The Role of Cryptography in the implementation of Cryptocurrencies

[1]M.Samuel John,[2]K.Parish Venkata Kumar,[3]M.Joshua

[1]Lecturer in Computer Science, Department of Computer Science, PVKN GovtCollege(A),Chittoor,AP
[2]Assistant Professor,Dept.of Computer Applications, VRSiddharthaEnggCollege,Vijayawada,AP
[3]QA Engineer, Ardent Technologies India PvtLtd,Hyderabad,TS

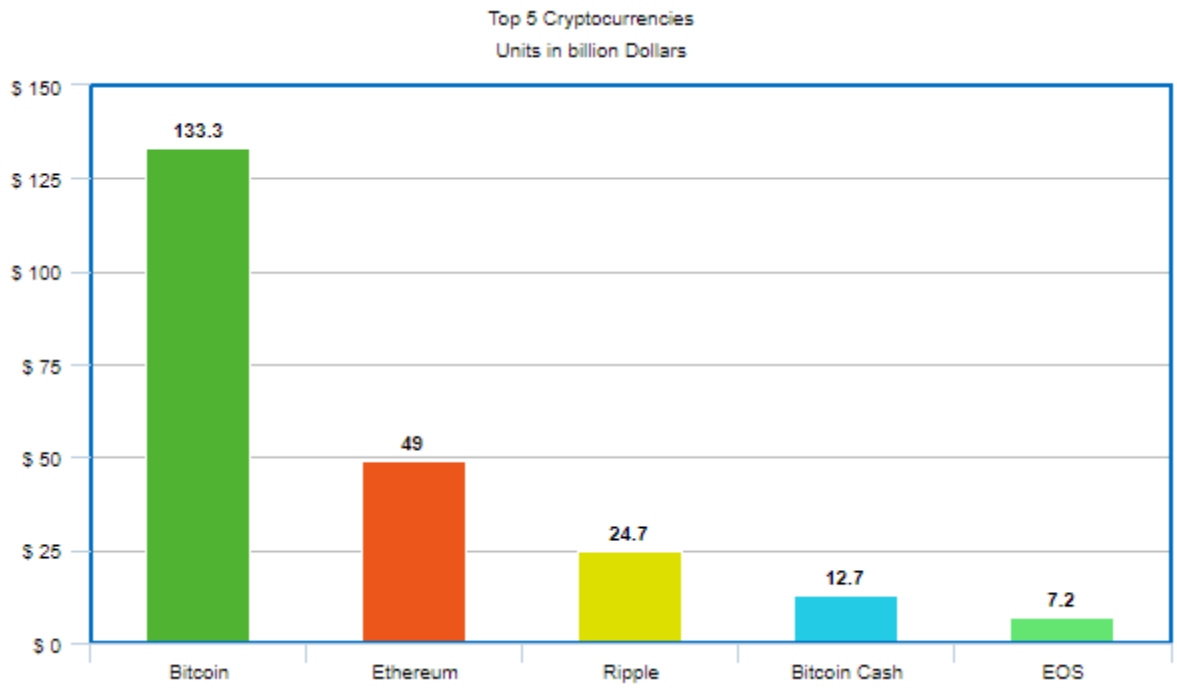
Abstract :Now a days, the increasing popularity of cryptocurrency for sending remittances is clearly seen through newspapers, public Internet and other electronic and printmedia. Day by day, more number of people is getting adapted to usecryptocurrencyfor remittance and eventually it became part of our lives.Cryptocurrency is an encrypted, peer-to-peer,virtual cash system for exchanging money.Cryptocurrency uses cryptography for three purposes:to secure the transactions, to verify the transactions and to control the creation of new units. This paper provides a comprehensive description on the role of public key cryptography incryptocurrencies.

***IndexTerms*–Cryptocurrency, cryptography, bitcoin, hash code, digital signatures, public-key cryptography.**

I. INTRODUCTION

Research shows that, cryptocurrencies like Bitcoin and Ethereum have gained huge fame in the recent times and more and more people are using them for remittances. In the recent years, both online and offline merchants are accepting cryptocurrency as a form of payment. All the transactions in this virtual cash system are made over the Internet. Unlike our traditional economic system where banks regulate the flow of currency, virtual cash system is a decentralized system[1], there is no central authority to process the transactions. It is anonymous system because users are identified by their virtual identity. Cryptocurrencies have no physical existence like fiat currencies or traditional currencies. Bitcoin is the most valued cryptocurrency[2] and Ethereum is the second most recognizable digital currency. The number of coins in circulation is increasing rapidly and now it is reaching 900[3]. The graph below shows the top 5 cryptocurrencies as of April 13,2018 [4].

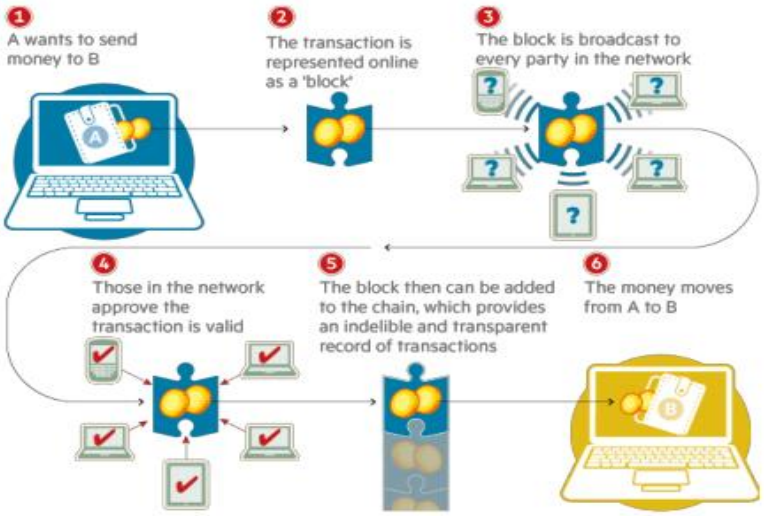
Figure 1: Top 5 cryptocurrency units in billion dollars.



II. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is used in virtual cash systems to ensure the security of the crypto economy. In public key cryptography, each user has 2 keys: A public key and a private key. Public key is known to everybody but the private key is known to the user only. The private key should not be shared with outsiders. Each of the keys is a long string of alphanumeric characters and generally stored in a digital wallet. Public key is used to verify the digital signature and also serves as an address on the network.Suppose that Alice wants to send 50 Bitcoins to Bob, she has to digitally sign this transaction using her private key. She can address the transaction to Bob's public key, which is Bob's address on the network. Later, the transaction will be collated into a "transaction block". This transaction has to be verified by the nodes within the network. Here, Alice's public key will be used to verify her signature. If Alice's signature is valid, the network will process the transaction, add the block to the chain and transfer 50 Bitcoins from Alice to Bob. The figure below shows the transfer of crypto currency from one person to other.

Figure 2: Working model of block chain technology.



III. DIGITAL SIGNATURE

Digital signature is a security mechanism which ensures the authenticity of a message. It is more powerful than hand written signature. In the digital cash system, every transaction is broadcasted to the network. Our private key is used to generate a digital signature for every digital transaction. The digital signature is a technique used to verify the authenticity of a message and the sender of a message.It provides authentication, non-repudiation, and integrity services. The sender takes the data, gets the hash code of the message, encrypts the hashcode by the private key toget the digital signature. The sender, after sending the data, cannot repudiate it because it is encrypted by the private key which the sender only knows. The digital signature creation process is shown in the following diagram.

The receiver takes the data and digital signature, decrypts the digital signature with the public key of the sender. Receiver also calculates the hash code of the received data. If the calculated hash code matches with the received hash code then the message is authenticated. Verification process is depicted in the figure below.

Figure 3: Implementing private key for digital signature in block chain technology.

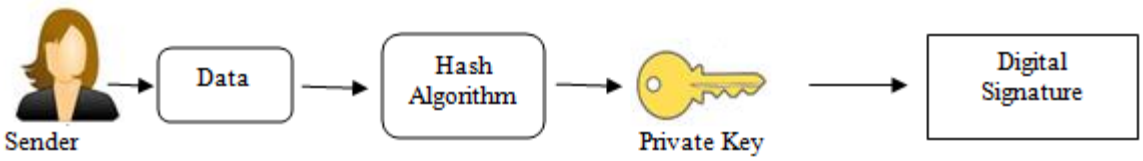
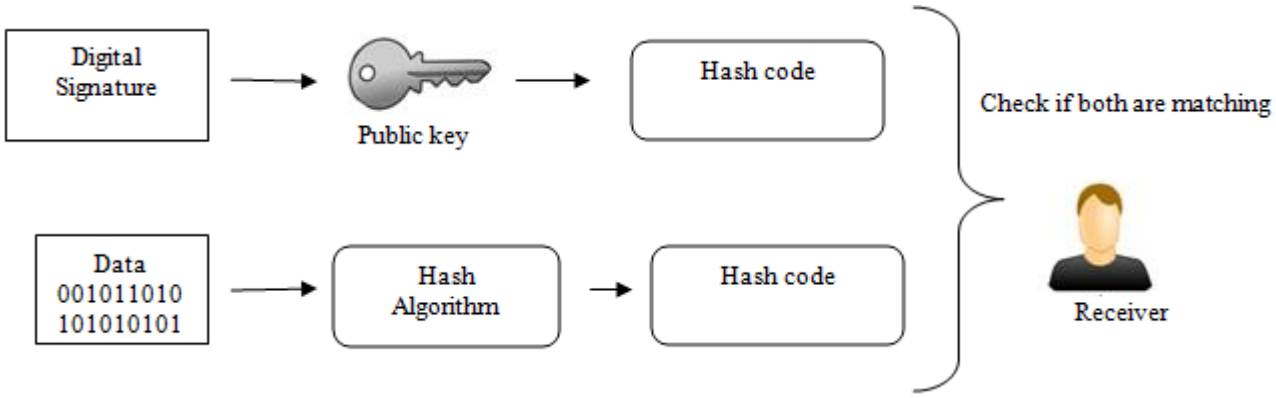


Figure 4: Encryption of data in block chain technology.



In the block chain technology, digital signatures are used to ensure that the transactions are made by the rightful persons.

IV. HASHING

Hash functions play a vital role in cryptography and information security. A hash function is a mathematical function that takes data of any size and produces a fixed size encrypted output(also called as Message Digest). Hash functions are generally used to store passwords. During the time of login registration, the hash of our password is stored in the database. When we try to login next time, our hash of our password is matched with the stored hash of our password. If both hashes match, then the user is said to be authenticated. Hash functions are used for digital signatures and authentication. The hash code for the same input always results in the same hash. If we change a single bit in the input data, it will fully change the hash output. Bitcoin and other major cryptocurrencies use SHA-256(Secure Hash Algorithm) hash algorithm. It is a popular hash algorithm that generates 256-bit hash code. Some other new cryptocurrencies use Scrypt over SHA-256. SHA-256 is complicated whereas Scrypt has fast transaction turnaround time.

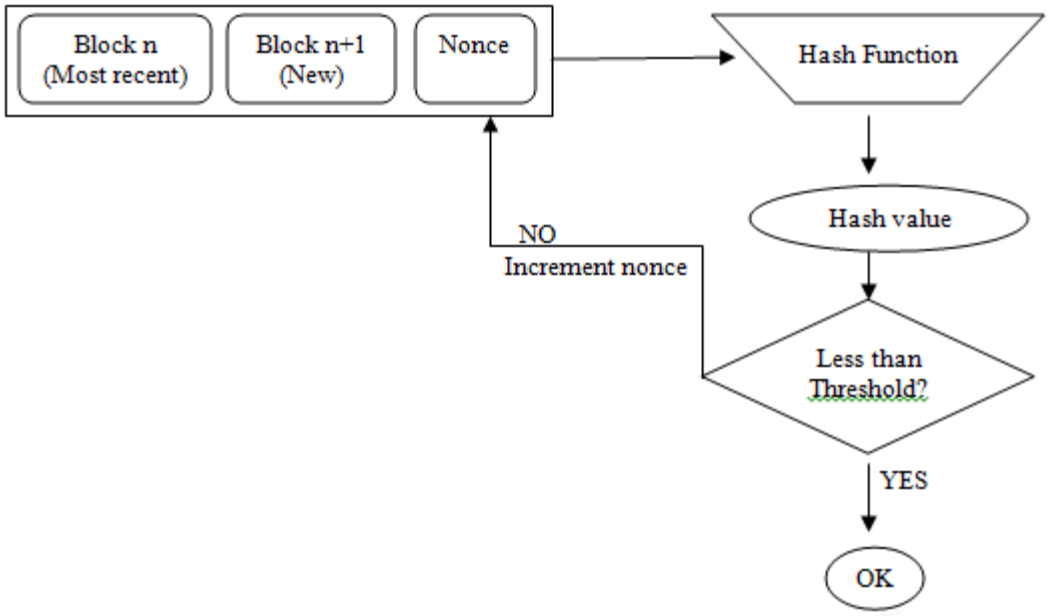
The table below shows some of the hash algorithms and the coins that use those algorithms.

Table 1. Coins that use the hash algorithm.

S.No.	Hash Algoritthm	Coins that use the hash algorithm
1	SHA-256	Bitcoin, Bitcoin Cash, Namecoin, Terracoin, Devcoin, Peercoin
2	Scrypt	Litecoin, Dogecoin, Novacoin, Latium, Worldcoin, Digitalcoin
3	Dagger Hashimoto-Ethash	Ethereum, Ethereum classic, UBIQ, Music coin
4	X11	Dash, Cannabis coin, Karmacoin, Xcurrency
5	Cryptonight	Monero, DigitalNote, DarkNetCoin, Electroneum
6	Equihash	Zcash, Hushcoin, Bitcoin Gold, Verge
7	Groestl	Myriad coin,DigiByte,Diamond coin
8	Lyra2REv2	Vertcoin, Monacoin, Shield
9	Blake	Honey, Tajcoin, Nevacoin, Blakestar
10	LBRY	LBRY Credits
11	NeoScrypt	Bollywood coin, Cerberus, Crowdcoin
12	Skunkhash	MUN Coin, Vapecoin

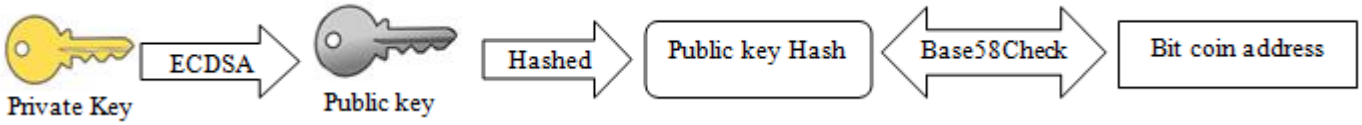
The figure below shows the role of hash functions in bitcoin's proof of work scheme.Block chain is the central mechanism for the bitcoin [5]. We cannot imagine block chain technology without hashing and digital signatures. Every block contains specific information such as, block number, data, cryptographic hash of previous block, cryptographic hash of the current block. Every block also contains another field called nonce. Nonce is a random number which is used for only one time. It is a 32-bit value used in a bitcoin network.

Figure 4: Implementing hash function for individual blocks.



Now, we see how cryptography is used in generating bitcoin addresses. After getting a public key/ private key pair, the public key is hashed and converted to a base58check format to generate the bitcoin address. Bitcoin uses a specific digital signature algorithm known as Elliptic Curve Digital Signature Algorithm (ECDSA) [6].

Figure 4: Representation of Curve Digital Signature Algorithm.



IV. CONCLUSIONS

Crypto currency is estimated to transform almost all industries in the next five years.Although some people treat crypto currency as a high-risk investment, still it is growing exponentially in a tremendous pace. Since no third party is involved in the transaction approval, these transactions are processed very fast and with low fees. In the recent past, some of the industries, colleges, and other organizations have been accepting cryptocurrencies as payments. The backbone for cryptocurrency is Cryptography and its algorithms. As new cryptographic algorithms are being developed to enhance the security, crypto currency implementationsare also subjected to change in the coming years.

REFERENCES

[1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". www.bitcoin.org. Retrieved from Bitcoin.org.
[2] http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.
[3] https://coinmarketcap.com/coins/views/all/ the number of Coins in circulation nears 900
[4] http://www.coinmarketcap.com, the top10 cryptocurrencies, market capitalization of major cryptocurrencies.
[5]Blockchain challenges and opportunities: a survey,ZibinZheng and ShaoanXie,Int. J. Web and Grid Services, Vol. 14, No. 4, 2018
[6] Bitcoin and Cryptocurrency Technologies: A Comprehensive IntroductionByArvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder