the underlying blockchain algorithm be being the first to solve a cryptographic puzzle. Mining is very competitive and requires significant computing power. Some cryptocurrencies, like Bitcoin, are limited in supply and a maximum number of coins will ever be created.

Participants interact with one another using pseudonyms, and their real identities are encrypted. The ledger uses public-key encryption, which is virtually impossible to break, because a message can be unlocked only when a public and a private element (the latter held only by the recipient) are linked.

The term blockchain is derived from the way transactions are stored. For example, every time a bitcoin is created or changes hands, the ledger automatically creates a new transaction record composed of blocks of data, each encrypted by altering (or "hashing") part of the previous block. The cryptographic connection between each block and the next forms one link of the chain. This process increases the mathematical difficulty of committing a successful fraud, because blocks of transactions, as well as individual transactions, are continuously validated. The algorithms also incorporate an ID for each buyer and seller in a transaction, adding those IDs to the block.

One of the most significant features of the blockchain architecture is the decentralized technology, which helps ensure that a transaction is reliably reported. When a blockchain transaction (e.g., a bitcoin sale) takes place, several separate computers, connected across the network, process the algorithm, and confirm one another's calculation. The record of transactions continually expands and is shared in real time by thousands of people, i.e., distributed ledger). The ledger stores basic information about each transaction (such as sender, receiver, time, asset type, and quantity). The blockchain process ensures validity, by mathematically linking each new transaction to those that came before it.

2.2 Mining

People who are running software and hardware aimed at confirming transactions to the digital ledger are cryptocurrency miners. Solving cryptographic puzzles (via software) to add transactions to the ledger (the blockchain) in the hope of getting coins as a reward is cryptocurrency mining.

To add new blocks to the blockchain, they must be mined (i.e., the computers that mine are paid with Cryptocurrency). In mining, the nodes must process cryptocurrency transactions and verify that they are real. They must solve a mathematical problem. When the problem is solved, the block of transactions is verified, and a new block is created. Each block has a new problem and a new solution for miners to find. The first computer to solve the problem receives new cryptocurrency (i.e., Proof of Work). Mining uses a lot of electricity. Large-scale miners use mining farms. These are warehouses with thousands of computer mining for various cryptocurrencies and are often located in China or Southeast Asia, where operating costs are low.

2.3 Cryptography

The keys that move balances around the blockchain utilize a type of one-way cryptography called public-key cryptography. The "hashes" (the one-way cryptographic codes that tie together blocks on the blockchain) use a similar type of cryptography. Meanwhile, transaction data sent and stored on the blockchain is tokenized (tokenization is a type of one-way cryptography that points to data but does not contain all the original data). The key to understanding these layers of encryption which ensure a system like Bitcoin's (some coins work a little differently) is found in one-way cryptographic functions (cryptographic hash functions, cryptographic tokens, and public-key cryptography are all names for specific, but related, types of one-way cryptographic functions). The main idea is that cryptocurrency uses a type of cryptography that is easy to compute one way, but hard to compute the other way without a "key". It is easy to create a strong password if you are in your online bank account, but very hard for others to guess a strong password after it has been created.

2.4 Trading Cryptocurrency

Cryptocurrency can be obtained most of the same ways other types of currencies can. You can exchange goods and services for cryptocurrency, you can trade dollars for cryptocurrencies, or you can trade cryptocurrencies for other cryptocurrencies. Trading is generally done via brokers and exchanges. Brokers are third parties that buy/sell cryptocurrency and exchanges are like online stock exchanges for cryptocurrency. One can also trade cryptocurrencies directly between peers. Peer-to-peer exchanges can be assisted by a third party.

2.5 Non-Fungible Tokens (NFTs)

A token that represents ownership of a unique digital item (e.g., of art, a government ID, or a specific unit of production) that could be physical, intangible, or digital assets. An NFT certifies that the holder owns the underlying digital asset and can sell, trade, or redeem it. It can be used for proving your identity and granting access (to either a virtual or physical space), tokenizing your supply chain to track inventory movement and ownership, or ownership of virtual items (e.g., games). Visual artists and musicians can use NFTs to sell works directly to fans. Venues are selling NFT tickets to events to reduce scalping and give more revenue to artists. Real estate professionals are using NFT deeds and contracts to streamline the process of buying and selling property. NFTs have been in development since 2014.

Fungibility is a characteristic of a digital or physical object that refers to its ability to be interchanged or replaced with another item of the same type (i.e., mutual interchangeability). Dollar bills and shares of the same class of stock are examples of fungible items.

NFTs are nonfungible due to complex encryption techniques that assign a unique ID (hash value) to the underlying object. A blockchain NFT transaction will typically contain, at a minimum, the unique ID and associated wallet addresses (The term "wallet" in this context, refers to the online accounts where digital assets are held, like logging in to a bank website and seeing the balances of different accounts).

NFTs are linked to an underlying item. NFTs are computer files combined with proof of ownership and authenticity, like a deed. They exist on a blockchain. Cryptocurrencies are fungible, one bitcoin is always worth the same as any other bitcoin. NFTs have unique valuations set by the highest bidder. Individuals who want to sell their work as NFTs must sign up with a marketplace, then mint digital tokens by uploading and validating their information on the blockchain (usually the Ethereum blockchain). This usually costs between $40 to $200. They can then list their work for auction on an NFT marketplace, like eBay.

NFTs are distinguished from other digital assets in that they are always linked to an underlying item that could be digital, intangible, or physical. The most common type of NFTs in existence in 2023 are those linked to a graphic art file (e.g., JPEG, PNG, GIF). NFTs' ability to prove ownership and provide an auditable trail of activity via a blockchain has been very important for graphic artists because it allows them to have definite proof that they created and own or have rights to an image.

3. The Outlook for Cryptocurrency

Users can use their digital assets to purchase products and services. These can include digital asset products such as NFTs but may also include things beyond the blockchain system like tickets to concerts or the deed to a house. Users spend their digital assets on items at physical retailers. Built into every point-of-sale system is the capability to accept digital assets as tender. Eventually, you will spend digital assets on everything from groceries to cars. Financial opportunities are being built into the options to purchase a digital asset. Being able to get a loan, insurance, or other financial instrument automatically agreed to by a provider via the blockchain. Users can trade digital assets much like in traditional stock markets. Users may want to trade to enact speculative investments or to acquire the currency necessary to play a new game. Games built on a blockchain can offer tokenized in-game currency to their players. Because the currency is a digital asset, users can have real ownership over the value they earn. This includes the right to sell to or exchange with other players in a way traditional game developers have never offered. In-game currency being traded for other digital assets between

gamers and potential gamers who are interested in joining the game. Decentralized apps (dApps) include any other applications built on a blockchain. dApps have a distinct advantage over traditional mobile and desktop apps in that they will have more direct access to user assets due to their foundation on the blockchain.

4. Conclusion

This technology will give greater access to financial services in emerging economies. Most people around the world lack access to banks and currency exchange. Blockchain-based distributed ledgers could change this. Just as the smartphone gave people without telephone lines access to communication, information, and electronic commerce, these technologies can provide a person the validity needed to open a bank account or borrow money. A person would not need to prove real estate ownership or meet other qualifications that are challenging in many countries.

Companies can use the distributed, publicly verified, and nearly real-time ledger of transactions for accounting, data mining, and records verification. This could reduce the effort spent on reconciling information among various computer systems. It could also link the systems to external information sources, such as pricing feeds (i.e., electronic vendors of trading data), in a more customizable and secure way.

Faster settlement and immediate notification would reduce the amount of cash and other collateral that a bank must hold to lessen settlement risk. Blockchain's transparent tracking of capital flows could require banks to keep less money on reserve for working capital or foreign exchange capital needs. A central, indisputable ledger of transactions would allow auditors and regulators to rapidly monitor the flow of financial data, avoiding after-the-fact verification.

A wide variety of supplementary businesses are quickly developing. Cryptocurrency exchanges, such as Armory and Coinbase, help their clients buy and sell cryptocurrency, store their holdings, manage the private encryption keys for those assets, and protect their currency holdings from online theft. Another company, Libra, helps corporations report, audit, and analyze digital asset transactions, regardless of the blockchain database used. Other startups, including Blockstream, Digital Asset Holdings, and itBit, make it easy for digital asset transactions for banks and other financial institutions. Wallet Recovery Services helps the owner of a lost or forgotten password try to recover it through decryption.

References

Ghimire, S., & Selvaraj, H. (2023). *A survey on bitcoin cryptocurrency and its mining*. Retrieved April 25, 2023, from https://www.researchgate.net/profile/Suman-Ghimire-5/publication/331040157_A_Survey_on_Bitcoin_Cryptocurrency_and_its_Mining/links/5cb7b6ba92851c8d22f2d9ba/A-Survey-on-Bitcoin-Cryptocurrency-and-its-Mining.pdf

History of Cryptocurrency: The idea, journey, and evolution. (2023). Retrieved April 22, 2023, from https://worldcoin.org/articles/history-of-cryptocurrency

Making sense of bitcoin, cryptocurrency and blockchain. (2023). Retrieved April 24, 2023, from https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

Today's cryptocurrency prices by market cap. (2023). Retrieved May 25, 2023, from https://coinmarketcap.com/

History of cryptocurrencies (how everything started). (July 29, 2022). Retrieved April 22, 2023, from https://www.analyticsinsight.net/history-of-cryptocurrencies-how-everything-started/

Seth, S. (May 15, 2022). *Explaining the crypto in cryptocurrency*. Retrieved April 25, 2023, from https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/

Tuwiner, J. (January 1, 2023). *Cryptocurrency statistics, facts & trends*. Retrieved May 1, 2023, from https://buybitcoinworldwide.com/cryptocurrency-statistics/

Siripurapu, A., & Berman, N. (February 28, 2023). *Cryptocurrencies, digital dollars, and the future of money*. Retrieved April 22, 2023, from https://www.cfr.org/backgrounder/cryptocurrencies-digital-dollars-and-future-money

Beyer, E. J. (April 6, 2023). Cryptocurrency and NFTs: What's the difference? Retrieved April 26, 2023, from https://nftnow.com/guides/cryptocurrency-and-nfts-whats-the-difference/#:~:text=NFT%20stands%20for%20non%2Dfungible,the%20blockchain%20as%20cryptographic%20assets