ETTF: A Trusted Trading Framework Using Blockchain in E-commerce

Wenlin Xie[1],Wei Zhou[3],Lanju Kong[1]✉,Xiangdong Zhang[4],Xinping Min[1],Zongshui Xiao[1],Qingzhong Li[12]
School of Computer Science and Technology, Shandong University, Jinan, China[1]
Dareway Software Co.,Ltd, Jinan, China[2]
CPC Shandong Provincial Part School Library, Jinan, China[3]
State Grid Chongqing Electric Power Corporation Customer Service Center, Chongqing, China[4]
*E*mail: klj@sdu.edu.cn

***Abstract*—Improving efficiency and performance is an important topic in the world today. As it is well-known, cooperative computing is an effective and traditional approach, and it is widely used in various fields. Inspired by this idea, take E-commerce for example, Security is one of its important indicators. In E-commerce, the security technology has become a major issue restricting the rapid development and popularization of E-commerce. Existing solutions leverage blockchain protocols to improve the credibility of transactions, but most of them have some limitations, such as a lower throughput and higher consensus latency, and these problems make blockchain technology difficult to be widely used. This paper presents a trusted framework $(ETTF)$ using blockchain protocol in E-commerce to achieve a higher credible trading. ETTF includes a peer blockchain protocol (PBP) based on a peer blockchain architecture to support the storage of massive transactions and instant transactions. In PBP, the throughput scales are nearly linearly increased with the computation: the more computing power available, the more blocks are selected per unit time. Besides, in order to ensure a higher security of transactions we have introduced a strong consensus algorithm(ECA) in E-commerce. ETTF is also efficient because the number of messages it requires is nearly linear in the network size. Compared to Bitcoin-derived blockchain, ETTF shows better performance on throughput, latency, and capacity in E-commerce.**

***Keywords*—Blockchain, consensus mechanism, instant, trusted.**

I. Introduction

The emergence of E-commerce has largely changed people's way of life, and it becomes indispensable to everyone. However, while E-commerce is bringing convenience to us, it has also exposed many problems that need to be solved. First of all, the issue that we need to worry about is security, which includes a lot of content, such as information security. Security is a crucial issue, which concerns the public's trust in e-commerce and even the ebb and flow of e-commerce. Second, the openness of transactions also should be taken into account carefully. Because e-commerce platform is a centralized system, provided services are massively centralized, which enables the platform to have almost all the information and credit, forming an absolute monopoly. In the event of a dispute between the customer and the platform, it is very disadvantageous to the customer, in some cases, the platform may even delete or tamper with the data. Even more seriously, once the platform fails, or be attacked maliciously by criminals [1], the result is disastrous (such as Information leaked, lost and tampered), especially in the field of e-commerce, which are unaffordable. In fact, however, such security incidents are not uncommon around us. In view of these problems, If it adopts the decentralized technology of blockchain, the problems could be well solved.

A blockchain is an open distributed database system. In addition to the private information on parties involved in the transaction, the data onto blockchain is open to all. Decentralization allows any node participating in a system, based on the Bitcoin-derived blockchain protocol [2], to enjoy exactly the same rights and obligations as all the other nodes. Because of consensus mechanism, all the nodes will complete the transaction information synchronization again and again according to it, so that the data onto all nodes in the blockchain network is completely consistent, based on consensus mechanism, all nodes will synchronize the data of transaction every 10 minutes, so that the ledger kept in each peer is completely consistent. Every block contains a hash value of the previous block, which is used to trace and connect to the previous block. Due to the hash algorithm has the characteristics of irreversibility and non-conflict, and the blocks are connected chronologically, it makes data very difficult to be tampered. In addition, once the information is verified and added to the blockchain, will be permanently stored. The modification of the database on a single node is invalid, unless more than 51% of the nodes in the system can be controlled at the same time, so blockchain of high stability and reliability. These properties [3] enables reliable transactions without a centralized management mechanism even if there are unreliable participants in the network, and make the double-spending difficult.

Although the technology of bitcoin-derived blockchain has many outstanding advantages, there are still some unsatisfactory issues need to be improved, such as the size of block, in Bitcoin-derived blockchain, it is currently limited to 1MB, resulting in that only 1 to 3.5 transactions per second for Bitcoin [4]. In e-commerce, not only a large amount of transactions need to handle simultaneously, and each transaction need to process immediately. Obviously, if E-commerce adopts Bitcoin-derived blockchain to solve those problems, it would not satisfy the demands of E-commerce very well. So, we

978-1-5386-1482-2/18/$31.00 ©2018 IEEE

present a Trusted Trading Framework Based on Blockchain in E-commerce $(ETTF)$, which can keep unlimited data and support instant transactions, and it can be a good solution to the above problems. Our objective is to construct a higher efficient, secure, public, trusted, and autonomous e-commerce environment.

Most blockchain protocols can guarantee a higher security of transactions by sending all transactions to other peers in the price of consuming much computation resources.

The key idea in ETTF is to construct a peer blockchain protocol which divides all peers into different committees. Unlike other blockchains, PBP doesn't leverage proof-of-work mechanism used in Bitcoin. Some blockchain protocols use a set of validation peers to validate the legality of transactions, but all of those blockchains consider the validation peer valid always. In PBP, we develop a validation peer selection algorithm, which can dynamicly change membership in each epoch. PBP is a collaborative protocol without wasting computation resources. Because PBP will increase communication costs. To reduce the communication costs, we develop a new propagation algorithm in E-commerce (EPA). EPA introduces a validation peer set as the representation of all peers to validate the legality of block. As PBP can't achieve the openness and a peer can still tamper the information, so we develop a new global consensus algorithm (ECA) that is run in all peers. ECA leverages proof-of-work mechanism to write the hash value of a block into a global block in every epoch.

By constructing a three-layer blockchain, we represent a Trusted Trading Framework$(ETTF)$ Based on Blockchain, which has better performance on E-commerce. There are two contributions to our research, on the one hand, ETTF can guarantee a higher credibility of transaction, support instant transaction, and keep unlimited data. On the other hand, under the same trust assumptions as Bitcoin, ETTF can achieve higher throughput and lower latency than Bitcoin by partitioning network into several sub-committees.

The rest of the paper is organized as follows. We discuss the related work about blockchain scalability in Section II, and provide an overview of ETTF in Section III. Section IV elaborates the ETTF. Section V gives the experimental results and analysis. Finally, we close this paper with conclusions in Section VI.

II. Related Work

The core technology in Bitcoin-derived blockchian innovation powering these systems is the Nakamoto consensus protocol for maintaining a distributed ledger known as the blockchain. The blockchain technology provides a decentralized, Byzantine fault-tolerant transaction mechanism, and promises to become the infrastructure for a new generation of Internet interaction, including anonymous online payments [5], remittance, and transaction of digital assets [6]. Ongoing work explores smart digital contracts, enabling anonymous parties to programmatically enforce complex agreements [7]. Despite its potential, Bitcoin-derived blockchain protocols also face a significant scalability barrier. Bitcoin has scalability issues in terms of throughput, latency, capacity, and network bandwidth. For example, increasing block size can improve throughput, but the causing bigger blocks take longer time to propagate in the network. Reducing the block interval reduces latency, but leads to instability that the chain is forked into branches.

Many consensus protocols use randomization mechanisms, especially in order to circumvent the well-known FLP impossibility resulted in deterministic asynchronous networks [8]. Generally, nondeterministic restatement of the consensus problem involves Las Vegas rules: the network must eventually reach consensus, although the amount of time taken may be unbounded. King and Saia [9] considered the Las Vegas rules is too strict for large scale networks. Since deterministic consensus requires at least message bits [10], any randomized consensus protocol using fewer than quadratic messages must be a Monte Carlo protocol with nonzero probability of failure [11], [12].

In other aspects [13], Zerocash [14] and Zerocoin [15] provide anonymous payments through the use of a novel type of cryptographic proofs. Unlike Bitcoin, is an anonymous payment system that can provide excellent blockchain privacy and more higher throughout. However, the parties entrusted to anonymize transactions in [16] can still violate users' anonymity, even if they are honest-but-curious. Ittay [17] Eyal presents Bitcoin-NG, a new Bitcoin-derived blockchain protocol designed to scale. Bitcoin-NG achieves that Byzantine fault tolerant, robust to extreme churn, and sharing the same trust model obviating qualitative changes in the ecosystem. Hong-Jie He [18] proposes a blockchain based fragile watermarking scheme to solve the issue of security and accuracy of tamper localization

III. Overview of The Trusted Trading Framework Using Blockchainin E-Commerce

We denote by p represents a peer. The identities of peers are established using public-key cryptography as follows: When a peer joins the network for the first time, p generates a public and private key pair. In E-commerce, each peer represents a third party payment platform, logistics platform or synthesis supervision platform. We introduce three types of peer: global blockchain generation peer (gp), global blockchain validation peer (vp), and ordinary peer (op). Only gp has the permission to generate global block, only vp has the permission to validate the legality' of global block. Each peer can deal with transactions. All peers compose Trusted Trading Network $(ETTN)$ based on ETTF.

ETTF proceeds in epochs. In each epoch, firstly, each peer writes the transactions into blocks. Meanwhile, according to peer's honesty that indicates the probability of tampering transaction, available mining power that indicates peer's computing power, ETTF generates gp and vp set from all peers. Secondly, all gp generate collaboratively E-commerce global block, and send global block to vp set. Thirdly, vp set integrate multiple global blocks into a single one and validate the legality of the global block. In TTEN, each peer must keep all global

blocks. op just manage peer blocks, and gp manage all peer blockchains.

ETTF includes two parts: Peer Blockchain Protocol (PBP) and a strong consensus algorithm in E-commerce (ECA). PBP is a blockchain protocol to protect the security of transactions in peer. ECA is just used to prevent the dishonesty peers to tamper other peer's transactions.

IV. THE TRUSTED TRADING FRAMEWORK USING BLOCKCHAIN IN E-COMMERCE

A. Peer Blockchain Protocol

To protect the security and trust of transactions in each peer, this paper presents a peer blockchain protocol (PBP). Each peer has a peer blockchain, which just keeps transactions involved in transfer of assets. In PBP, the status of each block introduces three types: undecided, valid and invalid. In peer blockchain, each peer micro block (PMB) contains a group of transactions, a vote list by vp set and includes signature list as shown in Figure 1a. Each peer key block (PKB) contains a group of PMB as shown in Figure 1b. There is a majority of positive or negative votes for a PMB in vp set, this PMB can go from undecided to valid or invalid. It's a rule that only valid PMB can be written into a PKB. If PMB is considered to be valid, those transactions PMB contained also are valid, and transactions are in effect that will be executed.

PBP proceeds in epoches. Each transaction and PMB goes from undecided to valid or invalid. To guarantee the time from occurrence of transaction to transaction in effect less than one second, multiple PMB will be generated in one time, but only one PKB will be generated in one time. To protect the security and trust of transactions, each PMB must be signature with vp set. As shown in algorithm 1: PBP can be divided into three steps: firstly, PBP checks the legality' of transactions. Second, PBP writes valid transactions into PMB, and sends to the vp set. Thirdly, PBP writes valid PMB into PKB.

In general, if a vp receives a PMB, vp checks legality of this PMB, and sends this PMB to any vp with peer itself signature. If majority of vp voted that the block is valid, all vp keep this PMB into itself peer blockchain. The traditional p2p broadcast mechanism will consume much more network bandwidth. If each peer sends the PMB with signature one by one in order, sometimes the first peer will never receive the voting result, if any peer breaks down, it will stop the process of voting. So, this paper develops a new broadcast mechanism EPA, which has lower communication costs. Our goal is to reduce the communication costs from N^N to $K \bullet N$, where N represents the number of peers in ETTN and $1 \leq K \leq N$. The key idea in EPA are to assign each identity to a random group. First, we divide all vp into m groups g_i. Second, each peer generates the next sending list by randomly selecting one peer form each groups, where $sendList = \{p_i, p_i \in \ g_i, 1 \leq i \leq m\}$. Suppose the number of peers in one group is N/m, the maximum of propagation frequency is $m \bullet N + m^2$. Because $m \bullet N + m^2 \leq 2N^2$, and $m \ll N$, so $m \bullet N + m^2 \leq K \bullet N$. Moreover, if any vp finds majority of vp voted PMB is invalid or valid, this vp returns this PMB to peer who sends this PMB at first and other vp . If the peer who sends this PMB at first, receives enough PMB with signatures, this peer will send a message to all vp to stop the voting process of this PMB. So, EPA has better performance than traditional mechanism.

In PBP, only if transactions were written into a PMB, anyone can't tamper the information in any ways. Because any PMB must be agreed with majority of peers, this PMB can be valid. Moreover, majority of vp must keep this PMB into their blockchain. If one peer wants to tamper an existing transaction, it's impossible to tamper all information in other peers simultaneously.

Algorithm 1 PBP

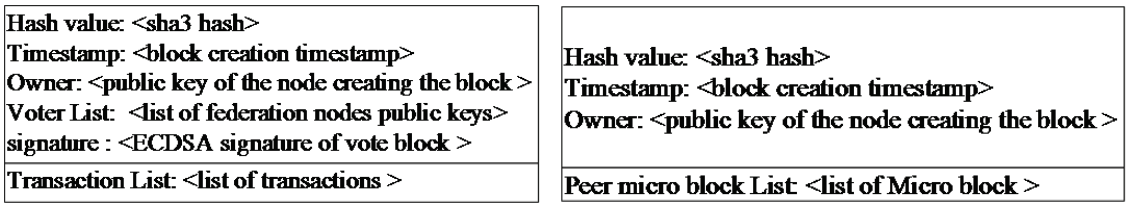
Input: Text:All Transactions
Output: Peer Key Block

for each transaction T, whose status$(T) == undecided$ **do**
  Check legality of T and assigned invalid or valid
  if status$(T) == invalid$ **then**
    Remove T
  end if
end for
for each time epochs **do**
  Select $VTset$, in which each T satisfies status$(T) == valid$
  if size$(VTset) \leq$ 1M **then**
    Write $VTset$ into a new PMB
  else
    $(VTset)$ will be divided, and writen into several PMB with a size of 1M
  end if
end for
for each PMB **do**
  if status$(PMB) == undecided$ **then**
    Send PMB to vp set
  else if status$(PMB) == invalid$ **then**
    Delete the PMB
    Reassign each T to undecided
    Return to step 1
  else if status$(PMB) == valid$ **then**
    Each T is in effect
    Write PMB into a new PKB
  end if
end for

B. E-commerce Consensus Algorithm

After each peer generate their PKB, it's necessary to construct a global blockchain $(E-Blockchain)$ to keep all PKB in ETTN. In ETTN, the E-Blockchain provides an index to all peer blockchain, so that each peer can validate PMB received from other peers. Figure 2 shows the architecture of block in E-Blockchain. Each global block (EGB) contains a group of PKB, the constructor and voter list.

In E-commerce, if we adopt the proof-of-work mechanism to generate EGB, it will consume much resources that don't



(a) Peer Micro Block Architecture

(b) Peer Key Block Architecture

Fig. 1. Block Model in peer blockchain

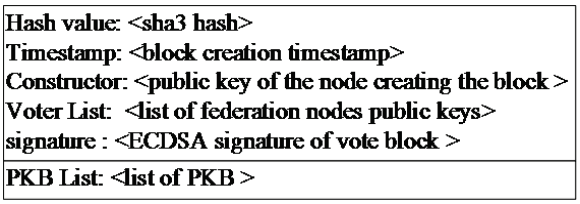


Fig. 2. Block Model in E-Blockchain.

need to waste. In other words, it will increase cost of E-commerce platform. Furthermore, the proof-of-work mechanism should be careful of the problem of crypts puzzle. In Bitcoin, the problem of crypts puzzle, sets by this value, is dynamically adjusted such that blocks are generated at an average rate of one every ten minutes. More problem difficulty lager, more time needed to generate a block. In E-commerce, to support instant transactions, it's necessary to use a collaborative mechanism without sacrificing security, which can reduce the consensus latency. So, we adopt a collaborative mechanism to generate EGB in epochs. Firstly, selecting one or more nodes from each peer select to form a gp-group, called global construction group (GCG), and then, a primary node will be selected from all nodes in GCG, finally, the primary node adopts the PBFT algorithm to generate EGB.

As shown in Algorithm 2, ECA can be divided into two steps: First, we need to build a global construction group (GCG). Each node(n) in the network randomly selects a set of nodes($n$set) from the whole network, then sends the selection results to other nodes in the network. Moreover, the nodes should belong to peers above $2/3$ of the whole network, and can not exceed 2 times the total number of peer in the whole network (Assuming that the network contains M peers and the number of selected nodes is m, then $2/3M < m <= 2M$). After this process is over, all nodes will count the votes, and the 2M nodes with the highest number of votes are taken as the global construction group. In this way, the identity of each node will be determined. Second, selecting a primary node$(Pnode)$ from GCG to construct EGB, the method is similar to building GCG. Every node in the GCG called construction node(cn). Each construction node randomly selects a construction node as a preselected object for primary node, and sends the result to other construction nodes. After voting, the construction node, who gets the most votes, would be taken as the primary node, and have the permission to generate EGB. The primary node constructs an EGB, and sends to other construction nodes. Each construction node received the EGB validates the legitimacy of EGB. If the EGB is valid, it will be sent to other nodes in the network, and the primary node continues the construction of the next EGB. If the EGB is invalid, it will be deleted, and a new primary node will be selected to proceed.

Algorithm 2 ECA

for each time epochs **do**
  for n_i in $\{n_1, ..., n_m\}$ **do**
    $votes \leftarrow$ Rselect $n$set, $2/3M \leq Size(\text{n}set) \leq 2M$
    $voteList \leftarrow GeneratevoteList(votes)$
    $SendcvoteList()$
  end for
  $voteList' \leftarrow AddvoteList$(all $voteList$)
  GCG $\longleftarrow$ top 2M nodes($voteList'$)
  for cn_i in GCG **do**
    $cvotes \leftarrow$ Rselect cn_j, $(1 \leq j \leq 2M)$
    $cvoteList \leftarrow GeneratecvoteList(cvotes)$
    $SendcvoteList()$
  end for
  $cvoteList' \leftarrow AddcvoteList$(all cvotes)
  Pnode $\leftarrow$ Select cn_i (Max($cvotes'$))
  EGB $\leftarrow constructEGB$(Pnode)
  $sendEGB()$
  for cn_i in GCG **do**
    $ValidateEGB()$
    if status$(EGB) == valid$ **then**
      $SendEGB()$
      NextEGB $\leftarrow constructnextEGB(Pnode)$
    else if status$(EGB) == invalid$ **then**
      $DeleteEGB()$
      NextPnode $\leftarrow selectNextPnode()$
    end if
  end for
end for

V. EXPERIMENTS

In this paper, we refer to Fabric and Ethernet Fang to implement the ETTF. The experiment environment as follows: 20 servers, each server is configured with 128G memory, 32

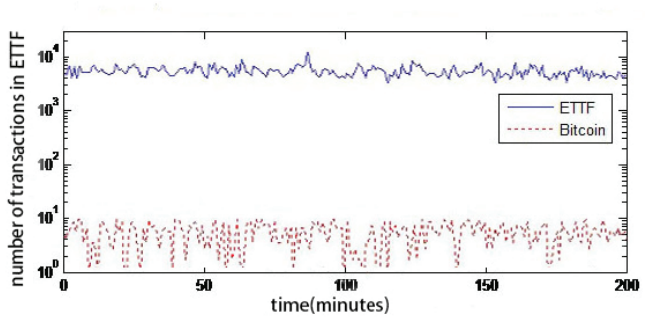


Fig. 3. the number of transactions per second

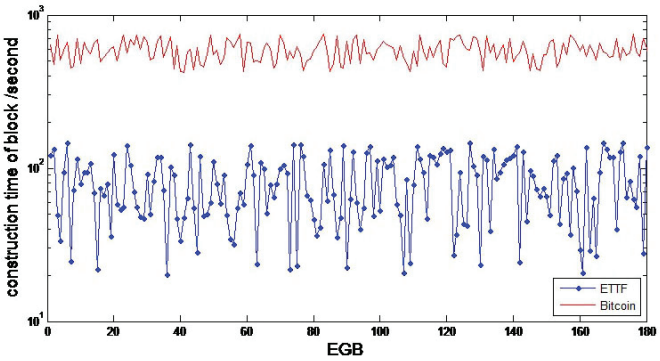


Fig. 4. the EGB constructed time

core CPUs, 10T storage space, and Gigabit network communication between servers, blockchain nodes are encapsulated through Docker technology. In this section, we conducted a series of experiments to evaluate the performance of ETTF by varying the throughput of transaction, transaction latency, and block size. This time we selected 300 nodes to carry out the experiment to fully observe the performance improvement in ETTF.

A. Throughput of transaction

Trading throughput is an important performance indicator. The main features of ETTF are two. First, it assigns each transaction to each peer, and the GP is only responsible for maintaining the hash value of the block in each peer. Followed by: transactions information written in the PMB, the hash value of PMB is stored in the PKB, and the PKB store the hash value of PMB, it is well known that the size of hash value is much smaller than its hash before the transaction data, so, logically, the EGB can carry a large amount of transaction data. As shown in Figure 4, the performance of ETTF in throughput is better, and can achieve higher throughput.

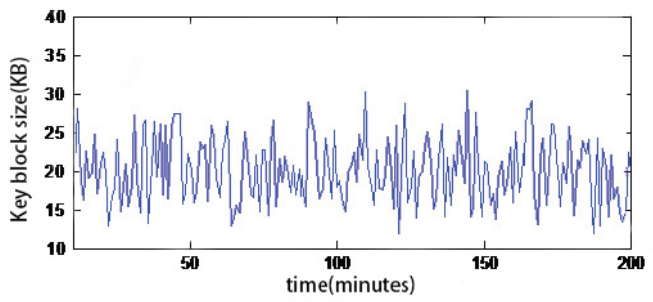


Fig. 5. the EGB size

B. Block Frequency

For Bitcoin, if we vary the frequency of block generation by reducing the proof-of-work difficulty, the security of the transaction may be reduced. For ETTF, we vary the frequency of micro block generation. For each frequency, we choose the block size such that the payload throughput is identical to that of Bitcoins operational system.

In ETTF, instead of POW, we build blocks based on PBFT in this paper, and the state of network communication is relatively good, so the delay would be much lower. Figure 4 shows that generating an EGB in ETTF takes much less time than building in Bitcoin-derived blockchain.

C. Block Size

In ETTF, each user just can commit one transaction in one time. And, the content of every EGB just contains a set of hash value, just like PKB and PMB, so the size of global block is very small, just a few KB as shown in Figure 6.

VI. Conclusion

In today's society, e-commerce has been an important part of our life, from mobile payment to bank deposits, so safety and efficiency has become a high-profile topic. Cryptography is the main research direction on the issues. The Bitcoin-derived blockchain with a series of technology combinations such as distributed storage, timestamp, hash-encryption, etc. achieves a highly trusted E-commerce environment. But it returns security by sacrificing efficiency, for example, generating a data block every 10 minute to avoid blockchain fork. In addition, the size of blocks is strictly limited, which limits the number and frequency of transactions.

To break through the bottleneck of instant and large-scale trading without sacrificing credibility. This paper presents a trusted trading framework in E-commerce $(ETTF)$. ETTF is based on blockchain architecture and a robust strong consensus algorithms, does not limit the size of blocks, supports instant transactions, and has no forks in blockchain. ETTF includes two parts: First, a peer blockchain protocol (PBP), which proceeds in epoches, could protect the security of transactions in peer. Among them, a propagation algorithm(EPA) uses voting mechanism and rotation mechanism, and vp set instead of all points, effectively reducing communication costs. Second, global consensus algorithm (ECA) prevents the dishonesty peers to tamper other peer's transactions by writing the hash value of a block into a global block in every epoch, and implementes instant transactions. ETTF makes it possible to achieve higher throughput and lower consensus latency by improving the scalability of the blockchain protocol, where

the key to latency is the is the ability of a single peer. ETTF enables all peers in the network to collaborate to build a public, trusted, decentralized autonomous system that shows better performance in e-commerce.

In future work, we will devote more energy to the application of blockchain and continue to study and improve consensus mechanisms and algorithms to achieve better security and efficiency.

ACKNOWLEDGMENT

This work is partially supported by NSFC No.61772316; the Science and Technology Development Plan Project of Shandong Province No. 2016GGX101008, No. 2017CXGC0702; Shandong Province Independent Innovation Major Special Project No. 2016ZDJS01A09; the Taishan Industrial Experts Programme of Shandong Province.

REFERENCES

[1] M.Trent, M.Rodolphe, M.Andreas, D.Dimitri, M.Troy, M. Greg, H.Ryan, B.S, Y.Alberto. "BigchainDB: A Scalable Blockchain Database (DRAFT).",2016.

[2] S.Melanie. "Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization." Texas Bitcoin Conference, pp.27-29, 2015.

[3] Swan, Melanie. Blockchain: Blueprint for a New Economy. " O'Reilly Media, Inc.", 2015.

[4] Blockchian.info, Number of Transactions, [online]. Available: https://blockchain.info/charts/n-transactions.

[5] A.Back, M.Corallo, L.Dashjr, M.Friedenbach, G.Maxwell, A.Miller, A.Poelstra, J.Timon, P.Wuille. 2014. Enabling blockchain innovations with pegged sidechains. Technical Report. http://www.blockstream.com/sidechains.pdf.

[6] Colored Coins Project. Colored Coins. http://coloredcoins.org/, retrieved Sep. 2015.

[7] Kendler, EH.Alison, A.Zohar, S.Goldberg. "Eclipse Attacks on Bitcoin's Peer-to-Peer Network." 24th USENIX Security Symposium (USENIX Security 15). 2015.

[8] A. Miller, J. LaViola. Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin. University of Central Florida. Tech Report, CS-TR-14-01, April 2014.

[9] V. King, J. Saia, Breaking the O(nsup2/sup) bit barrier: scalable byzantine agreement with an adaptive adversary, Journal of the ACM (JACM), vol. 58, no. 4, pp.18:118:24, 2011.

[10] D. Dolev, R. Strong, Authenticated algorithms for Byzantine agreement, SIAM Journal on Computing, vol. 12, no. 4, pp. 656666, 1983.

[11] H. Attiya, K. Censor-Hillel, Lower bounds for randomized consensus under a weak adversary, SIAM Journal on Computing, vol. 39, no. 8, pp. 38853904, 2010.

[12] R. Tempo and H. Ishii, Las Vegas randomized algorithms in distributed consensus problems, European Control Conference, vol. 13, no. 2-3, pp. 189203, Jun. 2007.

[13] Heilman, Ethan, Foteini Baldimtsi, and Sharon Goldberg. "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions." Fbim Transactions, pp37-48, 2015

[14] E.Sasson, A.Chiesa, C.Garman, M.Green, I.Miers, E.Tromer, M.Virza. Zerocash: Decentralized anonymous payments from bitcoin. IEEE Security and Privacy (SP), pp.459474, 2014.

[15] I.Miers, C.Garman, M.Green, and A.Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. IEEE Security and Privacy (SP), pp.397411, 2013.

[16] A.Saxena, J.Misra, A.Dhar. Increasing anonymity in bitcoin. Financial Cryptography and Data Security, pp.122139. Springer, 2014.

[17] Duffield, E., Hagan: Darkcoin: Peer-to-peer crypto currency with anonymous blockchain transactions and an improved proof-of-work system. Technical report (March 2014),http://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf.

[18] He, Hong-Jie, Jia-Shu Zhang, Heng-Ming Tai. "Block-chain based fragile watermarking scheme with superior localization." Information Hiding. Springer Berlin Heidelberg, pp.16, 2006