iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4682

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

A Review Paper on Regulating Bitcoin Currencies

Urshila Ravindran[1], Bipin Kumar Rai[2], Shivani Sharma[3]
[1]*Research Student,* [2,3] *Associate Professor Department of Information Technology ABES Institute of Technology Ghaziabad, Uttar Pradesh, India*

Abstract: Before the advent of Bitcoin, there was no mechanism to allow any two willing parties to make transactions between them without any involvement of a third party. Third parties were included in the process to prevent fraud. Hence, involving a third party meant extra charges for transaction which is a downside of the present online transaction system. Double-spending is an issue of digital currencies because digital tokens can be replicated easily and the transaction parties cannot verify the bona fides of the digital currency. Bitcoin has a procedure to prevent double-counting and check the authenticity of each transaction. Bitcoin cryptocurrency is based on the concept of cryptography, blockchain and peer-to-peer version of electronic cash. The Bitcoin network is growing significantly as there are no prerequisites required for making an account or investment in Bitcoin so it is basically a network open for all. Bitcoin is the first decentralized digital currency which is the reason for its popularity. This cryptocurrency opens up a whole new platform for financial transactions.

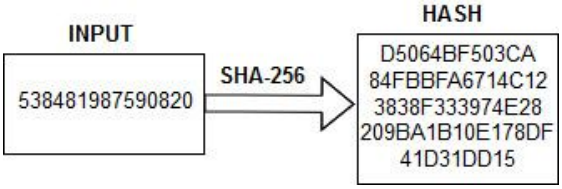
Keywords: Bitcoin, Cryptocurrency, Blockchain, Cryptography, Digital currency, Peer-to-Peer (P2P), Anonymity, Timestamp server, Distributed ledger, ECDSA

I. INTRODUCTION

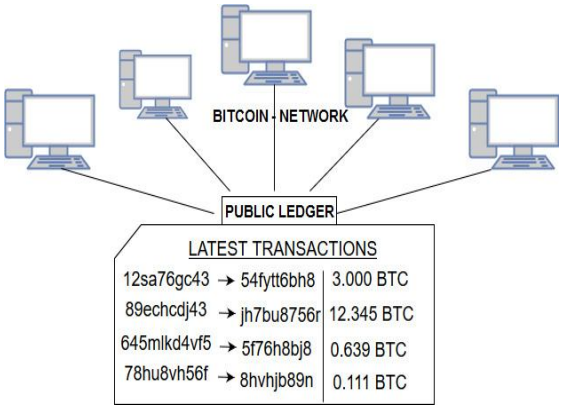
Bitcoin is an open source peer-to-peer virtual transaction system which is partially anonymous and an unregulated digital currency. By unregulated, we mean that it is not governed under any central authority. The idea behind this crypto currency was proposed by a pseudonymous person, Satoshi Nakamoto in 2008. Bitcoin was actually developed by an open source community. It is basically a private currency which is provided by a private enterprise for the sole purpose of combatting government's exclusive control on the supply and transfer of money. Unlike traditional currencies which are prone to a number of factors like recession, inflation, government policies/laws and political corruption, bitcoins are more stable. Bitcoin's value is not determined by law. Their value is directly proportional to supply and demand. Bitcoin emerged as a solution to the double-spending problem which can be possible while using digital cash scheme. It is a potential flaw in which a single digital token can be spent more than once. This digital token consists of a digital file that can be duplicated or falsified. Bitcoin transactions are irreversible. There is a peer-to-peer distributed timestamp server which records the order of transactions in a chronological way For example, if Bob wanted to send ₹100 to Alice via the Internet, he would have had to rely on a third-party service like Paytm. Intermediary parties keep a log of account holder's balances. In the above transaction, Paytm deducts the amount ₹100 from Bob's account and adds it to Alice's account. Digital money could be spent twice, without such intermediaries. Imagine that, there are no intermediaries with ledgers. In this case, digital cash is simply a computer file. Transaction of sending ₹100 between Bob and Alice is possible by attaching a money file to a message. But as in the case of email, sending an attachment to someone does not remove it from the sender's computer. The copy of the money file would be retained with Bob after she had sent it to Alice. Bob then could easily send the same ₹100 to anyone other she wants. This is the "double-spending" problem. It could only be solved by employing a ledger-keeping trusted third party until Bitcoin came into emergence. Bitcoin solves this issue by distributing the ledger among all the users of the system via a peer-to-peer network.

A. *How bitcoins work?*

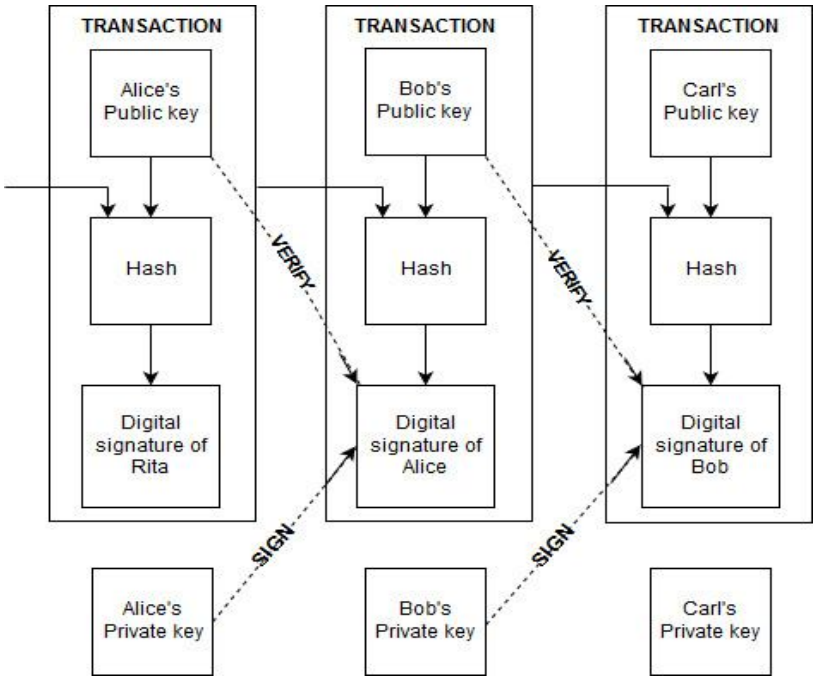
1) *Transactions:* A Bitcoin transaction does not involve the participation of any financial institution or government authority rather users perform all the steps of transaction by themselves. The transactions are encrypted with the implementation of SHA-256 hashing**.**



The encrypted transaction is then recorded in the public ledger running on thousands of computers who are a part of the decentralized network.



Electronic coin is defined as a sequence of digital signatures. Digital signatures are basically digital tokens. Each individual transfers the coin to the next individual by digitally signing a hash of the previous transaction and the public key of the succeeding individual and adding these to the end of the coin. The recipient can verify the signatures to validate the chain of ownership by this process.



The earliest transaction is the one that counts, so we do not consider the later attempts to double-spend. The only way to know if we didn't miss out any transactions is to be aware of all transactions occurring. Transactions are publicly declared in a ledger which is a mechanism for participants to agree on the chronological order of transactions. The recipient needs proof that at the time of each transaction, the majority of nodes agree that it was the first received.

B. Cryptographic Concept

A "cryptographic proof' system forms the basis of the Bitcoin, which allows an individual to make a transaction directly with another party without needing a third party to authorize the transaction. There are certain cryptographic concepts that should be known to get an insight into the Bitcoin concept. Cryptography is the phenomenon of keeping messages confidential and secure by providing authentication, integrity and non-repudiation of messages. Cryptography maintains the following objectives:

C. Authentication

The receiver of a message should be able to verify the source of its data. There should be a mechanism which can authenticate the sender of data i.e., using a public key.

D. Integrity

The sanctity of data is known as integrity of a data. It should be possible for the receiver of a message to verify that it has not been tampered during its transfer; an intruder should not be able to replace a legitimate one by a false message. Tampering can be both intentional and unintentional. Unintentional tampering takes place when the message packets may catch random bit errors or noise during their transit from one node to another.

E. Non-repudiation-

A sender should not be able to claim that the message was not sent by him but an imposter. It means that the message sender cannot deny the authenticity of the message.

F. Confidentiality

It refers to limiting the access of a piece of information to a set of individuals which is achieved by encrypting the information and sharing the secret key with the group. Now we describe some of the ways in which Cryptography plays an important role in Bitcoin: If two individual parties want to send messages in a confidential way, they may use the encryption technique to hide their actual message (plaintext) using encryption algorithm and encryption key. The encryption process in turn, transforms the original message to ciphertext in order to make them indecipherable by an intruder or anyone else. This encrypted message will be impenetrable and can be viewed only under the condition that you have the decryption key to convert it into the original message. Decryption is the inverse of encryption that performs the unscrambling of the encrypted text and getting the original form. Nowadays, in most scenarios, only the encryption/decryption keys are kept secret whereas the encryption and decryption algorithms are known or can be known. The two encryption algorithms commonly used in today's world are symmetric and asymmetric encryption algorithms. Symmetric encryption algorithm is where both the parties use the same key for encryption and decryption and asymmetric if both the parties use different keys. Symmetric-key encryption works well for encrypting data on your computer/server rather it is not such an efficient way for communication as it uses the same key for both encryption as well as decryption process. The downside of this algorithm is that individuals that wish to communicate with each other need some way to agree on a key and that preferably has to be face to face because you know that the whole reason you are encrypting your communications to begin with, is that you think your communication channel is insecure. You just cannot just send an encryption key in an email or text message or phone call since it can be intercepted intentionally or unintentionally by anyone else. All in all, it can be difficult for two individual parties to securely share the common key. being transferred by their actual owners. ECDSA has separate approach for digital signing and verification. The signing algorithm involves the use of the private key and the verification process consists of the public key. The private key is an unpredictably or randomly chosen number between 1 and the order. The public key is obtained from the private key by scalar multiplication of the base point to the value of the private key expressed as follows in the form of an equation:

Public key = Private key * Base point

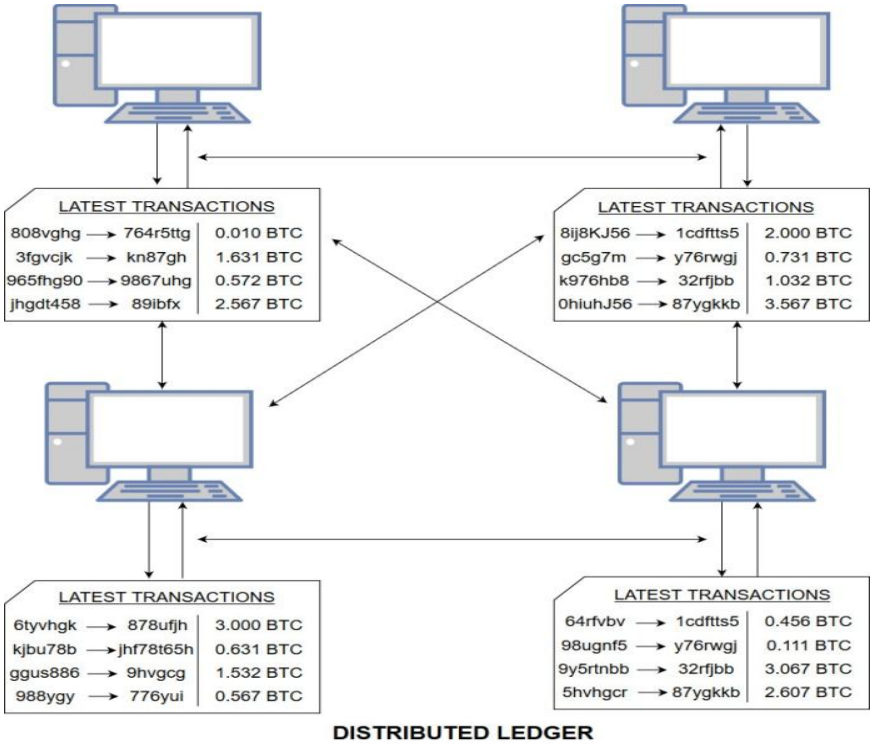
This represents the maximum possible number of private keys is equal to the order. ECDSA uses an elliptic curve and a finite field to digitally sign the transaction data in a way that third parties can verify the authenticity of the signature while the signer retains the sole ability to create the signature.

1) *Public-key cryptography:* introduces the combination of encryption, decryption and digital signatures. In this cryptographic technique, creation of a key pair of two different keys: the public key and the private key to encrypt and decrypt messages. Bitcoin uses the public key cryptography as it is considered far better than symmetric key cryptography when communication/transactions are concerned. Each Bitcoin transaction uses public-key encryption to ensure the parties involved in transaction with privacy. This encryption process generates two mathematically linked keys. One key is retained by the payee-somewhat like a private key such as a password or pin. A private key is a randomly generated, single unsigned 256 bit integer (32 bytes) which is used to access the Bitcoins kept in the payer's account. The other key is made public-like the name of a bank or an account location where the funds reside, which is also known as public key of the payee. The payee uses the public key to locate the payer's account. The payer's account can only be accessed and money can only be extracted by the other person if he has the associated private key. The payer then uses their own private key to authorize and enable the

extraction of Bitcoins from their account. All transactions associated with a public key are then broadcast to the entire Bitcoin community and stored in a transparent public ledger. Since the public key encryption is so complex, faking a Bitcoin transaction would require more processing power and is computationally hard than the entire Bitcoin network combined. Public encryption, hence, effectively ensures that Bitcoin transactions are secure.

G. Distributed Ledger

Distributed ledgers provide a constantly updating, shared and transparent record of any transaction taking place in their respective sequence. The transfer of ownerships of Bitcoins is also recorded in a distributed ledger. This phenomenon simplifies the business activities which are inherently complex. Using mutual distributed ledgers will play a significant role in achieving a reduction in office costs and market risks. Ledger is managed by a group of peers rather than leaving it to a central authority who share the responsibility for maintaining the ledger. Identity and integrity of the ledger ensured via establishing consensus among the peers who share maintenance of the ledger.



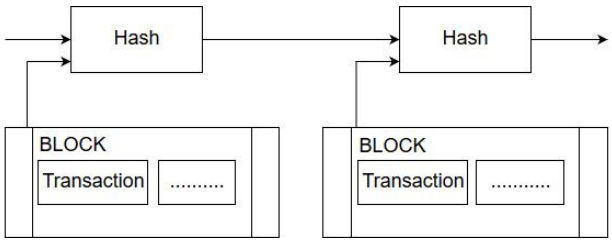
DISTRIBUTED LEDGER

Ledgers play an important role in determining the value of Bitcoins. The decentralized crypto currency was able to create a boom all over the world due to the faith the Bitcoin users have on the ledger supporting Bitcoin that it will maintain an accurate record of the operations and ownership. Anyone can obtain a copy of the ledger for reviewing it as all the ledgers are equal but ensuring the integrity of the ledger can be more typical. There are various reasons which behold the trust that the customers have on Bitcoin. Firstly, we can easily convert between Bitcoin and other currencies or value inherent in goods and services due to their correct measure of value. Secondly, the demand for Bitcoins is not going to die soon and hence, becoming a relevant factor for using them as a means to exchange value when needed. Lastly, the value of this currency remains stable and allows us to use it as a store of value.

H. Timestamp Server

Bitcoin uses a "peer-to-peer distributed timestamp server" concept to verify that the digital coins have not been double spent. Bitcoin performs decentralized time stamping on the block chain in a tamper proof manner.

A timestamp records the exact time that a Bitcoin is created or sent from one user to another which serves as a secure proof of the exact time at which that data existed.. A timestamp server works by taking a hash of a block of items or transactions to be time stamped and widely broadcasting the hash.



TIMESTAMP SERVER

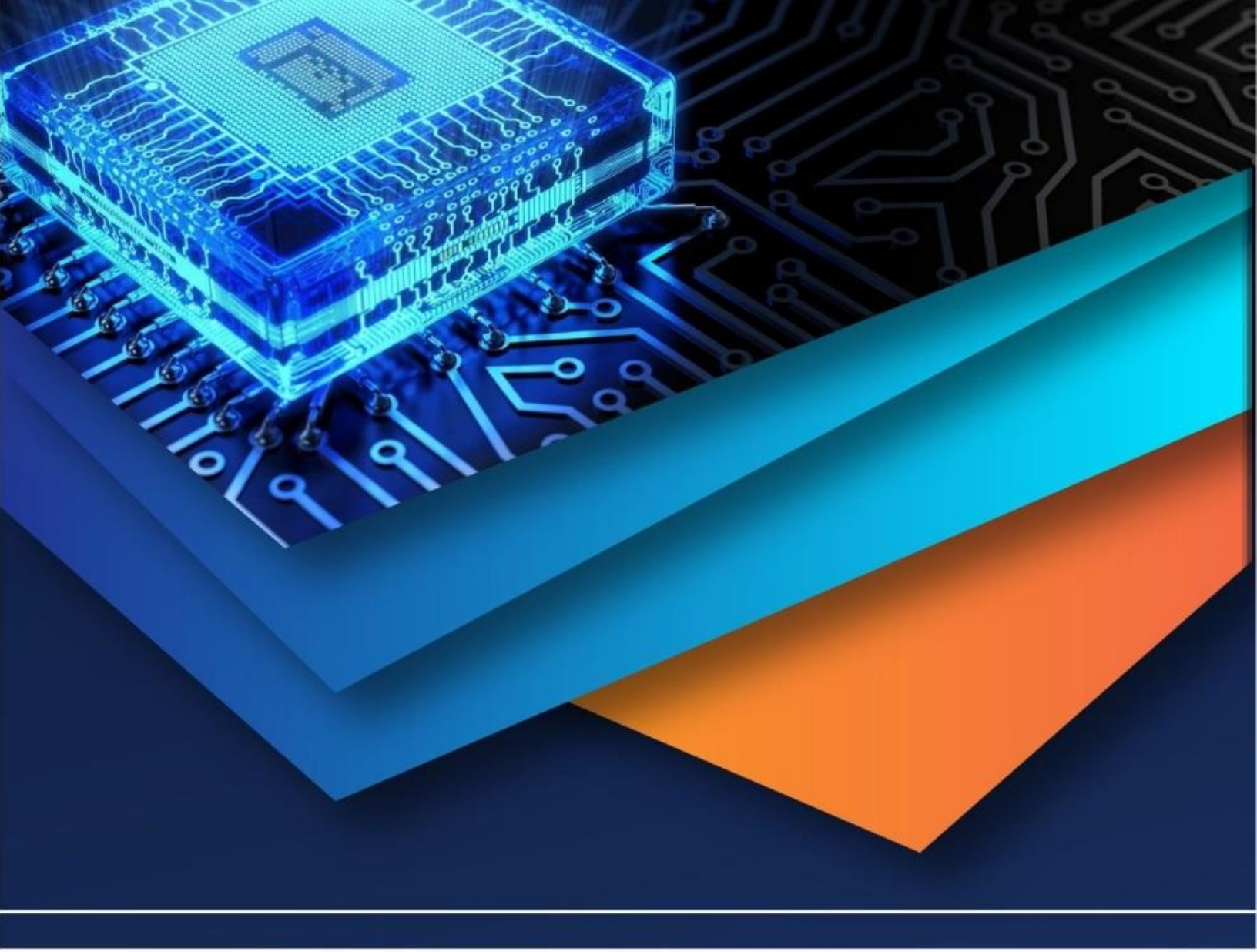
Every 10 minutes, a list of all Bitcoin transactions and their timestamps is recorded into a "block." These blocks are then aggregated into the "block chain" which acts as a master list that stitches together each 10 minute snapshot of the entire Bitcoin network. In other words, you can say each timestamp includes the preceding timestamp in its hash, forming a chain like structure, with each additional timestamp holding up the ones before it. The timestamp, hence, proves that the data must have existed at the time in order to get into the hash. The digital currency would devalue to 0 if tampering is done with the timestamp resulting in non-integrity of this currency. The year 2038 problem is delayed for another 68 years as this crypto currency uses an unsigned integer for the timestamp.

II. CONCLUSION

With the emergence of Bitcoin technology, we got the solution to the flaws in the existing digital transaction system. Use of cryptography enhances secure transactions by verifying them with the same state-of-the-art encryption technique used in military and defence softwares to maintain anonymity. Blockchain enables P2P (peer to peer) value transactions without a mediator and also helps in maintaining a public ledger to store all the transactions taking place all around the world resulting in elimination of the involvement of any intermediary party. Moreover, it consists of a transparent public ledger which records all the transactions after verification and the sequence in which they occur. In the past years after the arrival of Bitcoin, its use has been limited as a medium of exchange, excluding the illegal activities. An increase in Bitcoin investers has positively been associated with an increase in the Bitcoin exchange volume. It has been used as a way to make transactions outside of traditional and regulated channels and, presumably, as a conjectural investment opportunity. People invest on Bitcoin because they believe that someday it may develop into a full-fledged currency in the world. Bitcoin has been widely accepted all over the world and it remains free from government intervention. In the future consequences, it is possible that it will represent a phenomenal conceptually and technical achievement, which may well be used by governments or even existing financial institutions which could issue their own Bitcoins.

REFERENCES

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”,200
[2] Nicholas A. Plassaras, “Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF
[3] Malte Möser, “Anonymity of Bitcoin Transactions
[4] François R. Velde ,“Bitcoin: A primer”,201
[5] Glaser, Florian, Zimmermann, Kai, Haferkorn, Martin, Weber, Moritz Christian, Siering, Michael, ”Bitcoin– Asset or Currency? Revealing User’s Hidden Intention
[6] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
[7] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999
[8] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993
[9] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980
[10] Andy Yee, Internet architecture and the layers principle: a conceptual framework for regulating Bitcoin, Aug 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY