Design and Features of Block Chain and Algorithm

Xinghe Lu(✉)

Malvern College Qingdao, Qingdao 266109, China
jasonlu05@protonmail.com

Abstract. Nowadays, there are more and more blockchain technologies used by cryptocurrencies. They use different algorithms to transfer and keep users safe. Some of them are new and full of efficiency, and some are wasteful. Today cryptocurrency has influenced human life firmly, so it is necessary to improve some of it. In this paper, we will first organize some famous kinds of cryptocurrency, then compare their algorithms and applications and propose future development trends.

Keywords: Block chain · Bitcoin · Ethereum · Tether · BNB

1 Introduction

With the development of blockchain techniques, cryptocurrencies are becoming more and more popular. Among them, Bitcoin, Ethereum, Tether, BNB are widely known these days. *Bitcoin* is a decentralized digital currency that enables instant payments around the world [1]. Bitcoin uses peer-to-peer technology to function without central authority: transaction management and currency issuance are carried out collectively by the network. Bitcoin is the first successful implementation of a distributed cryptocurrency. Bitcoin has all the desirable properties of a financial asset. They are portable, durable, divisible, recognizable, fungible, scarce, and difficult to counterfeit. However, the number of available used bitcoin is limited (estimated at 21 million). Ethereum is a kind of crypto-currency like bitcoin. Ethereum is also a platform and programming language, including the digital currency Ether (Ether) and the Ethereum script used to build and publish distributed applications, the smart contract programming language. The issuance of ether is capped at 18 million per year. Transactions, pack and upload blocks, mining, creation, and way to prevent double-spending and ensure that the wallet has enough bitcoin to pay are similar to bitcoin. So, the author will not repeat them in the "Characteristic" part.

Tether is a stablecoin developed to observe and match the value of a fiat currency. It is pegged to the US dollar, meaning it maintains a value of $1 [2]. As a stablecoin, Tether is supported by traditional assets, which secure a large reserve, making it an important factor that maintains a sound crypto market. Tether is less volatile than other coins because it holds a fixed value that follows its fiat currency. And Binance coin (BNB)

S. Kadry et al. (Eds.): BDEIM 2022, AEBMR 233, pp. 562–569, 2023.
https://doi.org/10.2991/978-94-6463-124-1_66

was created to allow users of the Binance exchange to pay for its services [3] easily. Binance is the most widely used exchange worldwide. BNB is developed to support user experience in the Binance exchange. Some of BNB's characteristics include cheaper transaction costs, fast and secured transactions, and a potential rise in its value in the future.

In this paper, we will first detail the characteristics of bitcoin, Ethereum, tether and BNB. Then we will outline their algorithms and applications and finally propose future development trends for them.

2 Characteristics of Cryptocurrency

2.1 Bitcoin

In bitcoin, firstly, the immense amount of users and be used wildly. For a coin to have any value, the creation of coins must be limited. Following a mutually agreed upon set of rules, new coins are mined slowly. A user can run a software program that searches for a solution to a complex math problem by mining; the math problem's difficulty is precisely known. This difficulty is automatically adjusted on a predictable schedule so that the number of solutions found globally in a given unit of time is constant: the global system aims for 6 per hour [4, 5].

The transactions of bitcoin could be easily explained by using Alice and Bob. Such as, Alice wants to pay Bob 1 bitcoin. Alice adds Bob's address and the number of bitcoins to transfer to a message: a 'transaction' message. Alice signs the transaction with her private key and announces her public key for signature verification. Digital signatures use asymmetric encryption. The private key is used in the SHA-256 to generate a digital signature. Anyone can use the public key to authenticate the digital signature. Then Alice broadcasts the transaction on the Bitcoin network for all to see. Everybody can use the public key to check whether Alice created the message. Each owner transfers the coin to the next by digitally signing the previous transaction's hash and the next owner's public key and adding these to the end of the coin.

Double-spending could also be prevented in bitcoin. For example, when multiple valid continuations to this chain appear, only the longest such branch is accepted and extended further. So If somebody wants to double-spending, that person would need to muster more computing power than all other Bitcoin users combined. Meanwhile, bitcoin payments are based on transaction records, not balances. A transaction must have records showing that the amount of revenue exceeds the amount of the expense for the transaction to continue. Lastly, to pack and upload blocks in bitcoin, the information of the new block (the SHA-256 function value of the previous block + the basic information of the new block + all transaction records contained in the new block) is combined into a string. Find another number randomly and add it to the end of that chain to form a new chain. Recalculate the SHA-256 of this new string. The block can be uploaded if the first 72 bits are all 0.

Bitcoin is also widely used now. Some nations have implemented Bitcoin Cash machines. They can use bitcoins to pay for their daily life. Such as Australia. Bitcoin Cash machines were designed to sell Bitcoin to users in fiat currency, serving as another choice for people unfamiliar with the exchange. Most of these Bitcoin Cash machines in Australia have the option of both buying and selling Bitcoin. Also, some businesses, organizations, or individuals accept Bitcoin and other cryptocurrencies to pay.BitcoinWide.com is a global, open, and accessible platform to search for them. And local businesses, like cafes and restaurants, also accept Bitcoin. Users can use Coinmap.org to browse thousands of companies all over the world.

2.2 Ethereum

Ethereum provides a more powerful contract programming environment, and users can write smart contract applications. Ethereum can realize complex logic in various commercial and non-commercial environments, such as firms paying salaries to labor and Tenants paying rent. Traditional software systems can be chained through smart contracts, and more powerful management capabilities can be exerted. This is equivalent to hiding the complexity of the underlying technology and allowing application developers to focus more on application logic and business logic. Meanwhile, there are two kinds of users in Ethereum. External owned accounts and smart contracts. Application developers upload programs (reusable code snippets) to the Ethereum virtual machine state, and users make requests to execute these code snippets with different parameters. The programs that we upload to the network and are executed by the network are called smart contracts. Externally owned accounts can use private keys to sign transactions and are not associated with any code. Smart contracts are controlled by their code and have code associated with it. A message sent between two externally owned accounts is simply a transfer of value. However, a message from an externally owned account to the smart contract account activates the contract account's code, allowing it to perform various actions. Smart contracts cannot initiate a transaction themselves. Instead, a Smart contract only triggers a transaction in response to a transaction after receiving it (either from an externally owned account or another contract account). Every user can create a smart contract and expose it on the network, using the blockchain as its data layer, paying fees to the network. Users can then invoke the smart contract to execute their code and pay the network [6].

In the Ethereum network, there is a standardized computer (called the Ethereum Virtual Machine, or EVM) whose state is agreed upon by everyone in the Ethereum network. Everyone participating in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer. Furthermore, any participant can broadcast requests to this computer to perform arbitrary computations. Whenever such a request is broadcast to the network, other participants on the network verify, confirm, and execute ("perform") the computation. This command causes a state change in the EVM propagated across the network. One of the most significant advantages of smart contracts over ordinary contracts is the automatic execution of results when contract conditions are met. Users do not need to wait for manual execution results. In other words: smart contracts do not require trust. Every computation made by a transaction on the Ethereum network incurs a fee, which is paid in "gas. "Gas measures the cost unit required in a specific calculation.

Non-Fungible Tokens (NFTs) are another addition to the Ethereum blockchain that have gained popularity over the past two years. Although NFTs were born on Ethereum in 2017, they were not known to the public until recently. NFTs have revolutionized the art world, providing what has long been considered vital, artwork's provenance. Although some NFT marketplaces have been launched on other blockchains, Ethereum still has several of the largest NFT marketplaces in the world, such as Open Sea and Super Rare. Traditional auction houses have also realized the value of the NFT market, with Sotheby's and Christie's holding multiple NFT auctions. MakerDAO is an Ethereum-based peer-to-peer organization that provides users with cryptocurrency lending services. Users can deposit Ethereum-based tokens into the protocol to borrow. The smart contract makes this dream come true.

2.3 Tether

Tether is created by fully backing it with a large traditional reserve. To be specific, the creation of Tether occurred by holding 1:1 deposits of USD at banks (Hicks). The creation also involves using private authorization keys to sign and transmit the creation of transactions. The created tokens will be authorized but will not stay in Tether's treasury. It will be released to respond to the demand of the market. To transact in Tether, a new user must register and go through the verification process. This process also requires activation of Two-Factor Authentication (2FA). A user can use exchanges to buy and sell Tether. The process depends on the exchange, but the common way of buying involves entering an exchange, choosing a payment method, and then selecting Tether. To sell, the user must determine the quantity, choose a payment method, and release the tokens. And to prevent double-spending, Tether was built following the Omni Layer protocol based on Bitcoin's blockchain. It means that it also has a proof-of-work (PoW) mechanism. It is a consensus mechanism that requires users to solve a puzzle to validate transactions and prevent any system from taking over (Frankenfield and Anderson).

When using Tether, it is 100% backed and fully transparent. All Tether tokens (USD ₮) are pegged at 1-to-1 with a matching fiat currency and are backed 100% by Tether's reserves. They publish a daily balance sheet of current assets and reserves. Tether tokens allow customers to transact across different blockchains without the inherent volatility and complexity typically associated with digital tokens. Tether tokens exist because digital tokens are built on various blockchains, including Algor, Ethereum, EOS, Liquid Network, Omni, Tron, Bitcoin Cash's standard ledger protocol, and Solana. Therefore, it is feasible to issue tether tokens on various blockchains depending on the shipping protocol. At the same time, Tether tokens allow customers to transact across multiple blockchain chains without the inherent volatility and complexity typically associated with digital tokens. It avoids Volatility as Tether avoids volatility and is more liquid than other cryptocurrencies. It helps investors evade the unpredictability of other cryptocurrencies that can cause losses. Tether allows crypto investors to avoid volatility, creating losses by drastic high and low changes. Aside from this, Tether's liquidity is more stable [2]. It allows investors to easily transfer and trade coins while reducing the risks of losses caused by drastic price changes.

The Tether can function within multiple blockchains, which makes it popular among investors due to its ease of transfer. It means that it can be stored or transferred to different wallets. Transactions such as transferring from one wallet or cryptocurrency to another can happen within a shorter waiting period. The usual processing period can be less than 2 min to 5 min. Keeping Tether in a wallet within an exchange can make buying and selling faster. Also, Tether also lowers transaction fees. The coin allows worldwide transfer with fees lower than other coins and banks. Large businesses in the crypto ecosystem have incorporated Tether coins. It can work with exchanges, wallets, payment systems, and ATMs worldwide [7]. Hence, it allows easy utilization of fiat currencies within the blockchain systems. Overall, the transfer is cheaper and more convenient.

Tether uses cutting-edge blockchain technology to ensure security. It complies with stringent global security standards and government laws, guaranteeing users that their investments are secured. In addition, Tether guarantees transparency. It maintains daily records that users can view to aid decision-making. Overall, Tether or USDT avoids volatility, is more liquid, allows cheap and fast transactions, and is transparent. Most importantly, Tether guarantees security and safe transactions, lessening users' worries. Further, Tether is convenient to use as most online, and physical stores globally have started to accept Tether coins as payments. Meantime, investors in cryptocurrency will use USDT as a medium of exchange and a safe-haven asset. For example, when users think that the price of bitcoin may fall, convert bitcoin to USDT, hold USDT first and wait for the next time to enter the market because it is a transaction between cryptocurrencies, the time and cost will be higher than cryptocurrencies, Fiat currency conversion to save. Users can also use USDT to participate in financial management solutions of various exchanges or Defi decentralized finance to earn income.

2.4 BNB

The BNB token was initially built upon ERC-20 before its transfer to the Binance Chain ("BNB"). BNB tokens were created with 200,000,000 coins. However, its value is maintained through quarterly auto burns. During transaction, user needs to enter the Binance platform and validate the login attempt using two-factor authentication. To buy, the user will tap "Buy," choose BNB, enter the amount, select the payment method, and confirm the transaction. Selling BNB follows the same process but requires tapping "Sell". The transaction involves a digital signature, which is a mechanism that validates the entered data. The generation of codes ensures the validity of the transaction. Binance utilizes Binance Smart Chain (BSC) to make it impossible for a person to double-spend. BSC involves consensus mechanisms such as "proof-of-stake (PoS) and proof-of-authority (PoA) " ("How to Buy Binance"). PoS requires users to stake capital through smart contracts. This is used to validate the entries to avoid double-spending or being compromised. PoA also avoids double-spending by validating the transactions by requiring users to stake their identity or reputation as collateral. These consensus mechanisms avoid double-spending risks and make each transaction more valid and secure.

BNB is used to transact within the Binance exchange, which offers incentives and discounts that can lower the fees involved in trading. As the Binance exchange is the largest in the world, BNB has become widely used. It also offers convenience for traders within the exchange as it involves faster transactions. Transactions using BNB are fast and secure mainly because it operates within the Binance Smart Chain (BSC). Its feature includes smart contract programming, which supports secured transactions. Smart contracts also involve programs that activate upon meeting a predetermined condition.

This algorithm allows automation of responses that can lead to faster transactions. Also, BNB is a good investment as its future value can increase due to its potential to become more widely used. Merchants, including service providers and hospitality companies, accept BNB payments [3]. Its potential acceptability and use in the future can increase the demand for BNB. This situation can also lead to higher values. Last but not least, the BNB Auto-burn can reduce the volatility of BNB coins. The auto-burn process involves burning up to 100,000,000 BNB coins [8]. The process quarterly adjusts the amount of BNB within the BSC, which allows transparency. However, its main purpose is to raise the value of the unburned tokens.

3 Challenges of Common Cryptocurrency

Firstly, BTC and ETH will use PoW. When miners mine a new block, they must operate on the SHA-256 cryptographic hash function, where the random hash value in the block starts with one or more 0s. As the number of 0s rises, the amount of work required to find this solution grows exponentially, and miners try to find this solution repeatedly. In this, if the attacker wants to modify the information of the block that has already appeared, the attacker must complete the workload of the block plus all subsequent blocks and eventually catch up with and surpass the workload of the honest nodes. It is a waste of the node's computing power. Secondly, BTC broadcasts records of transactions. So, when people use bitcoin more frequently, It will be hard to synchronize records. Thirdly, USDT is a centralized, stablecoin. So, users need to take some risks, which are shown as follows.

(1) The risk of account opacity. Since the date of USDT's issuance, Tether has announced a 1:1 peg to the US dollar, but the public has always doubted whether it has sufficient US dollar deposit reserves. Tether has so far only released an audit report written by a law firm rather than a professional accounting firm, proving that it has sufficient reserves. In essence, its account status is not transparent, and it is difficult to confirm that it has sufficient reserves through strict third-party audits. Moreover, in March 2019, Tether's official website changed the statement that it was 1:1 anchored with the US dollar to be backed by reserves such as US dollars and equivalents. At the end of April 2019, Tether Chief Legal Officer Stuart Hoegner confessed that only 74% of all USDT issued by Tether could be backed by currency or equivalents. Tether's practice of changing day and night will inevitably make people doubtful.

(2) Risk of misappropriation of client funds. In April 2019, the New York State Attorney General's Office believed that Tether misappropriated $850 million from Bitfinex to cover losses. Bitfinex claimed this was just an accident when working with a third-party company. According to the screenshots of the accusation documents on the website of the New York Attorney General's Office, five important people, including the CEO, CFO, and chief legal counsel of both Tether and Bitfinex, hold the same positions in the two companies, that is, the two companies are essentially composed of A management group operates. Given the highly overlapping relationship between the executives of the two companies, if there is no evidence to prove it, it is inevitable to be suspected of misappropriation of funds.

(3) Risk of lack of effective regulation. Tether and the exchange Bitfinex are registered in the British Virgin Islands and Hong Kong, respectively, and are not regulated by the US financial system. However, the extraterritorial jurisdiction of US law has the effect of "long-arm jurisdiction", that is, as long as an act that occurs in a foreign country has an "effect" in the territory of the country, regardless of whether the perpetrator has the nationality or domicile of the country, regardless of whether the act complies with the law of the place where the perpetrator is located, the domestic courts can exercise jurisdiction over the litigation consequences arising from such effects. On the one hand, the strict extraterritorial jurisdiction of the United States may cause Tether to suffer huge fines, which will cause damage to the rights and interests of USDT holders; on the other hand, Tether lacks effective supervision, and the rights and interests of stablecoin holders cannot be effectively protected. Comply with the relevant laws of the host country, such as anti-money laundering, anti-terrorist financing, and foreign exchange control. The issue of jurisdiction is the biggest current dispute between New York State prosecutors and Tether. For holders of Chinese USDT, an unregulated stablecoin issuer is like a cat beside a fish tank, which has never been able to win the public's trust.

4 Discussion

The computing power of Bitcoin and Ethereum miners can be used to perform some valuable calculations. In my opinion, these calculations should cost roughly the same amount of computing power to computing. A miner can be assigned multiple computing tasks as long as the computing power required to complete these computing tasks is the same as the computing power required to calculate the correct hash in the previous version. Also, they should not come from a committee, because this violates the principle of decentralization. This committee will be able to control miners' mining speed. At the same time, the time required for auditing and calculation is too long, and the efficiency is too low to meet the speed of blockchain packaging. A possible we could do is to let the world's top 1000 universities choose the topic. If a miner finds an abnormal amount of computation, the school will be disqualified from posting a question. In this way, all universities that comply with the regulations can have free supercomputers. When the university publishes the calculation, it uses the signature. It discloses the public key to allow all users to have the right to check, to prevent miners from maliciously threatening the university due to the abnormal amount of calculation.

Another thing would be is that we all know that Western countries (such as the United States and the United Kingdom) have many powerful universities and their rankings are very high. But I think this won't make the coins of users worldwide controlled by Western countries because firstly, it is not easy to simultaneously control all the universities in one's own country. Secondly, if they collectively choose a calculation problem with an abnormal amount of calculation, they will be collectively banned. Finally, the penetration rate of cryptocurrencies in Western countries is higher than in other regions. If they control Bitcoin and Ethereum, these two cryptocurrencies will depreciate rapidly, so there is no reason for them to exchange their big losses for other countries' small losses.

5 Conclusion

Nowadays, cryptocurrencies are becoming more and more popular, such as bitcoin, Ethereum, tether, BNB. In this paper, the authors introduced the above cryptocurrencies, and talked about their algorithms and applications. Through the analysis of these cryptocurrencies, it can be known that their computing power can be used to perform some valuable calculations. In the future, more value in cryptocurrencies will be found, and they will be used in more scenes.

References

1. Bitcoin Wiki. https://en.bitcoin.it/wiki/Main_Page
2. Thomson Reuters™. https://checkpointlearning.thomsonreuters.com/Mktg/CorpNews/ECCNEWS054/ECCNEWS054.html
3. Help: Introduction - Bitcoin Wiki. https://en.bitcoin.it/wiki/Help:Introduction
4. Panagou, Eleni, and Manolis Vavalis. "Towards an Open and Decentralized Case Law Curation Ecosystem.“ PLoS One, vol. 15, no. 10, Public Library of Science, Oct. 2020, p. e0240041
5. "FAQs." Tether, https://tether.to/en/faqs/. Accessed 28 August 2022.
6. Hicks, Coryanne. "What Is Tether? How Does It Work?" Forbes, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-tether-usdt/. Accessed 28 August 2022.
7. Lisa, Andrew. "Binance Coin (BNB): Why It is So Interesting to the Cryptocurrency World." Yahoo! Finance. https://finance.yahoo.com/news/binance-coin-bnb-why-interesting-120011296.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGhA-dcrBarOdEeuxeauXsWGb0QzehJwYYK54ZwtysXz3-ZadRRPJwCBlVpy20HIau7D9xDZ9w-WxVFmT3UrSCySgHNRC0Gf24TpJiHSmgGHpQ3agLP8lP-GGPnuL_shFAUZL2pYq8IYnZTOARwIrZq_z3npHBVp-VFEdfqJ7TKK. Accessed 28 August 2022.
8. "What is BNB?" Binance, https://www.binance.com/en/bnb. Accessed 28 August 2022.