Asia Pacific Journal of Information Systems
Vol. 30 No. 1 (March 2020), 21-30

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2020.30.1.21

Bitcoin Cryptocurrency: Its Cryptographic Weaknesses and Remedies

Anindya Kumar Biswas[a,*], Mou Dasgupta[b]

[a] *Ph.D. Scholar, Department of Computer Application, NIT Raipur, India*
[b] *Assistant Professor, Department of Computer Application, NIT Raipur, India*

ABSTRACT

Bitcoin (BTC) is a type of cryptocurrency that supports transaction/payment of virtual money between BTC users without the presence of a central authority or any third party like bank. It uses some cryptographic techniques namely public- and private-keys, digital signature and cryptographic-hash functions, and they are used for making secure transactions and maintaining distributed public ledger called blockchain. In BTC system, each transaction signed by sender is broadcasted over the P2P (Peer-to-Peer) Bitcoin network and a set of such transactions collected over a period is hashed together with the previous block/other values to form a block known as candidate block, where the first block known as genesis-block was created independently. Before a candidate block to be the part of existing blockchain (chaining of blocks), a computation-intensive hard problem needs to be solved. A number of miners try to solve it and a winner earns some BTCs as inspiration. The miners have high computing and hardware resources, and they play key roles in BTC for blockchain formation. This paper mainly analyses the underlying cryptographic techniques, identifies some weaknesses and proposes their enhancements. For these, two modifications of BTC are suggested — (i) All BTC users must use digital certificates for their authentication and (ii) Winning miner must give signature on the compressed data of a block for authentication of public blocks/blockchain.

Keywords: Bitcoin, Cryptocurrency, Cryptographic Hash Function, Digital Signature, Private- and Public-key

Ⅰ. Introduction

Bitcoin was first introduced by Satoshi Nakamoto as a pseudonym in 2008 and started functioning in January, 2019 (Nakamoto, 2008). It is an independent online currency system, where both the cash and payment transaction are allowed. However, unlike traditional payment systems that made transactions through trusted third parties, Bitcoin is a complex virtual currency system enabling transfer of money between two or more parties directly. It has unique features than other similar systems as the users in

*Corresponding Author. E-mail: anindya.kr.bws@gmail.com

BTC are anonymous and every transaction is recorded after verification through a P2P public network (Meiklejohn et al., 2013). For these, it uses some cryptographic techniques for securing ownerships of money and creating/maintaining ledger book as chaining of blocks available to all. However, there are some confusions about BTC for its decentralization, anonymous payments, irrevocability etc. and thus, it is suspected that the money laundering criminals would be attracted in BTC for racketing, scamming, cheating etc., and some cases are already reported (European Central Bank, 2012).

This paper cryptanalyzes the crypto-techniques used in BTC system and observes that the users' anonymities, which do not make associations to real-world individuals, is one of the main reasons for criminals' attraction. Since BTC makes transactions using public keys of users and validates the same again using public P2P network comprising unidentified people, no full-proof secure cryptosystem is possible without any secret and/or users' authentication. Although BTC uses digital signature, exhaustively computable hard problem and P2P network ledger book/protocol as cryptographic protection, all are publicly related activities using public parameters and thus, the system remains insecure. With these views, we propose a modification of BTC in this paper that if the users' anonymities are removed, the weaknesses of BTC would be avoided and it becomes a real-life currency system, where the users with their money/property, transaction identities etc. can be known. For this, we propose the inclusion of digital certificates, which link certificate owners with public keys, to BTC transaction and blockchain. The digital certificate system is already available online on Internet through PKI (Public Key Infrastructure) and it is easily accessible to users (Stallings, 2003).

The virtual BTC cryptocurrency is very popular and many people are interested for the system for its easy money transfer, transaction, payment, ledger maintenance etc. However, our study/observation shows that Bitcoin lacks two significant aspects—(i) Full virtuality and users' anonymities may cause numerous attacks as BTC users are not authenticated and (ii) The proof-of-work of a block/blockchain is though computationally intensive, it is not cryptographically hard (for a hard problem, no polynomial-time algorithm exists) and thus, the block and/or blockchain tampering attack may occur as valid block(s) may be generated using alternative nonces. So, our main motivations in this paper are to remove these weaknesses by avoiding users' anonymities using their digital certificates and providing the winning miner's signature to a block before joining to the public blockchain ledger. The proposed enhancements are significant as they would make BTC well-secured with a slight overhead required for maintaining digital certificates and computing/verifying digital signatures.

The paper is organized as follows. In section 2, a literature review and the Bitcoin cryptocurrency basics with cryptanalysis of its transaction and block/blockchain formation are given. Section 3 gives the proposed enhancements of the BTC cryptocurrency. Finally, the paper is concluded in section 4.

Ⅱ. Literature Review and BTC Cryptocurrency

A literature review on different cryptocurrency techniques with their salient features is provided in this section. In addition, the basics of BTC cryptocurrency especially on BTC transaction and block-

chain formation, and their cryptanalysis are included.

2.1. Literature Review

As mentioned earlier, Satoshi Nakamoto first introduced BTC cryptocurrency with distributed public blockchain ledger over P2P networks, where each BTC transaction in a block signed by a sender is verifiable by users in the network (Nakamoto, 2008). It is so popular and developing digital currency that the number of users after two years from initiation in 2009 became nearly *60,000* (Bitcoin, Wikipedia). An analysis and protection against double-spending attack for fast payment in Bitcoin are given in (Karame and Androulaki, 2012), where the attack means to double spending of the same BTC to different users. Authors have developed an attack model, necessary conditions for successful double-spending attack and propose for preventing the same in BTC. However, it is mentioned in (Nakamoto, 2008) that if the fraction of honest peers exceeds dishonest ones in the network, this attack can be disregarded.

As a cryptographic hash function called SHA-256 is used in BTC for computing a fixed-length message digest of arbitrary-length blocks (Stallings, 2003), a document provides the security guidelines for achieving required security strength to avoid relevant vulnerabilities from different hash functions (Dang, 2012). A work on economics of Bitcoin mining in presence of adversaries is presented in (Kroll et al., 2013), where it is mentioned that though the system is protected by proof-of-work, a motivated adversary might be successful to disrupt and crash the BTC currency system. In another work (Badev and Chen, 2014), it is mentioned that BTC is a complex currency system as its implementation includes cryptography, public blockchain ledger, incentive driven mining for computation of blocks/blockchain etc. On empirical analysis based on publicly available data, it is stated that less than *50%* of all BTC are used in transaction, about half of these is less than *$100* equivalent (small-value transactions were involved for online gambling service), and though a few large-value transactions above *$40,000* equivalent were made, however, they were not used for payment of goods/services.

On an issue of Bitcoin as a money-like informational commodity (Bergstra and Weijland, 2014), authors discuss about moneyness— a certain system represents a money & instead of binary values with yes/no, it is a matter of degree, and money-likeness— it's a functionality resembles that of money. They also criticize cryptocurrency— (i) It must be a currency and a certain level of acceptance/usage must be confirmed, however, Bitcoin did not receive such acceptance, (ii) Bitcoin system and its variations (alternative designs) should be given of same type, however, Bitcoin is not of that type. In (Lo and Wang, 2014), it is mentioned that Bitcoin, which is an alternative to existing currency systems, enables transactions across nations and currency denominations without interfering central entities. However, authors put question on the success of Bitcoin P2P network (types of intermediaries for functioning, and rationales for growth) for fulfilling the functions as a fiat money system.

In (Garay and Kiayias, 2015), authors study the core of Bitcoin currency system as Bitcoin-backbone and propose/analyse applications that can be built on the top of it. They identified and proved two fundamental properties of BTC— *Common prefix* and *Chain quality* as byzantine agreement and public transaction ledger, respectively. As BTC system has timed commitments, some secure multiparty computations are developed over BTC (Garay and Kiayias, 2015), for instance, secure multiparty lotteries using

Bitcoin currency (Andrychowicz et al., 2016). These protocols have practical significance as the online gambling sites can be replaced by them.

2.2. Bitcoin Cryptocurrency Basics

Bitcoin is a decentralized currency system developed using some cryptographic techniques and a P2P public network consists of BTC users and some key players called miners. The users are identified by ECC (Elliptic Curve Cryptography) based public keys, and a transaction is signed by sender's secret key using ECDSA (Elliptic Curve Digital Signature Algorithm) (Johnson et al., 2001). A cryptographic hash function known as SHA-256 (Secure Hash Algorithm-256) is used for calculation of message digest. A set of transactions per an interval (10 minutes) form a block and a block with the solution of the BTC's underlying hard problem and the hash of its previous block creates chaining of blocks known as Blockchain used as a public ledger book of the BTC. The details of BTC's transactions and the Blockchain are addressed now.

2.2.1. BTC Transaction

A Bitcoin transaction comprises sender's address-set, different receivers' address-set and the amount of BTCs to be transferred, where each address-set consisted of several public keys form a wallet and all the public keys in the sender's address-set belong to a sender. However, the number of receivers in a transaction is two or more and accordingly, the receivers' wallets are formed. For integrity and validity, each transaction is digitally signed and broadcasted by sender over P2P Bitcoin network for other users' validation, and the same is accepted if the signature verification is satisfied. For instance, if a user with public-key *PU-A* sends *C* BTCs to a user with public-key *PU-B*, then the transaction becomes

$$TX \parallel SIG_{PR\text{-}A}(TX)$$

where, $TX = wallet_{PU\text{-}A}$ sends C BTCs to $wallet_{PU\text{-}B}$ and $SIG_A(TX)$ is the ECDSA digital signature signed on message TX by sender. For the sake clarity, ECDSA is briefly described below.

ECDSA Parameters

$E(F_q)$: Set of EC points with finite field F_q
Q : A base point such that $n \times Q = 0$ (zero at infinity) and n is large
$1 \leq x \leq n$: x is a sender's secret key
P : P is a user's public key, where $P = x \times Q \pmod{n}$

ECDSA Signature Generation

1. Select a random number $1 \leq k \leq n\text{-}1$ and compute $k \times Q = R\ (x_1, y_1)$ (note that for each signature generation, a new value for k is required).
2. Compute $r = x_1 \pmod{n}$, if r = 0, go to *1*.
3. For message m, compute $e = SHA\text{-}256\ (m)$, where e is an integer.
4. Compute $s = k^{-1}(e + x \times r) \pmod{n}$, where k^{-1} is multiplicative inverse of k mod n. If $s = 0$, go to *1*.
5. Signature $(m) = (r, s)$

Signature Verification

If $P \neq 0$, P is on the curve and $n \times P \neq 0$

1. Compute $e = SHA\text{-}256(m)$, $w = s^{-1} \pmod{n}$, $u_1 = e \times w \pmod{n}$ and $u_2 = r \times w \pmod{n}$

2. Compute $u_1 \times Q + u_2 \times P \Rightarrow (ew + rxw) \times Q \Rightarrow (e + xr) \times s^{-1} \times Q \Rightarrow (e + xr) \times (e + xr)^{-1} \times (k^{-1})^{-1} \times Q \Rightarrow k \times Q = R(x_1, y_1)$
3. For calculated x_1, if $x_1 \pmod n = r$, the signature is verified, otherwise rejected.

2.2.1.1. Cryptanalysis of BTC Transaction

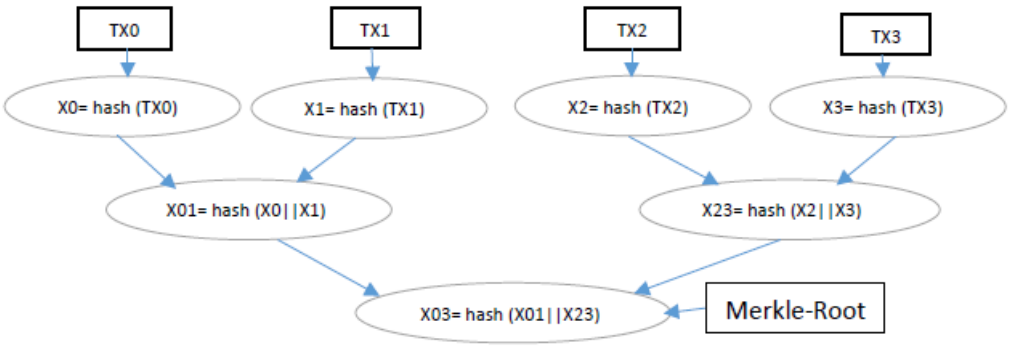
The Bitcoin transaction with sender's signature is secure as (i) It is authenticated, because it cannot be forged as the sender's private-key is unknown to opponents, (ii) It maintains integrity, because the transaction cannot be changed without changing the signature and (iii) It supports nonrepudiation, because the sender cannot deny after issuing a transaction. However, the transaction has the following security weaknesses:

1) Since the public keys forms the sender's wallets, the owner of a transaction remains anonymous. Although the signature verification assures transaction sum, it remains silent about the total owner's capacity amount and as a result, the validity of the transaction cannot be checked, i.e., whether the owner belongs required amount of BTCs mentioned in transaction or not. For a true currency system, a real-world identification for each user is necessary.
2) Since one signature per transaction is required, the sender would use one private key for signing the transaction. Since there is no public- and private-key pair information to the P2P network users, the identification of the corresponding public key for signature verification (by others) would be difficult.
3) If a private-key is compromised, then the corresponding public-key is cryptographically useless and as a result, it would loss the wallet partly from the Bitcoin currency system.
4) Due to anonymity, the users in Bitcoin cryptocurrency are not authenticated, which may create several cryptographic vulnerabilities in the system.

2.2.2. Bitcoin Blockchain as Distributed Public Ledger

The blockchain is the BTC ledger book formed by implicit chaining of blocks, where each block contains a set of verified transactions made during an interval of *10* minutes as this time is supposed to be required to generate a block. The blockchain is publicly available in distributed manner and accessible by all, however, none of the blocks constructed based on a computationally hard problem can be tampered. The transactions broadcasted in an interval are collected and grouped by miners into a candidate block after verification of the digital signatures. The miners then contest to solve the hard problem known as *proof-of-work* and after solution, the block is recorded to the blockchain. The winning miner, who first solves the problem, is also recorded and incentivized for the coin generation in BTC system. Initially, the incentive rate was *50* BTC per block until November, 2012 with blockchain size of *2, 10, 000* blocks, then, it was reduced to half, that is, to *25* BTC per block until 2016, and presently, its rate is 12.5 BTC/block. That is, the block incentive rate is reduced to half in every four years and it gradually reduces to zero when targeted BTCs of *21,000,000* are created in 2140. The formation of block and its hard problem are briefly described below.

Let TX_{set} represents the transaction-set during an interval, the candidate block is formed as



<Figure 1> Merkle Hash Tree

candidate-block = (*hash*(last-block of blockchain) || *Merkle-Root*(TX_{set}) || Time-Stamp)

where *Merkle-Root*(TX_{set}) is the merkle-root computed by applying Merkle-hash function on the transaction-set as shown in <Figure 1>, above (Merkle, 1988), where four transactions are used.

Now, a number of miners compute the following by adjusting a parameter *nonce*

hash(candidate-block || nonce) = *X* (hash of new block)

such that *X* becomes lesser than a pre-specified threshold. This is known as the hard problem of the BTC specified as the *proof-of-work*, that is, the hash values of all the blocks of blockchain are lesser than the threshold and they are self-certified. The hash function used here is a cryptographic hash function known as *SHA-256* (Stallings, 2003), which produces a *256*-bit or 64 hexadecimal digits output, and the threshold is set such that some of the first hexadecimal digits are zero. It is known as the *difficulty* (number of zeros) in BTC system. For instance, if the *difficulty* = *6*, then, first six hexadecimal digits of the hashed output are zeros and it is taken as threshold value of BTC, and all the computed hash values for the blocks must be lesser than it. Note that the complexity of getting a solution of the hard problem increases with the proportional to $16^{difficulty\ (=6)}$(or 2^{24}).

2.2.2.1. Cryptanalysis of BTC's Blockchain

The blockchain with the proof-of-work appears to be fine, however, it suffers from some cryptographic weaknesses as mentioned below:

1) First of all, the problem in BTC is tractable, i.e., the problem has straight forward algorithm. However, for security protection, each public-key cryptosystem contains an intractable hard problem for which no algorithm exists though it accompanied with a trap-door for solution. For instance, RSA's underlying hard problem is the prime factorization of a large composite (Stallings, 2003). Thus, the miners, who have high computing resources and electric power, can solve the problem easily. Also BTC currency system would be insecure as the blockchain is publicly accessible and the attackers, who are generally assumed to be more re-

sourceful/powerful than the miners (even cryptographers), can generate fake blockchain.

2) Secondly, it is found that the miners in BTC network solve the task by incrementing the *nonce* and validating hash-output with the threshold iteratively, and if so, the miner who have highest computing power and resources will always win the contest and get most of the BTCs for recording the blocks in blockchain. Thus, BTC system would suffer from this unfairness situation.
3) Finally, a secure cryptosystem generally is developed based on one or more secure keys/values like IPSec (Internet Protocol Security), SSL (Secure Socket Layer), etc., however, no such secure value has been used in blockchain formation and thus, the public blockchain ledger is insecure practically.

As an alternative of the proof-of-work used in BTC, a scheme known as Hashcash that computes a token, can be used (Back, 2002).

Ⅲ. Proposed Enhancement of BTC Cryptocurrency

As shown, both the BTC transactions and blockchain have some weaknesses, and this section proposes some enhancements for them. As we know, BTC is a unique cryptocurrency and it is a hope for the future payment system, because it is totally different from the so-called different card-based systems fully deployed using the existing banking process. Since the transactions and blockchain are the heart of BTC, the security protections for them are necessary and some of the enhancements in these regards, are provided.

3.1. Enhancement of BTC Transaction

The main weakness of BTC transaction is due to having the anonymities of users. Although this feature for a payment system is expected, a true currency system with everything on computer-generated parameters seem to be impractical, i.e., some sorts of real-world linking are required. For instance, when a sender makes a transaction with public keys as the identities of sender-receiver, it does not make complete sense without the real-world identities of entities involved. The main point is that the transaction amount in each BTC needs to be verified and it is not possible as the balance status of a user due to his/her anonymity, remains unknown. So, we propose for inclusion of users' identities in BTC for their authentication, although user-anonymity would be removed, a real-life currency system would be resulted. For this, a digital certificate that has ITU-T *X.509* (International Telecommunication

<Table 1> Format of Digital Certificate (X.509)

	Version
	Certificate serial number
Signature algorithm identifier	Algorithms
	Parameters
	Issuer name
Period of validity	Not before
	Not after
	Subject name
Subject's public-key information	Algorithms
	Parameters
	Public Keys
	Issuer unique identifier
	Subject unique identifier
	Extensions (Optional)
Issuer's Signature	Algorithms
	Parameters

Union-Telecommunication) standard/certification, would be used in each BTC transaction. The format of the certificate for clarity is given in <Table 1>, below (Stallings, 2003):

As shown, the certificate cannot be tampered as issuer's signature is provided, and the subject and his/her public-key are uniquely identifiable and thus, the certificate owner is authenticated. The certificate is issued by a certificate authority (CA) and maintained online through PKI (Public Key Infrastructure). Any user can request for issuing a certificate and for validation, PKI maintains a directory and supports for solution of any dispute of the certificate. PKI also maintains a certificate revocation list of users time to time so that the users are always kept updated with their digital certificate.

Thus, a BTC transaction, according to our enhancement, must be signed and attended at least with the sender's digital certificate corresponding to the private-key used for the signature generation. Thus, a digital certificate, which guarantees the ownership of public-key, may be used in Bitcoin networks. The modified transaction is shown below:

$$TX \parallel SIG_A(TX) \parallel CERT_A$$

where $CERT_A$ is the digital certificate corresponding to the public key *A*. Note that all the weaknesses mentioned in *section 2.1.1* would be removed.

3.2. Enhancement of BTC Blockchain

Note that there is a fallacy for the parameter *nonce* in the BTC, in one way it produces hard task for the security of the public blockchain ledger and in other way, it also produces the weakness in the blockchain simultaneously. Since nonce is not guarded and multiple nonce values for the same block would exist, the opponents with high computing power/resources can generate incorrect, but valid block, and thus, the system remains unprotected. As remedy, at least one private-value must be incorporated in block/blockchain for its security and for this, similar to the security of transactions mentioned above, each new block must be accompanied by the digital- signature and certificate of the winning miners. Thus, the proposed block formation would be as follows:

$$Block = Y \parallel SIG_{Win\text{-}miner}(Y) \parallel CERT_{Win\text{-}miner}$$

where $Y = (hash(\text{last-block of blockchain}) \parallel Merkle(TX_{set}) \parallel \text{Time-stamp} \parallel \text{nonce})$ and $SIG_{Win\text{-}miner}(Y) = ECDSA(private\text{-}key_{Win\text{-}miner,}\ hash(Y))$. Although *nonce* is available in the proposed block, it would be deleted from the block when the coin-generation reward becomes zero (and the miners would be incentivized by the transaction processing fees only).

Ⅳ. Conclusions

Bitcoin is a popular decentralized cryptocurrency system with some unique features not present in any present-day card-based system and others. It mainly uses public- and private-key pairs for users' anonymities, BTC wallets, digital signature generation/verification, cryptographic hash functions, Merkle hash-tree, and more importantly, a computationally hard proof-of-work for generation/validation of blocks/blockchain ledger. In this paper, two security weaknesses in cryptographic transactions and blockchain, which are the heart of BTC, are identified for users' anonymities and possible tampering of block/blockchain, respectively. For removal of these vulnerabilities, we propose for inclusion of digital certificates, which are available through PKI and use

of authenticated blocks (and blockchain as well) signed by the wining miners. Although a little computational overhead is increased, the BTC cryptocurrency system would convert into a real-life system with strong safeguard against relevant attacks.

<References>

[1] Andrychowicz, M., Dziembowski, S., Malinowski, D., and Mazurek, L. (2016). Secure multiparty computations on bitcoin. *Comm. of the ACM, 59*(4), 76-84.

[2] Back, A. (2002). *Hashcash- A denial of service counter-measure*. Retrieved from http://www.hashcash.org/papers/hashcash.pdf.

[3] Badev, A., and Chen, M. (2014). *Bitcoin: Technical background and data analysis*. Finance and economics discussion series, divisions of research & statistics and monetary affairs, Federal Reserve Board, Washington, D.C.

[4] Bergstra, J. A., and Weijland, P. W. (2014). *Bitcoin: A money-like informational commodity*. Retrieved from http://science.uva.nl/research/prog/publications.

[5] Bitcoin - Wikipedia, Retrieved from http://en.bitcoin.it/wiki/Introduction

[6] Dang, Q. H. (August, 2012). *Recommendation for applications using approved hash algorithm*. Publication 800-107 Revision 1, Technical report, National Institute of Standards and Technology (NIST).

[7] European Central Bank, Virtual Currency Systems (October, 2012). *ECB reports*. Retrieved from http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencieschemes201210en.pdf.

[8] Garay, J., Kiayias, A., and Leonardos, N. (2015). The Bitcoin Backbone Protocol: Analysis and Applications. In: Oswald E., Fischlin M. (eds) *Advances in Cryptology - EUROCRYPT 2015. EUROCRYPT* 2015. Lecture Notes in Computer Science, vol 9057. Springer, Berlin, Heidelberg.

[9] Johnson, D., Menezes, A., and Vanstone, S. (2001). The elliptic curve digital signature algorithm. *International Journal of Information Systems, 1*, 36-63. https://doi.org/10.1007/s102070100002

[10] Karame, G., Androulaki, E., and Capkun, S. (2012). *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*. IACR Cryptology ePrint Archive, 2012(248). Retrieved from http://eprint.iacr.org/2012/248.pdf.

[11] Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The economics of bitcoin mining, or bitcoin in the presence of adversaries. *Proceedings of WEIS*.

[12] Lo, S., and Wang, J. C. (2014). *Bitcoin as money?* Federal Reserve Bank of Boston, Current Policy Perspective, No. 14-4.

[13] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. *Proceedings of the 2013 conference on Internet Measurement Conference*. Retrieved from https://doi.org/10.1145/2504730.2504747

[14] Merkle, R. C. (1988). A digital signature based on a conventional encryption function. In: Pomerance C. (eds) *Advances in Cryptology — CRYPTO '87*. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg.

[15] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer electronic cash system*. http://bitcoin.org/bitcoin.pdf.

[16] Stallings, W. (2003). *Cryptography and network security-principles and practices*. Third Indian Reprint, Pearson Education.

◆ About the Authors ◆

Anindya Kumar Biswas

Anindya Kumar Biswas has completed his B.Tech in CSE, M.Tech in IT and enrolled in PhD research scholar as full time JRF in the Department of Computer Application at National Institute of Technology (NIT) Raipur, India. He has published some research articles in Journal and Conference proceedings. His research interests include Cryptography, Information Security, Wireless Networks and Network security.

Mou Dasgupta

Mou Dasgupta is an Assistant Professor in the Department of Computer Application, National Institute of Technology Raipur, India. She has obtained Master of Computer Application (2007) from West Bengal University of Technology and Ph.D. (Computer Science, 2012) from Indian Institute of Technology (Indian School of Mines), Dhanbad respectively. Her research interests include Optimization of Computer Networks, Information Security, Internet of Things etc.

Submitted: March 26, 2019; 1st Revision: September 9, 2019; Accepted: October 4, 2019