Proceedings of the 5th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/15/20230811

Research on digital currency based on encryption technology

Yubo Zhang

School of Computer Science, Xi 'an Polytechnic University, Xi 'a Shaanxi,710000, China

42009040113@stu.xpu.edu.cn

Abstract. Digital currencies have become an increasingly popular topic of discussion in recent years. Digital currencies are virtual forms of currency that operate outside the traditional banking system. They are based on cryptographic technologies and are often decentralized, meaning they are not controlled by a central authority. The most well-known digital currency is Bitcoin, but there are many other types of digital currencies in existence. Digital currencies can be used to purchase goods and services online or transferred between users directly without intermediaries like banks. They have gained popularity due to their potential for increased security, transparency, and efficiency in financial transactions. In today's digital currency, a variety of digital currencies emerge in an endless stream, and crypto technology is also constantly developing to improve the security of digital currency payments. In section 2, this paper briefly introduces several common digital currencies and encryption algorithms, and in section 3, this paper introduces these typical digital currencies in detail through the analysis of representative literature. Bitcoin is mainly encrypted based on blockchain technology, and its encryption principle is mainly divided into three parts: public key encryption, hash function, and proof of work. Ethereum is a distributed blockchain platform with encryption principles similar to Bitcoin, including public key encryption and hashing algorithms. Ripple is a distributed cryptocurrency. Its encryption principle mainly adopts the public-private key encryption system. In terms of encryption technology, blockchain technology, the Hash algorithm and symmetric and asymmetric encryption are also popular encryption algorithms in digital currencies.

Keywords: bitcoin, Ethereum, ripple, blockchain, hash.

1. Introduction

Digital currency, additionally recognized as Cryptocurrency, is a cryptocurrency asset primarily based on cryptography. It makes use of cryptography to impenetrable transactions and manipulates the advent of new units, making it greater impervious and obvious than standard economic systems. The origins of digital currency can be traced back to the late 1990s when computer scientist Nick Szabo coined the term "bit gold". Bit gold was a precursor to Bitcoin and other digital currencies, relying on complex algorithms to verify transactions and prevent double-spending. However, it wasn't until 2009 that the first digital currency, Bitcoin, was introduced to the world. Bitcoin was created by an unknown person or group using the pseudonym Satoshi Nakamoto, and it quickly gained popularity among tech enthusiasts and libertarians who were drawn to its decentralized nature and potential to disrupt traditional financial systems [1].

DOI: 10.54254/2755-2721/15/20230811

In section 2 this paper briefly introduced the types of digital currencies and the classification of cryptographic technologies they use. This paper gave a brief background on Bitcoin, Ethereum, and Ripple and the cryptography they use. In terms of encryption technology, this paper also introduced three main encryption technologies: Blockchain, Hash, and Symmetric and asymmetric encryption. Blockchain encryption technology is a technology that uses cryptography to protect the data in the blockchain network. On the blockchain, every transaction needs to be encrypted, including the content of the transaction, the time of the transaction, the parties to the transaction, and so on. A blockchain is created by organizing this data into blocks, each of which contains an encrypted summary that is connected to the summary of the block before it uses a hash function. An algorithm known as hash encryption converts arbitrary-length inputs (messages) to outputs with set lengths. For message integrity checks, digital signatures, and password storage, hash encryption is utilized. The same key is used for both encryption and decryption in symmetric encryption, also referred to as private key encryption. Asymmetric encryption, commonly referred to as public key encryption, is a method that encrypts and decrypts data using two keys: the public key and the private key.

In section 3, this paper gives a detailed description of these currencies by analyzing their representative works. Bitcoin is a digital cryptocurrency that is issued and traded using blockchain technology. Bitcoin's features include decentralization, anonymity, and fixed circulation. It does not rely on banks or government agencies, can transact across borders, and can make fast money transfers in a short time. Ethereum is a distributed computing platform based on blockchain technology with smart contract capabilities that can support the development and operation of a variety of decentralized applications. At the heart of Ethereum are Ether, the cryptocurrency within the platform and the "fuel" charge for the execution of smart contracts on the platform. Ethereum realizes more flexible smart contract functions based on blockchain technology. Compared with other blockchain projects such as Bitcoin, Ethereum has more kinds of applications and more powerful scalability. Ripple is a digital cryptocurrency, as well as a decentralized payment protocol and open-source global payment network. Ripple uses blockchain technology and cryptocurrencies to help users quickly and easily transfer assets without the need for complex transfer processes and high fees. Ripple also offers an "XRP" digital currency that can be used to transfer money and make payments across borders. Compared to other digital currencies, Ripple focuses more on speeding up transactions and reducing transaction costs, as well as making payments more secure.

2. Preliminary

2.1. The introduction of digital currency

Bitcoin. The digital currency has been successfully implemented in recent years and has gradually swept the world, but the idea of digital currency has been proposed as early as the third technological revolution [1]. In 2008, bitcoin was proposed by the anonymous Satoshi Nakamoto, which aims to make money transactions free and safe by removing the control of money circulation by traditional financial institutions. Bitcoin used a generator of the computational proof which contains a system that utilizes a P2P distributed timestamp server as the chronological order of transactions [2]. Bitcoin's encryption technology employs two types of keys, namely a public key and a private key. The public key is used to determine the next owner of a Bitcoin during a transaction. The prior transaction's digitally signed hash is also included in the definition of the transaction [2]. The same encryption and decryption techniques are used by both private and public keys, but only certain communications can be decrypted by each key individually [3]. The public key is used for verification in a Bitcoin transaction, whereas the private key is used for signing. Figure 1 [1] shows the structure of a Bitcoin transaction on a blockchain.

DOI: 10.54254/2755-2721/15/20230811

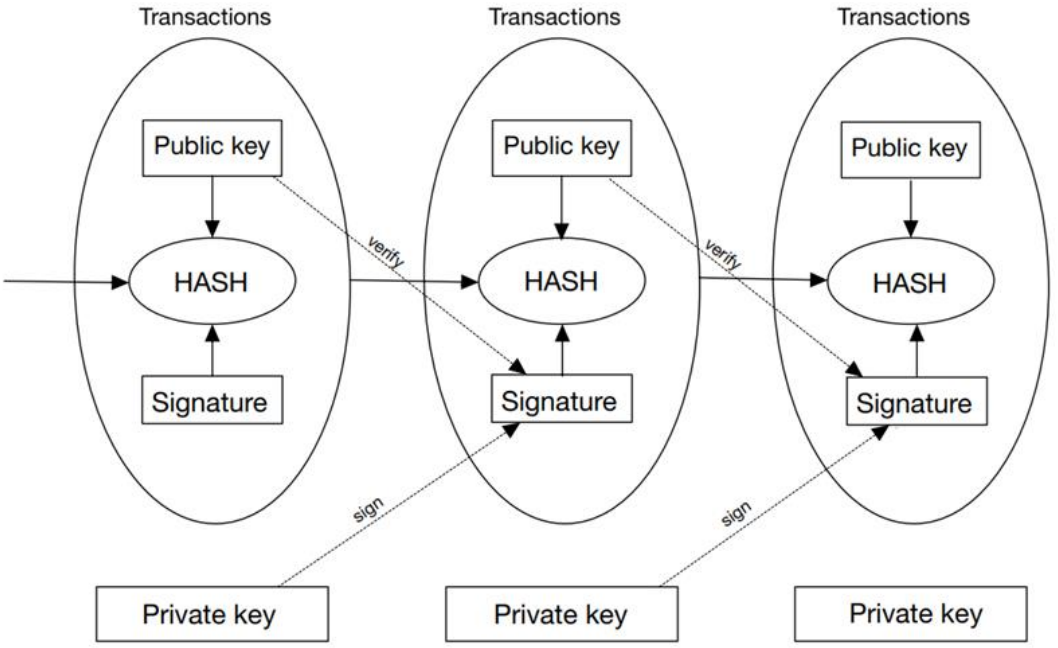

Figure 1. An Ethereum block with hashed transactions into a Merkle tree [1].

In addition, the Bitcoin network also adopts a distributed accounting system, that is, blockchain technology. Each node has a complete ledger that records the balance and transaction history of each user [4]. When a user initiates a new transaction, the node will verify it in its ledger. If the transaction is legal, the transaction will be packaged into a new block and broadcast to other nodes in the network. Other nodes will also validate this new block and add it to their ledger.

Ethereum. Ethereum is an open-source, distributed blockchain platform. It can not only support cryptocurrency transactions but also the execution of smart contracts [5]. Ethereum uses its virtual machine (EVM) to execute smart contract code and uses ether (ETH) as a token for cryptocurrency. Ethereum's blockchain technology is very similar to Bitcoin, and it is a ledger system maintained by distributed nodes. Each block contains transaction information, timestamps, and hash values of the previous block [5], [6]. The following is the specific process of Ethereum encryption: First, the user needs to generate a pair of public and private keys. The public key can be used to receive ether or smart contracts, and the private key is used for signed transactions or smart contract execution. When a user initiates a transaction or executes a smart contract, he needs to sign it with the private key to prove this is the operation that the user has sent. At this time, the private key is only held by the user, ensuring the security of the transaction or contract. Use the hash function to convert the signed transaction or contract into a string of numbers [1]. The string of numbers is called a transaction hash or a contract hash value. The transaction or contract hash value is broadcast to the entire network for validation and recording by other nodes [7]. Other nodes can decrypt the signature with the use of the public key and confirm the legality of the transaction or contract. If the verification is successful, the transaction or contract will be introduced to the block. Each block in the blockchain incorporates the hash fee of the preceding block, and this interconnected hash fee chain constitutes an immutable ledger system [8]. If someone tries to change any records in the block, the entire blockchain system will fail and need to be rebuilt [9]. An Ethereum block is shown in Figure 2 [1].

DOI: 10.54254/2755-2721/15/20230811

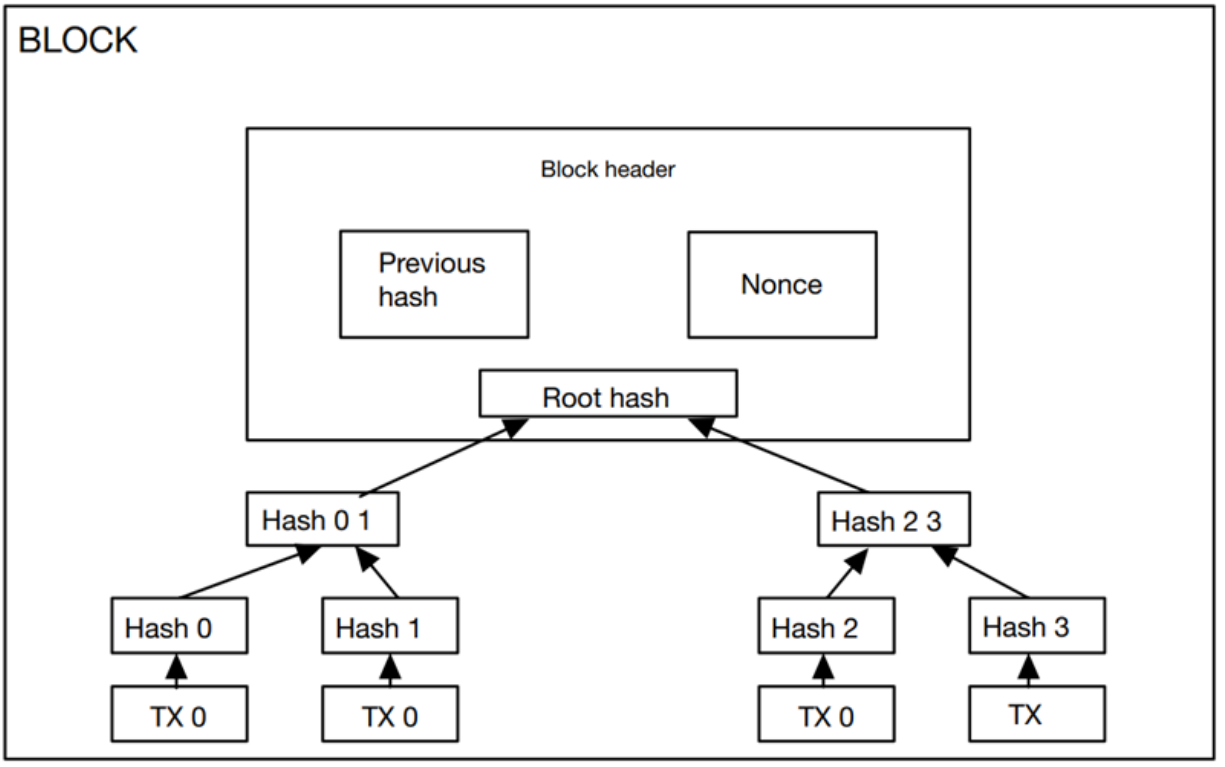

Figure 2. An Ethereum block with hashed transactions into a Merkle tree [1].

Ripple. Ripple [10] is a digital currency based on distributed ledger technology, also known as blockchain [11]. Its encryption principle mainly involves public key encryption and hash functions. Specifically, the encryption process of Ripple is as follows: the sender uses its private key to digitally sign the transaction information and broadcast it to the entire network [12]. The nodes in the network verify this information, including verifying the validity and availability of the digital signature, and whether the sender's Ripple balance is sufficient. If the verification is passed, the node adds the transaction information to the distributed ledger and performs hashing, that is, the transaction information is combined with a random number to generate a fixed-length hash value composed of numbers and letters [12]. The node then broadcasts the hash value to other nodes in the network so that other nodes can also verify the validity and availability of the transaction information.

2.2. The introduction of encryption techniques

The main technologies used in various digital currencies are blockchain technology, and the two core technical points of blockchain are consensus mechanism and cryptography. Next, this paper will introduce two types of cryptographic algorithms mainly applied in the blockchain, one hashing algorithm, and the other is symmetric encryption and asymmetric encryption algorithm.

Hash: Hash encryption is an encryption algorithm that compresses messages of any length to a certain length of the message digest. The simple precept of Hash encryption is to enter the plaintext information into the hash function, and then use a unique mathematical characteristic to convert messages of any size of the entry into a fixed-length output [13]. This output price is generally known as a hash cost or a summary. The simple facts shape of the hash on the blockchain is proven in Figure 3 [13].

DOI: 10.54254/2755-2721/15/20230811

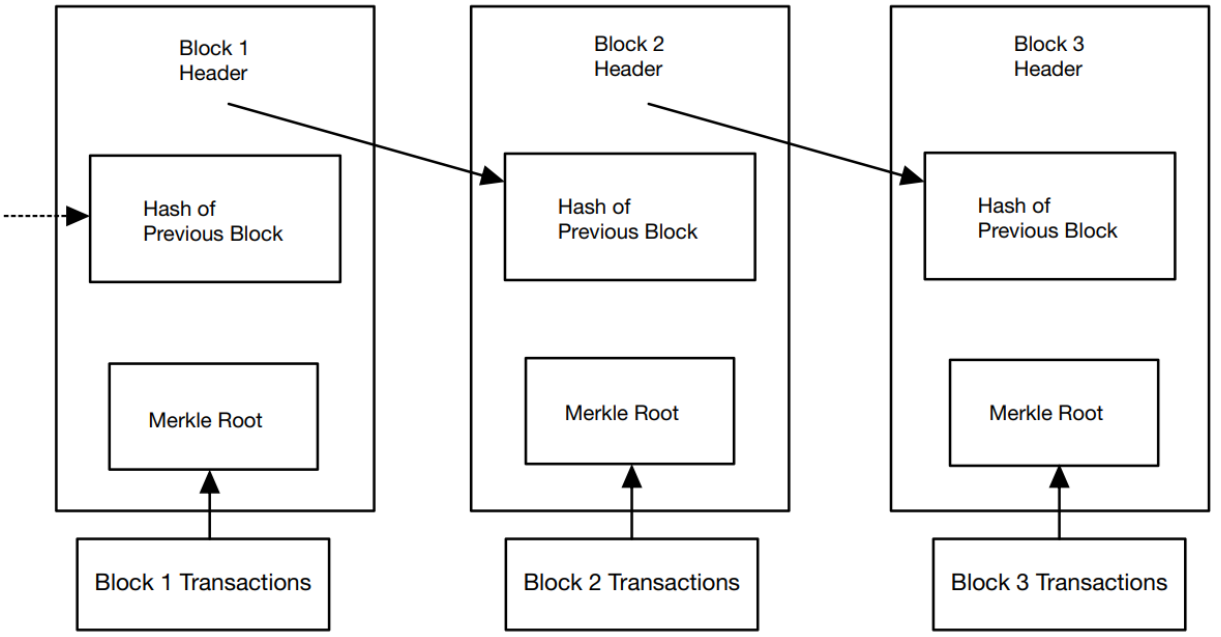

Figure 3. The basic data structure of the hash on the blockchain [13].

An important feature of the hash function is uniqueness, that is, the same input always produces the same output, and even if the input is only a small change, it will lead to different hash values. This hash value can be used to verify the integrity and consistency of the message, as any modification to the original data will result in different hash values. Another important feature of Hash encryption is irreversibility, that is, the original data cannot be reversed through hash values. This feature makes Hash encryption very useful when protecting sensitive information. Once the data is encrypted by hash, this cannot restore the data unless it has the same inverse function as the hash function.

Symmetric Encryption and Asymmetric Encryption Algorithm: Symmetric encryption refers to the encryption technique of encryption and decryption the use of the equal key, whether or not it is encryption or decryption, the equal key is used [14]. Common symmetric encryption algorithms consist of DES (Data Encryption Standard), 3DES (Triple Data Encryption Algorithm), AES (Advanced Encryption Standard), etc. The benefit of a symmetric encryption algorithm is that the encryption and decryption pace is quick and the encryption effectivity is high, however, the drawback is that the safety of the key is without problems threatened. Asymmetric encryption refers to the encryption approach of encryption and decryption the usage of distinctive keys, additionally acknowledged as public key encryption. In uneven encryption, the public key used for encryption can be made public, and the non-public key used for decryption needs to be stored secret [15]. Common uneven encryption algorithms consist of RSA (Ron Rivest, Adi Shamir, Leonard Adleman), ECC (Error Correcting Code), etc. The benefit of the uneven encryption algorithm is that the key protection is high, however, the drawback is that the encryption and decryption velocity is sluggish and the encryption effectivity is low.

Usually, symmetric encryption and asymmetric encryption are used together to give full play to their respective advantages, to achieve more efficient and secure encrypted communication. The comparison of common encryption algorithms of symmetric encryption and asymmetric encryption is shown in Table 1 [14], [15].

DOI: 10.54254/2755-2721/15/20230811

Table 1. The comparison of symmetric encryption and asymmetric encryption [14], [15].

Factors	Symmetric Encryption Algorithms			Asymmetric Encryption Algorithms
	DES	AES	3DES	RSA
Block Size	64 bit	128 bit	64 bit	Variable
Key Size	56 bit	128,192,256 bit	168 bit(k1,k2 and k3) 112 bit(k1 and k2)	Depends on the number of bits in the modulus n where n=p*q
Created By	IBM in 1975	Joan Daeman in 1998	IBM in 1978	Ron Rivest, Adi Shamir, and Leonard Adleman In 1978
Speed	Slow	Fast	Very Slow	Slowest
Rounds	16	9,11,13	48	1
Attack	Brute Force Attack	Side Channel Attacks	Brute Force Attack	Wiener's Attack

3. Literature review

This article summarizes the representative literature on digital currency in recent years, as shown in Table 2 below.

Table 2. Literature Review.

Type and Representative work	Main idea	Advantage	Disadvantage
Bitcoin [1][2][3][6]	Encryption and transactions are conducted via blockchain	High level of security, quick transactions, Low transaction cost	Limited supply, high market price volatility, not being covered by insurance, and anonymity lead to illegal behavior
Ethereum [4][5][7][8][9]	The blockchain technology platform that supports smart contracts	High scalability, smart contract function, decentralization, high security, openness, and interoperability	Throughput limitations, user requirements for technical knowledge, high energy consumption, and systems prone to congestion and delays during peak trading periods
Ripple [10][11][12]	Use blockchain and consensus algorithms, through the internal ledger to achieve currency conversion of different values	Decentralized, fast money transfer, low transaction costs, multiple ways to transact, very flexible technology architecture	Transactions are public and can be tracked and traced; Subject to institutional review and regulation; they have Low security and credibility; High price

3.1. Bitcoin

The main focus of "Blockchain Technology, Bitcoin, and Ethereum: A Short Overview" is the concept of Bitcoin transactions. As defined, the Bitcoin ledger represents a state transition system that records the ownership status of every Bitcoin ever created through transactions and a state transition function [1]. Both Hashcash and Bitcoin employ proof-of-work hashing algorithms, but Bitcoin's algorithm is based on SHA-256.To achieve proof-of-work in Bitcoin, a nonce is added to the block until the resulting value meets the required number of zero digits at the beginning of the block hash. Once completed, this cannot be undone without double counting, and any subsequent blocks will have incorrect hashes if

DOI: 10.54254/2755-2721/15/20230811

manipulated by a malicious attacker [1]. Therefore, the longest chain in the network with a majority consensus rule is followed, which means that an attacker would require significant processing power to override the votes of the most trustworthy nodes and participate in the competition problem if they want to modify a block. In a Merkle tree, transactions within a block are hashed. A Merkle tree is a binary tree structure with numerous leaf nodes and a root hash of all of its offspring nodes. Since any discrepancies in the tree will be mirrored somewhere along the blockchain, merge trees are essential for long-term maintainability. As a result, nodes' blockchain storage systems can use less space. The network only keeps the root hash found in the block header after all transactions in a block have been gathered together and the block has been validated.

In "Bitcoin: A Peer-to-Peer Electronic Cash System," the problem of a receiver not being able to confirm whether a sender has not repeatedly copied the same money is addressed. The payee must demonstrate that most nodes always receive transaction data for the first time whenever a transaction takes place to resolve this issue [5]. The solution that is being suggested comprises a timestamp server that creates a hash of the object block that needs to be timestamped and extensively disseminates it. The existence of the data at the moment the hash value was input must be demonstrated. Each timestamp contains the previous timestamp in its hash, forming a chain that makes subsequent timestamps stronger [5]. This paper aims to establish an allocated timestamp server on a peer-to-peer basis with a proof-of-work system like Adam Back's Hashcash [2]. Proof-of-work involves starting with a nonce to a block and scanning for a value that provides the required zero bits when hashed using SHA-256. The amount of work required is exponentially confirmed by the number of zeros necessary [2].In a timestamp network, proof-of-work is achieved by adding a nonce to a block until a value that satisfies the proof-of-work requirement is found. Once the CPU workload meets the proof of work, the block can't be modified if it doesn't work again since subsequent blocks are chained after it. Any attempt to alter the block will also require redoing all blocks after it [2]. Figure 4 illustrates the changes made to the blockchain before and after implementing the timestamp server.

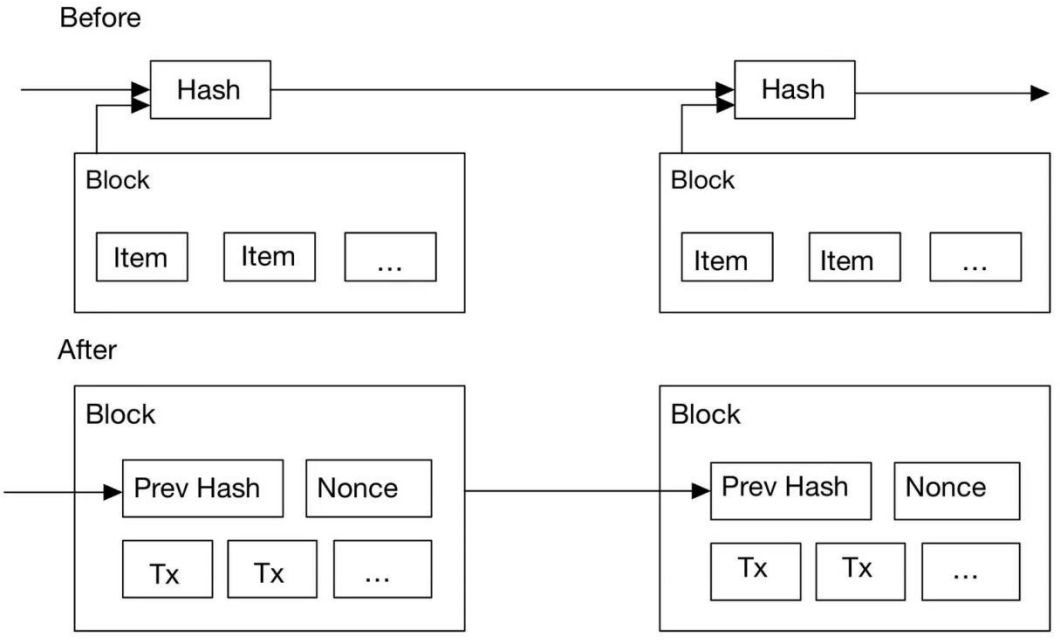

Figure 4. Timestamp the change in the relationship between the stack of the blockchain before and after the server is used [2].

DOI: 10.54254/2755-2721/15/20230811

The page additionally addresses Bitcoin transactions, which can be verified without a complete neighborhood node. Until he is confident that he has the longest chain, the character must keep a copy of the block header from the longest proof-of-work chain that was obtained by querying the local node and obtaining the Merkle branch that connects the transaction to the block where its timestamp is located. He cannot independently validate the transaction, but by connecting it elsewhere in the chain, he can see that a community node has recognized it, and the blocks that follow it confirm that the community has extensively disseminated it, as illustrated in Figure 5 [2].

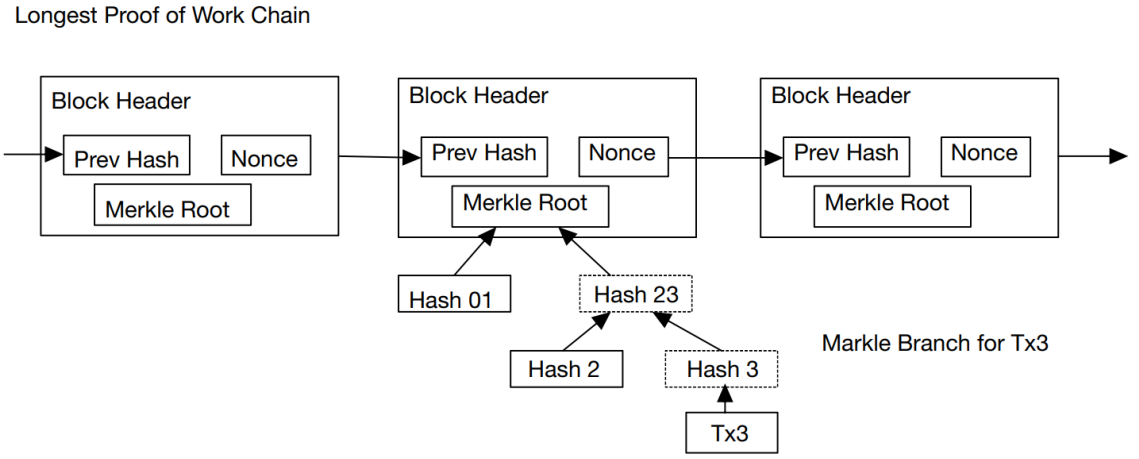

Figure 5. Simplified Payment Verification [2].

Similar content is described in other representative works. To sum up, Bitcoin is a decentralized digital currency and is one of the applications of blockchain technology. Bitcoin uses a simplified payment verification (SPV) and state transition system in transactions to ensure the visibility and security of each transaction. And the method that the payee cannot verify that one of the owners has not spent coins repeatedly is proposed and solved, the payee needs to prove that most nodes received the information for the first time when each transaction occurred. In terms of cryptography, Bitcoin cryptography relies mainly on two basic techniques in cryptography: public-key cryptography for storage and consumption, and cryptographic verification of transactions.

3.2. Ethereum

Vitalik Buterin gives a succinct overview of Ethereum and its transactional design in his well-known essay. With Ethereum, developers will be able to build consensus-based apps with arbitrary functionality as well as incorporate and improve the notions of scripts, cryptocurrencies, and on-chain meta-protocols. These applications combine the benefits that these distinct paradigms' scalability, standardization, feature completeness, ease of development, and interoperability provide. Ethereum is a utility that makes use of the most abstract layer of the blockchain, which may be used in a variety of ways. It can function as a blockchain with a built-in Turing-complete programming language, enabling anybody to develop decentralized apps and smart contracts with their own unique or specific rules for ownership, transaction formats, and state transition functions [4].

In terms of transactions, Ethereum and Bitcoin are very similar, however, there are also significant variations in the following three areas: First, unlike Bitcoin transactions, which can only be made externally, Ethereum messages can be created by external entities or contracts. Second, an explicit option is provided for the inclusion of Ethereum message data. The idea of functions is also included in Ethereum messages, and if the recipient is a contract account, they can decide whether to respond.

DOI: 10.54254/2755-2721/15/20230811

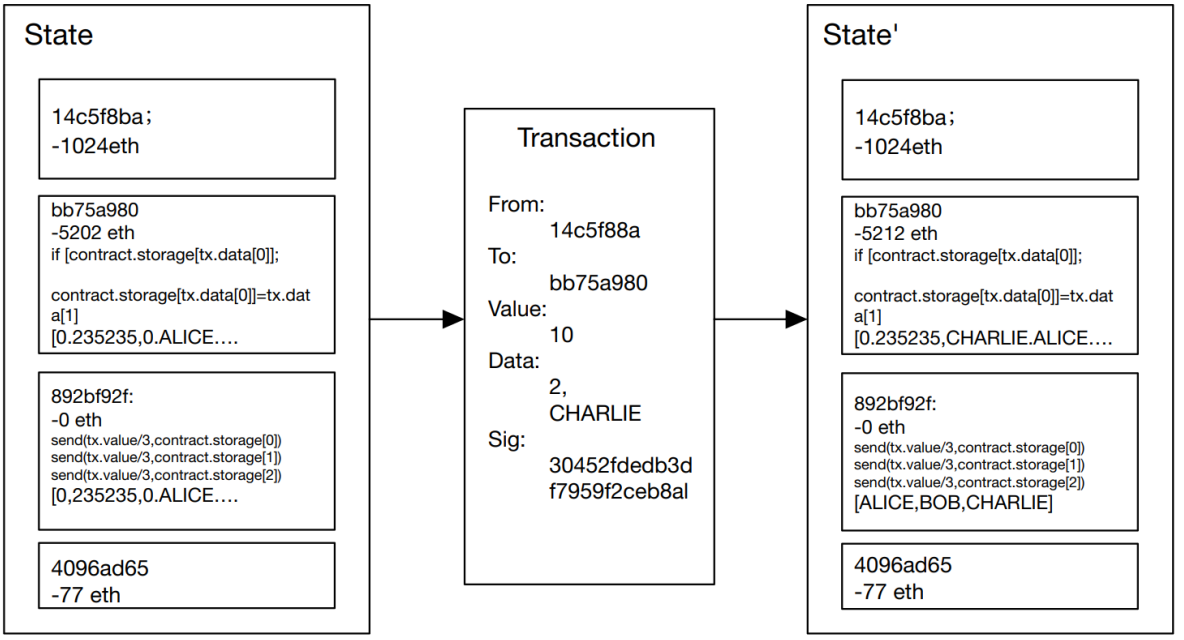

Figure 6. Ethereum State Transition Function [4].

The time duration transaction in Ethereum is used to factor out a signed packet that retail outlets a message despatched from an externally owned account, the transaction consists of the receiver of the message, the signature that identifies the sender, the volume of Ethernet, and the statistics to be sent, and two values named Startgas and Gasprice [4]. For every transaction, to forestall exponential bloat and countless loops in code, this paper wants to set a restriction on the computation steps that the code can perform, together with preliminary messages and any greater messages derived in the course of execution.

In the piece entitled "Defining the Ethereum Virtual Machine for Interactive Theorem Provers," the Ethereum Virtual Machine (EVM) is described. An external account can start a transaction in the EVM by contacting an existing account or initiating a contract. The whole transition between states of the EVM is known once the transaction is started. The state of contracts produced by external accounts after formation is publicly inspectable, even though this is not covered in full. Contracts and external accounts can both call one another. A balance, gas, and data outflow occur when a third-party account calls an account. When an external account is called, a straightforward balance transfer takes place. The balance transaction is done to the called account, and then the called contract's code is executed, if the called account is a contract. The execution of code has the power to change how executed contracts are stored, read every balance in the account and codes, and do much more. The Ethereum implementation contract is displayed in Figure 7 [7].

In the Ethereum Virtual Machine (EVM), transactions are grouped into blocks which serve as units of protocol between nodes on the Ethereum network. The EVM has specific rules for examining the block number of a transaction and the hash value of previous blocks. While blocks in the network generally form a tree structure, there is only one large branch in terms of the state of the EVM, so this paper assumes that the EVM operates sequentially like a computer.

DOI: 10.54254/2755-2721/15/20230811

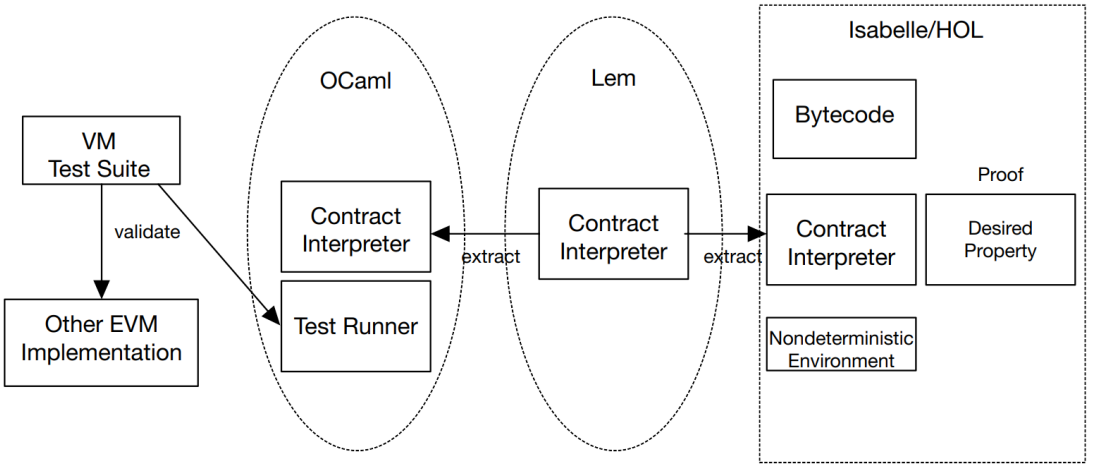

Figure 7. Execution of contract [7].

The environment here refers to anything outside the boundaries of the EVM in addition to every transaction on the EVM other than the verified contract because this article also views a system as a contract. Even tighter than a single account, the entire system symbolizes a single contract call. The contract can invoke the environment, and it also can respond to the calling account. Additionally, the environment has the right to base contract calls on credits outside of its control. Reentrant calls are taken into account when the network refers to our agreement in Figure 8. Reentrant calls are seen as a component of the environment in Figure 9, where the system depicts just one invocation of our contract. Despite the validity of both techniques, this work chooses Figure 9 since it corresponds to the program syntax, which states that CALL commands are followed by further actions in the identical message call rather than the subsequent actions within the reentrant contact [7].

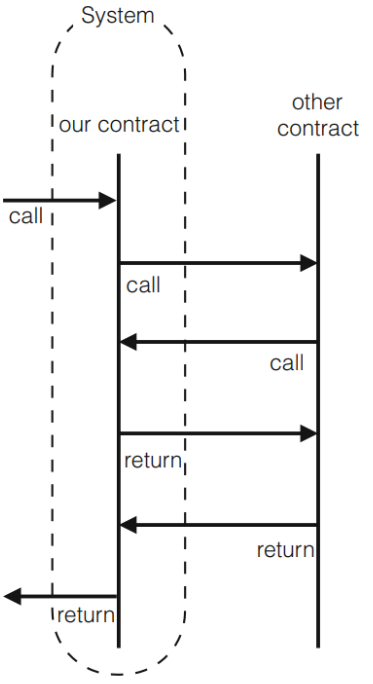

Figure 8. The system is the contract [7].

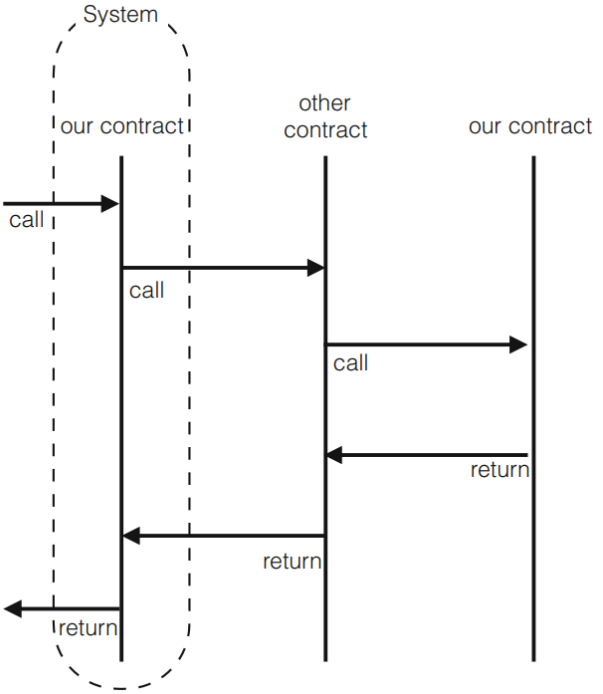

Figure 9. The system is a single invocation [7].

DOI: 10.54254/2755-2721/15/20230811

Similar content is described in other representative works. To sum up, Ethereum is an open-source, distributed computing platform based on blockchain technology that can run smart contracts as well as decentralized applications. Ethereum features include programmability, decentralization, openness, security, and scalability. It has its digital currency, Ether, and is the basis for many decentralized applications. At the heart of Ethereum is the Ethereum Virtual Machine (EVM), a stack-based virtual machine that can execute smart contracts. The goal of Ethereum is to build a global decentralized computer to provide developers and users with a wider range of application scenarios and a better service experience.

3.3. Ripple

The Ripple Protocol Consensus Algorithm uses the way that all nodes communicate once every few seconds to reach consensus, at which point the modern ledger is deemed "closed" and becomes the closing closed [10]. This ensures that the network remains correct and consistent. Assuming that the consensus algorithm no longer forks in the neighborhood and is successful, the closing closed ledger maintained via the capacity of all nodes in the neighborhood will be the same. It wants to be tested that all trouble-free nodes agree on the same set of transactions, regardless of their UNLs (Unique Node List), to meet the requirements of the protocol. Because proof of correctness through the way of itself does no longer guarantee protocol consistency, UNLs may additionally moreover be different for each server. For example, a fork may also be applied with no restrictions on the participants of UNL and the measurement of UNL is no longer larger than 0.2^{+}total the place the complete is the number of nodes in the complete network. This can be illustrated with the aid of an easy instance: think about that there are two clusters in the UNL diagram, every higher than 0.2^{+}in total. All nodes are aggregated to structure a cluster, the place the UNL of every node is the identical set of nodes. Because the two factions do now not share any members, every faction can violate the settlement by way of attaining the right consensus independently of every other. Disagreements between factions forestall consensus on the required 80% consensus threshold, so if the connectivity of the two factions exceeds 0.2^{κ}total, then there is no longer an opportunity for a fork [10].

What the utility can show is its convergence, even although many of the elements are subjective: the consensus procedure will cease in a finite time. The limiting component for algorithm termination is conversation extend between nodes due to the fact the consensus algorithm itself is deterministic and has a preset quantity of rounds t earlier than consensus termination, i.e. The modern set of transactions is declared permitted or disapproved (even if no transaction has extra than 80% of the required settlement at this point, and the consensus is the solely trivial consensus) [10]. The response time of the monitoring node appreciably limits the response time of the node and gets rid of all UNL nodes with a latency increased than the preset bounded b, which ensures that the consensus will terminate at the top sure of tb. But the bounds of correctness and consistency described above should be blissful via the last UNL, deleted after all nodes have been satisfied. If the preliminary UNLs of all nodes meet these conditions, however, some subsequent nodes are eliminated from the community due to latency, and the correctness and consistency ensured will no longer be routinely maintained however need to be comfortable by using a new set of URLs.

Ripple: Overview and Outlook are different from the above, this article not only discusses the protocol consistency algorithm of Ripple but also analysis Ripple under the hood. As previously mentioned, Ripple's consensus protocol is a round-based asynchronous protocol executed by the network's validation server. At the end of each round, all relevant servers publish a newly formed ledger that has been closed after validation by the network.

Transactions are broadcast throughout the network during the collection phase and are subsequently received by the authentication server. The verification server next validates the associated signature and checks the transaction sender's public key from the ledger to confirm the sender's legitimacy. In the candidate set (CS), valid transactions are momentarily saved for later verification. The verification server next examines the relevant XRP transaction history to ensure that the issuing account has enough credit before concluding that the accuracy of transactions stored in CS is accurate. The verification

DOI: 10.54254/2755-2721/15/20230811

server also determines whether there is a trust path between the sender and receiver for IOU payments. Each validation server gathers verified transactions into a verified proposal, which is then sent out over the network. Table 3 summarizes the common fields present in all Ripple transaction types [12].

Table 3. Common fields contained in all Ripple transaction types [12].

Field	Internal Type	Description
Account	Account	The individual account address that started the transaction.
AccountTxnID	Hash256	(Optional) The hash value identifies another transaction. For the present transaction to be valid, the transaction that preceded it (by Sequencing Numbers) additionally has to be valid and equal the hash. The combination of two transactions simultaneously is made easier by this field.
Fee	Amount	(Required) The number of drops represents the amount of XRP that will be lost as a penalty for distributing this transaction around the network.
Flags	UInt32	(Optional) Bit-flags for this transaction, as a set.
LastLedgerSeq	UInt32	(Optional) A perfect ledger sequence quantity that a transaction can show up in.
Memos	Array	(Optional) Additional statistics were used to perceive this transaction.
Sequence	UInt32	(Required) A transaction must have an identification number that must be precisely one higher than the most recent transaction from the same account that was authenticated for it to be regarded as valid.
SigningPubKey	PubKey	(Required) The public key that corresponds with the private key utilized to sign this transaction is shown in ASCII.
SourceTag	UInt32	(Optional) A random integer is utilized to specify the purpose of this payment.
TransactionType	UInt16	The type of transaction.
TxnSignature	VariableLength	(Required) Transaction signature.

This is done in Ripple by first creating a hash tree of every single transaction that passes verification, then signing the tree's root. When verifying server v receives another proposal from the entire network, it determines if the proposal's issuer is the server listed in its UNL and confirms the accuracy of the transactions it contains [12].

Similar content is described in other representative works. In conclusion, Ripple is a digital currency based on distributed ledger technology. It is positioned as a fast and reliable global payment system. Ripple's blockchain system uses a unique consensus algorithm - the Ripple Protocol consensus algorithm. The algorithm is a trust-based algorithm that reaches consensus by integrating the opinions of individual nodes, rather than solving consensus problems through computation. As a result, Ripple's transaction speed is very fast and can be completed in a matter of seconds. In addition, Ripple's transaction fees are relatively low because it employs a trust-based consensus algorithm rather than a computationally intensive proof-of-work algorithm. Ripple's cryptocurrency, XRP, is a digital asset used to pay transaction fees. When a user transacts using the Ripple network, the transaction fee will be paid in XRP. Ripple also offers a network called RippleNet, a global payment network designed to connect financial institutions around the world. RippleNet enables financial institutions to conduct fast, reliable, low-cost transactions on a global scale.

DOI: 10.54254/2755-2721/15/20230811

4. Conclusion

Bitcoin, Ethereum, and Ripple are among the most well-known and valuable digital currencies in the world today. This paper mainly introduced several digital currencies and their main encryption technologies and then carried out a detailed analysis and introduction based on the representative works of these digital currencies. Both Bitcoin and Ethereum are based on blockchain technology, with Bitcoin enabling secure and transparent transactions and storage of value through decentralized, peer-to-peer networking and blockchain technology, while Ethereum is an open-source platform based on blockchain technology that aims to give developers the tools to build decentralized applications. XRP uses a technology called a "consensus ledger," a distributed ledger system that tracks and records every transaction, through both symmetric and asymmetric encryption. Also in the aspect of encryption technology, the main application is blockchain technology, Hash algorithm, and symmetric encryption algorithm.

The future direction of digital currencies is becoming increasingly significant in the global economy. Moving beyond being just speculative assets, digital currencies have evolved into a more stable store of value and an efficient payment system. As such, their appeal continues to grow among investors, businesses, and consumers alike. One potential direction for digital currencies is their widespread adoption as a means of payment and commerce. Major companies like PayPal, Square, and Visa are already integrating digital currencies into their payment systems, and more are expected to follow suit. This opens up new opportunities for digital currencies to become mainstream payment methods, with the added benefit of being faster, cheaper, and more secure than traditional payment systems. However, the future of digital currencies isn't without challenges. Regulatory issues, security concerns, and privacy risks remain major hurdles to overcome. Additionally, the volatility that has plagued many digital currencies in the past still needs to be addressed. Nonetheless, the potential benefits of digital currencies are too great to ignore, and as long as these obstacles are addressed, their growth and adoption will continue to trend upwards.

References

[1] Dejan Vujičić, Dijana Jagodić and Siniša Ranđić 2018 International Symposium INFOTEH-JAHORINA Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview pp 21-23

[2] Satoshi Nakamoto 2008 Bitcoin: Decentralized business review A peer-to-peer electronic cash system

[3] Rainer Böhme, Nicolas Christin, Benjamin Edelman and Tyler Moore 2015 Journal of Economic Perspectives Bitcoin: Economics, Technology, and Governance vol 29 pp 213–238

[4] Vitalik Buterin 2014 white paper A next-generation smart contract and decentralized application platform

[5] Gavin Wood 2014 Ethereum project yellow paper Ethereum: A secure decentralized generalised transaction ledger vol 151 pp 1-32

[6] Sompolinsky, Yonatan,and Aviv Zohar 2015 Financial Cryptography and Data Security: 19th International Conference Secure high-rate transaction processing in bitcoin

[7] Yoichi Hirai 2017 Financial Cryptography and Data Security Defining the Ethereum Virtual Machine for Interactive Theorem Provers pp 520–535

[8] Cachin Christian 2004 Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques Springer Science & Business Media

[9] Nicola Atzei, Massimo Bartoletti and Tiziana Cimoli 2017 Principles of Security and Trust: 6th International Conference, Held as Part of the European Joint Conferences on Theory and Practice of Software Principles of Security and Trust A Survey of Attacks on Ethereum Smart Contracts pp 164–186

[10] Brad Chase, Ethan MacBrough 2018 arXiv preprint Ripple Research Analysis of the XRP Ledger Consensus Protocol vol 1802.07242

DOI: 10.54254/2755-2721/15/20230811

[11] Xiaotie Deng and Fan Chung Graham 2007 Third International Workshop Internet and Network Economics vol 4858
[12] Frederik Armknecht,Ghassan Karame,Avikarsha Mandal,Franck Youssef and Erik Zenner 2015 Trust and Trustworthy Computing: 8th International Conference Ripple: Overview and Outlook pp 163–180
[13] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone 2019 arXiv preprint Cryptography and Security Blockchain Technology Overview
[14] Monika Agrawal and Pradeep Mishra 2012 International Journal on Computer Science and Engineering (IJCSE) A Comparative Survey on Symmetric Key Encryption Techniques
[15] Gurpreet Singh 2013 International Journal of Computer Applications A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security vol 67