Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/110315

Privacy Preserving Non-interactive Proof of Assets for Bitcoin Exchanges

Maya Mohan[1,*] *and M. K. Kavitha Devi* [2]

[1] Department of Computer Science and Engg, NSSCE, Palakkad, Kerala, India
[2] Department of Computer Science and Engg, TCE, Madurai, Tamilnadu, India

Received: 27 Dec. 2016, Revised: 2 Mar. 2017, Accepted: 13 Mar. 2017
Published online: 1 May 2017

Abstract: Bitcoin is a decentralized cryptocurrency for e-payments.Bitcoin exchanges stand for the trading of customers' bitcoins against major paramount currencies.The users' bitcoins can be stored in a digital wallet offered by the Bitcoin exchange.Precisely, Bitcoin exchanges are equivalent to banks,providing security for the customer's bitcoins in their absence.An exchange always need to be solvent interms of its assets and liabilities to meet its long term financial obligations .Maxwell was the first one who proposed a cryptographic based proof of liabilities .But the scheme is not secure enough to keep the user information confidential.Later Dagher et al. proposed a privacy preserving proof of solvency for Bitcoin exchanges.But the scheme works in an interactive manner.This restricts the proof computation offline.This paper addresses the first non interactive proof of assets using hybrid commitment schemes in the non programmable random oracle model.The non-interactive zero knowledge proof is defined in the common reference string model.

Keywords: Cryptocurrency,Bitcoin Exchange, Zero Knowledge Proof,Hybrid Commitment Scheme,Proof of Asset,Pedersen Commitment Scheme

1 Introduction

In the current era, e-transactions are achieved using digital currencies [1] [2] .Cryptocurrencies are digital currencies, which build on strong cryptographic algorithms, enable the fund transfer efficiently all over the world without any intervention of bank regulatory.The main attraction of cryptocurrencies are their low transaction fee. Bitcoin [3] is the leading cryptocurrency [4] from its birth till today that make use of peer to peer system (P2P) for e-payments and works in a decentralized manner. The bitcoin trading is done through bitcoin wallet software. The transactions are managed using public key cryptographic scheme and digital signature scheme. The unique address generated from the public-private key pair by the wallet called the Bitcoin address is used for performing e-transactions. Bitcoin uses a complex structure and considered to be a revolutionary attempt against double spending without any trusted third party. Bitcoin scripting language which is not turing complete is used for representing the transactions. A transaction consists of inputs and outputs.The input proves that the spender is having enough number of bitcoins to spend and the outputs denote to whom the bitcoin is transferring and the amount. The transaction is considered to be valid only if the spender is trying to spend an unspent transaction amount.A transaction script is shown in Table 1.

The metadata provides the housekeeping information such as entire hash of the transaction, version number,number of inputs and outputs,transaction publication time for escrow transactions,size of the transaction etc.For normal transactions the lock_time is set to zero.The array of transaction input gives the information regarding the previous transactions.It includes the hash of the previous transaction along with an index indicating the claimed output of the previous transaction.The signature script shows the ability of the user to claim the outputs of the previous transaction.The array of transaction output contains the value and the bitcoin script for evaluation that includes the hashed public key of the recipient.The script evaluation is carried out using stack.The transaction is valid only if the spender is trying to spend an unspent transaction.Once the script is ready ,it will broadcast in the bitcoin network.In the P2P network, a node on receiving a transaction from

* Corresponding author e-mail: mayajeevan@gmail.com

Table 1: Bitcoin Transaction script

Transaction script contains three parts
Metadata 1 : ”*hash*” : ”23*a*56*d*.....”, 2 : ”*ver*” : 1, 3 : ”*vin_sz*” : 2, 4 : ”*vout_sz*” : 2, 5 : ”*lock_time*” : 4567, 6 : ”*size*” : 300
Inputs ”in”:[”prev_out”: ”hash”:”567da3...” ”n”:0 , ”scriptsig”:”34c2a...”, ”prev_out”: ”hash”:”54e3a2...” ”n”:0 , ”scriptsig”:”22bc12a...”]
Outputs out:[”value”: ”5.08”, ”scriptpubkey”: OP_DUP OP_HASH160 692e27..... OP_EQUALVERIFY OP_CHECKSIG”, ”value”: ”3.12”, ”scriptpubkey”: OP_DUP OP_HASH160 84ac31..... OP_EQUALVERIFY OP_CHECKSIG”]

another node verifies,stores and forwards the transaction to all connected nodes.In this way the transaction validation is carried out in the Bitcoin network.Bitcoin miners grouping the verified transactions into to a block for optimization.The block structure is given in table 2.

Table 2: Bitcoin Block script

Block script contains two parts
Metadata 1 : ”*hash*” : ”531*b*3*a*7*c*.....”, 2 : ”*ver*” : 2, 3 : ”*prev_blk* : ”023*a*.....”′ 4 : ”*time*” : 21234, 5 : ”*bits*” : 456746700, 6 : ”*nonce*” : 567433056, 7 :*mrkl_tree*”′ : ”3457890335576...”, 8 : ”*n_txn*” : 49 9 : ”*size*” : 181527
Body of the Block ”txn”:[.....] ”*mrkl_tree*” : [”6*a*5.....” ”75*c*.....”]

The block header contains a version number that denotes the software version used for creating the block. The Prev_blk field indicates the hash value of the previous block.The time field indicates the current time in seconds.The hash ,bits and nonce fields are used for the mining process.The field n_txn denotes the total number of transactions added to the block and mrkl_root is the hash of all transactions in the block.The size field gives the total size of the transactions and it should be less than 1000000 bytes.The blocks are linked together through hash pointers form the blockchain. The merkle-hash tree is used for maintaining the blockchain as shown in figure 1. The leaf node of the merkle tree contains the transaction and the other nodes hold the hash values.The entire block’s hash value is stored in the hash pointer.For creating the new block the miners have to find the solution for a predefined mathematical problem called proof of work(PoW).The miners will be rewarded with bitcoins for the successful block creation.

The Bitcoin network’s accuracy and stability depends on various socioeconomic factors [5]. The customers assets will be lost even if one such factor fails.The security of customer assets are tightly coupled with the private keys used. So utmost protection needs to be given for cryptographic keys [6].It is the user responsibility to secure the secret keys in order to protect their bitcoins. There exists plenty of methods for the key management in Bitcoin [7]. One of the simplest way is to store the pool of keys on a disk which is not accessible by a third party. But if there is a malware it can steal data from the disk [8]. Another widely used method is the split control [9]. This needs the cooperation of multiple devices to generate the key which helps in avoiding single point of failure. But the network dilemmas may cause the key production. Offline storages [10], password protected wallets, password derived wallets are some of the remedies but they still face some drawbacks.

Many users prefer online exchanges to keep their assets equivalent to online banking. Exchanges help in storing bitcoins and also perform currency conversions.They are playing a vital role in the Bitcoin network and having strong influence over Bitcoin markets.The trading taking place at the exchange determines the value of the bitcoin.The bank information as well as the client’s identity is maintained by the exchange.For selling the bitcoins, the client has to transfer the bitcoins to the exchange’s wallet where the exchange possess the private key.The transactions that deal with bitcoin deposits and withdrawals will be added to the blockchain whereas the bitcoin trading is available only in the bitcoin database.A great level of user’s privacy can be attained using exchanges.The exchange is capable enough to settle the bitcoin of all of its users at any point of time. Bitcoin exchanges need to be committed to its users all the time rather than the fractional reserving system followed by the traditional banks.
From literature survey it is understood that only few proposals have emerged related to the preservation of privacy of the assets of the Bitcoin exchanges .Maxwell [11] was the one who first proposed proof of liabilities based on cryptography for verifying the assets. But it

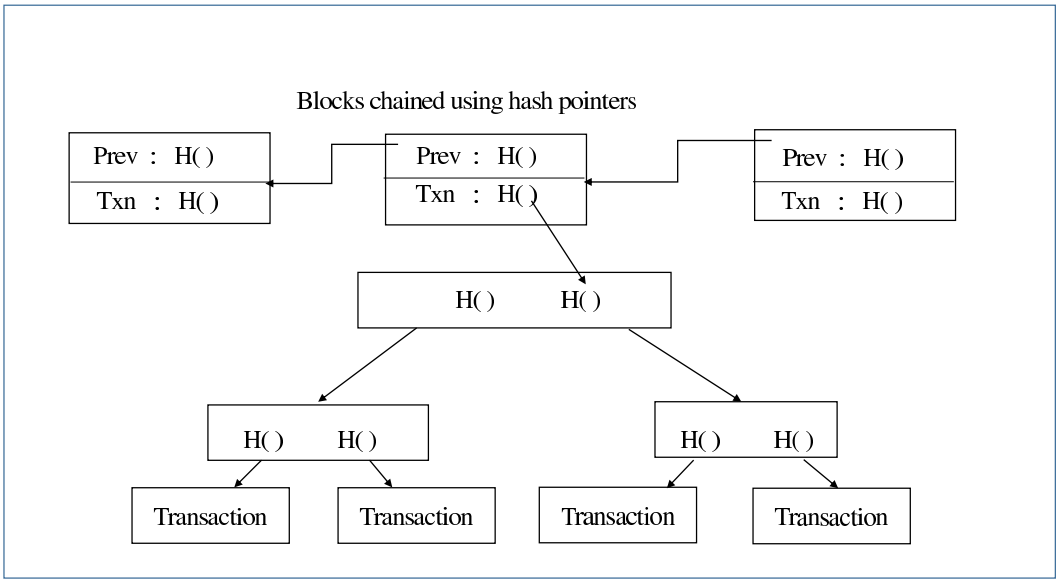

Fig. 1: The blockchain

leads to some privacy issues pointed out by some exchanges.Most of the exchanges operate with a minimum number of accounts by clubbing various customers' holdings. For security reasons the secret keys of these accounts may be kept in cold storage (offline).The exchange can have unique Bitcoin addresses for each of its customers but it necessitates large cryptographic proofs. Maxwell's proof has the provision of proving exchanges' total liabilities as well as users' account verification. It uses binary Merkle hash trees [12]for this purpose. Hash based commitment is used in Maxwell's scheme. The root node has a total commitment of the customer's balance that represents the total liability of the exchange.Only a part of the hash tree is necessary for the verification of each customer account. Unfortunately, it does not have any mechanism for hiding the total liability of the exchange which is residing in the root node. The protocol is not structured enough to hide the complete details of the customers balance.

Later Dagher et al.[13] introduced the privacy preserving proof of solvency with a lot of security options. It highlights the features like complete security for user assets, confidentiality of the exchanges' total assets and unlinkability [14] with the Bitcoin addresses the exchange hold etc. Provisions make use of commitment schemes [15] and zero knowledge proofs [16] for proving solvency in an interactive manner. In Provisions[13]the total asset (set of all bitcoins, the exchange have the signing power) is hidden using cryptographic techniques. An adversary could know only one information that is the total liability (set of all bitcoins available in user accounts) is less than the exchange's total asset. The exchange is said to be solvable if asset dominates liability or the difference of both is almost negligible. The proof of asset is made interactive in Provision. This paper proposes a Provision based non-interactive proof of assets using non-programmable random oracle model [17]. It uses a CRS model (Common Reference String) [18] to make the proof, non- interactive zero knowledge and sound [19] [20]. It is efficient enough to calculate the proof of assets of Bitcoin exchanges in less time since it is not incorporated with any complex computation. Establishing a trustworthy exchange attracts more customers and large deposits. The exchanges ensure that the deposits and withdrawals of each individual are hidden from the outsiders [21]. Some jurisdiction legally demands proof of solvency in bitcoin exchanges [22].

The objective of this paper is to enable an exchange to publicly prove its total asset in a non-interactive manner. Fiat-Shamir scheme is the suitable candidate for this purpose [23]. But it uses random oracle model. We used hybrid commitments [24] in the non- programmable random oracle model[NPRO] [25] to achieve non-interactiveness.The paper is structured as follows.The Section II describes the basic concepts and definitions

related to sigma protocol, zero knowledge proof and commitment scheme.The Section III illustrates privacy preserving non interactive zero knowledge proof of assets for Bitcoin exchanges .The results and discussions are included in section IV and in section V , the conclusion.

2 Basic Concepts

Proof of Assets (PoA) makes use of a Common Reference String(CRS) for defining the public parameters for providing the assets of the exchange . Let g and h be the generators of the group G of order q. According to the Bitcoin policy, anyone can calculate the amount of bitcoin possessed by each Bitcoin address. Let Y be the public key, $Y \in G$ associated with each Bitcoin address then the balance correlated with each public key is denoted as $B(Y)$. The balance $B(Y)$ can take a value in the range between 0 and 2^{51}. The exchange E possesses a large set of public keys which is anonymous that corresponds to the Bitcoin addresses used in the Bitcoin transactions .In the Bitcoin block chain , the exchange E knows a set of public keys for which it knows the private keys. Using Zero knowledge proof and commitment scheme, the exchange convinces the public about it assets. The ownership of the public keys is kept confidential.

Hybrid Commitment Scheme-The commitment schemes used in cryptography allow the user to hide the information for a certain amount of time from other users.It is designed in such a way that once the user is committed something he cannot change the value,only he can reveal it in a later time.Among the commitment schemes,Pedersen commitment scheme is considered to be the most secure scheme, holding the commitment properties computational binding and perfectly hiding. The hybrid commitment scheme used in PoA is similar to Pedersen commitment [26] since it is equivocal. For example, in Pedersen commitment, any message $x \in Z_q$, the commitment $C = g^x h^r$ where r is a random value and g and h are generators of G . The public parameters g and h are of Diffie-Hellman tuple [27] and their relative discrete logarithm is not known. No information about x is revealed since Pedersen commitments are perfectly binding [28].

Zero Knowledge Proofs-The exchange's asset is proved in zero knowledge using the hybrid commitment scheme .In zero knowledge proofs ,the verifier is convinced with the fact the prover is saying, without revealing additional information by the prover.Zero knowledge protocol enable the prover to prove a statement to the verifier without publishing any data other than the validity of the statement.Zero knowledge proofs play a vital role in many areas of cryptography. Zero knowledge proofs are unavoidable in proving the security in multiparty communication in the presence of adversaries [29,30,31,32]. It can be efficiently proved using sigma $(\sum)$ protocol [33].

Sigma Protocol$(\sum)$-The $\sum$ protocols are public-coin Honest Verifier Zero Knowledge (HVZK) [34] proof systems. It is an interactive three round public-coin protocol [35] with a prover P and a verifier V and to prove that the statement $x \in L$ with zero knowledge.The properties it hold are:

- –The verifier provides only a single random string ,the challenge e
- –If the statement $x \notin$ L,then for every first message from the prover there exists only one verifier message that can be answered.
- –There exists a simulator that could generate the same distribution as a real proof system for a given statement x and challenge e

In non-interactive zero knowledge (NIZK) there is no interaction between P and V for proving the statement x.To fulfil NIZK proofs the standard set up CRS is used. The Fiat-Shamir (FS) transform is a NIZK transformation in the random oracle model [36] . In FS transform, the verifier's challenge is replaced by a hash value obtained from the previous prover message. Any concrete instantiation of the hash function in the FS transform leads to an insecure scheme. By applying the FS transform to a $\sum$ protocol guarantees zero knowledge for a cheating verifier. As there is no interaction,it increases the efficiency of the protocol. But FS transform is sound only in the RO model.

For proving PoA we are considering a NIZK with CRS similar to FS using non-programmable random oracle model. The transformation achieves zero knowledge property in the standard model and soundness in the non-programmable random oracle model. The difficulties arise in the zero knowledge composition in the random oracle is not a problem in this transformation. It implies that for the simulation RO is not required and it needs only to prove the soundness. The commitment scheme used is similar to the Pedersen commitment scheme, for which a trapdoor exists by which the commitment can be decommitted to any value. It is similar to the FS transform except the commitment value is hashed rather than hashing the previous message of the prover.

The scheme uses the hybrid trapdoor commitment by which the CRS can be chosen in two different ways. When the commitment is perfectly binding it guarantees soundness and when it is equivocal ensures zero knowledge. The commitment scheme can be constructed from any hard language [37] incorporating a $\sum$ protocol. A concrete instantiation of the scheme provides security under the DDH assumption. A similar transformation introduced by Damgard by setting a regular trapdoor for the commitment scheme [38] . This can not be used since there is no possibility of rewinding the adversary because of the non-interactive nature of the protocol. The zero knowledge construction in the NPRO model proposed by [39] [40] are not completely non-interactive. It requires at

least two messages to handle deniability and transferability issues of NIZK proofs. We basically work on Lindell's transform [25] based on hybrid commitments. According to Lindell the membership hard language L and each commitment, pick an instance of ρ as input such that if $\rho \notin L$ the hybrid commitment scheme is perfectly binding else equivocal if a witness for $\rho \in L$ is known. A polynomial relation R is a subset of the set $\{\{0,1\}^* \times \{0,1\}^*\}$ and x is an instance of language L and w is its witness then the membership $(x,w) \in R$ is bounded in polynomial time. The random oracle model is defined as, $RO : \{0,1\}^* \rightarrow \{0,1\}^n$ where $n \in Z_q$.Some definitions of this paper is taken from [25].

Definition 2.1: A protocol (P,V) constitutes an interactive proof system for a NP language L holding the following requirements,

–Completeness: $\forall x \in L$ and the witness w ,such that $(x,w) \in R$ hold: $Pr[\langle P(w), V\rangle(x) = 1] = 1$

–Soundness : For every $x \in L$,there exists a cheating prover such that for every z, $Pr[\langle P^*(z), V\rangle(x) = 1] < v(|x|)$ Where v is the negligible function.

The three round public-coin protocol π is defined as,

–On input $1^n, x$ and w , P computes a message a and send it to V
–V picks a random challenge $e \in Z_q$ with length t and send it to P
–On input (x,a,e,w) P computes z and send to V
–V accepts or rejects based on (x,a,e,z)

Definition 2.2: Protocol $\pi = (P,V)$ is a $\sum$ protocol for relation R is said to be three round public-coin protocol if the following condition hold:

–Completeness: If P and V follow the protocol for any $x \in L$ and witness w where $(x,w) \in R$ the verifier always accepts
–Special Soundness : For a PPT algorithm A and any given x, the pair of accepting transcripts (a,e,z) and (a,e',z') for x where $e \neq e'$ gives w such that $(x,w) \in R$
–Special HVZK: There exists a simulator Sim^*such that for all $e, Sim^*(e) \rightarrow (a,z)$ such that (a,z) is having the same distribution as that of the real proof system provided the verifier is using the same challenge.

In the adaptive NIZK [25] both the prover and the verifier have access to the public set up, the CRS. Adaptive zero knowledge means that zero knowledge and soundness properties satisfy when the statements are chosen as a function of the CRS. If the statements selected are unbounded then it holds adaptive unbounded zero knowledge. The soundness property is defined in the non-programmable random oracle model.

Definition 2.3: A probabilistic polynomial time machine with the parameters $(GenCRS, P, V)$is said to be adaptive non interactive unbounded zero knowledge for a language L defined in NP with a relation R satisfying the conditions,

–Perfect completeness: For any randomly chosen $\rho \leftarrow GenCRS(1^n)$, for all $(x,w) \in R$ $Pr[V(x,\rho,P(x,w,\rho)) = 1] = 1$
–Adaptive Soundness defined in the non-programmable random oracle model: For every PPT function f and PPT P^*(cheating prover)
$Pr[V(\rho, f(\rho), P^{*F}(\rho)) = 1] \leq v(n)$, for all $n \in Z_q$ where
$f : \{0,1\}^n \backslash L \leftarrow \{0,1\}^{poly(n)}$ $v \leftarrow$negligible function
$F : \{0,1\}^n \leftarrow \{0,1\}^*$ any random function
$\rho \leftarrow GenCRS(1^n)$
–Adaptive unbounded zero knowledge: There exists a PPT simulator Sim for any NP language L and the set of relations R such that for every PPT function f defined as, $f : \{0,1\}^n \times \{0,1\}^{poly(n)} \cap R \leftarrow \{0,1\}^{poly(n)}$and for every PPT V^*(cheating verifier) the difference in probability is negligible. $Pr[V^*(Real_f(P^f(n,p))) = 1] - Pr[V^*(Sim_f(n,p)) = 1] \leq v(n)$

$Real_f(P^f(n,p))$ and $Sim_f(n,p)$ denotes the outputs from the real proofs and the simulated proofs.
Real Proofs: $Real_f(P^f(n,p))$

1.$\rho \leftarrow GenCRS(1^n)$,for all $n \in Z_q$
2.$\vec{x}, \vec{\pi}$ are initialized to null
for $i = 1$ to $p(n)$
(a)$x_i \leftarrow f_1(\rho, \vec{x}, \vec{\pi})$ (choosing the immediate x_i to be proven)
(b)$\pi_i \leftarrow P(\rho, fn_1(\rho, \vec{x}, \vec{\pi}), fn_2(\rho, \vec{x}, \vec{\pi}))$ (generating the i^{th} proof)
(c)The vectors,$\vec{x} = x_1, x_2, \ldots, x_i$ $\vec{\pi} = \pi_1, \pi_2, \ldots, \pi_i$
3.Return the output $(\rho, \vec{x}, \vec{\pi})$

Simulated Proofs: $Sim_f(n,p)$

1.$\rho \leftarrow Sim(1^n)$,for all $n \in Z_q$
2.$\vec{x}, \vec{\pi}$ are initialized to null
for $i = 1$to $p(n)$
(a)$x_i \leftarrow f_1(\rho, \vec{x}, \vec{\pi})$ (choosing the immediate x_i to be proven)
(b)$\pi_i \leftarrow Sim(x_i)$ (Simulator Sim generates the proof π_i for proving $x_i \in L$)
(c)The vectors,$\vec{x} = x_1, x_2, \ldots, x_i$ $\vec{\pi} = \pi_1, \pi_2, \ldots, \pi_i$
3.Return the output $(\rho, \vec{x}, \vec{\pi})$

Where fn_1 and fn_2 are the primary and secondary outputs of function f

Definition 2.4: A hybrid commitment scheme is a PPT algorithm with tuples $(GenCRS, Com, Sim_{com})$ defined as,

– $\rho \leftarrow GenCRS(1^n)$, for all $n \in Z_q$
– $(GenCRS, Com, Decom, RD_{com})$ For any message $l \in \{0,1\}^n$ computing a non-interactive perfect binding commitment $Com_\rho(l,k)$ and a decommitment $Decom_\rho(l,k)$ where k is any random number. The verification algorithm RD_{com} outputs, $l \leftarrow RD_{com_\rho}(Com_\rho(l,k), Decom_\rho(l,k))$ with high probability.
– (com, sim_{com}): For any PPT adversary A the outputs of $Real_{com}$ and Sim_{com} are computationally indistinguishable.

Real commitments: $Real_{com}, A(1^n)$

1.$GenCRS(1^n) \rightarrow \rho$
2.The vectors $\vec{c}, \vec{d}$ are initialized to null
for $i = 1$ to $p(n)$
(a)Choose $l_i \leftarrow A(\rho, \vec{c}, \vec{d})$
(b)$c_i = Com_\rho(l_i, k_i)$ for all $k_i \leftarrow \{0,1\}^{poly(n)}$
(c)$d_i = Decom_\rho(l_i, k_i)$
(d)Vectors $\vec{c} = c_1, c_2, \ldots, c_i$ and $\vec{d} = d_1, d_2, \ldots, d_i$
3.Return the output $A(\rho, l_1, l_2, \ldots, l_{p(n)}, \vec{c}, \vec{d})$

Simulated commitments: $Sim_{com}(1^n)$

1.$Sim_{com}(1^n) \rightarrow \rho$
2.The vectors $\vec{c}, \vec{d}$ are initialized to null
for $i = 1$ to $p(n)$
(a)Generate $c_i \leftarrow Sim_{com}$
(b)Choose $l_i \leftarrow A(\rho, \vec{c}, \vec{d})$
(c)$d_i = Sim_{com}(l_i)$
(d)Vectors $\vec{c} = c_1, c_2, ..., c_i$ and $\vec{d} = d_1, d_2, ..., d_i$
3.Return the output $A(\rho, l_1, l_2 ... l_{p(n)}, \vec{c}, \vec{d})$

The commitment scheme based on DDH assumption of Lindell is used for proving PoA. For the sake of completeness the scheme is explained as follows.

1.Run $G(1^n)$ for the public parameters(G, q, g, h)
(a)Perfect Binding
Choose ρ_1 and ρ_2 randomly from Z_q
Calculate $u = g^{\rho_1}$ and $v = h^{\rho_2}$
GenCRS is (G, q, g, h, u, v)
(b)Equivocal
Choose $\rho \in_R Z_q$
Calculate $u = g^\rho$ and $v = h^\rho$
AltCRS is (G, q, g, h, u, v)
2.Commitment
For committing $l \in \{0,1\}^n$
choose a random value $k \in_R Z_q$
Calculate $c_1 = g^k / u^l$ and $c_2 = h^k / v^l$
such that the commitment $c = (c_1, c_2)$
3.Decommitment
For decommiting $c = (c_1, c_2)$ provide l and k
4.RD_{com} The receiver outputs l if satisfy the equations $g^k = c_1 u^l$ and $h^k = c_2 v^l$ else return $\perp$.

In case 2(a) (g, h, u, v) is not a Diffie-Hellman tuple hence the commitment scheme is perfectly binding and in case 2(b) since (g, h, u, v) is a DH tuple the scheme is equivocal.

Using $\sum$ protocol for the relation R, non-interactive zero knowledge is obtained in the non- programmable random oracle model with CRS is depicted as follows. Let P_1 and P_2 be the prover algorithms and V be the verifier algorithm for $\sum$ protocol then,

1.$x \in L$ and the witness w , such that $(x, w) \in R$
2.$CRS : GenCRS(1^n) \rightarrow \rho$ and $s \leftarrow key$ for the hash function
3.Prover Side
(a)Calculate $a = P_1(x, w)$
(b)Calculate $c = Com_\rho(a, k)$
$d = Decom_\rho(a, k)$ where c and d are commit and decommit values respectively.
(c)Compute the challenge ,$e = hash_s(x, c)$
(d)Calculate $z = P_2(x, w, a, e)$
(e)The proof generated ,$\pi = (x, c, d, z)$
4.Verifier Side
(a)Calculate a from c and d, i.e. $a = RD_{com}(c, d)$
(b)Calculate $e = hash_s(x, c)$
(c)Return the output $V(x, a, e, z)$

3 Privacy Preserving Non-interactive Proof of Assets

The Bitcoin exchange should hold adequate measures to hide the total assets and users holdings.The exchange should maintain unlinkability from its Bitcoin addresses.In Dangher et al. scheme ,they introduced a privacy preserving proof of solvency for Bitcoin exchanges.The scheme is build on $\sum$ protocol and zero knowledge proofs.The protocol publicly proves its total assets and liabilities without revealing them. It also provides high confidentiality for user information .But proving the assets require an interaction between the exchange and the user.This will restrict the exchange to prove its asset independently.To the best of our knowledge there does not exist any privacy preserving proof of assets for Bitcoin exchanges in a non interactive manner.

3.1 PoA with Non Programmable Random Oracle

Provision [13] for exchanges can be made non-interactive using hybrid commitments in the NPRO model. In PoA protocol, the exchange constructs a large set of public

keys, PuK which is kept anonymous corresponds to the Bitcoin addresses appeared in the block chain. A commitment to its total asset is created by the exchange and proves in zero knowledge that the cumulative balance of all public keys the exchange owns is equivalent to the committed value by concealing the public keys it owns. The exchange gathers the set of public keys available in the Bitcoin blockchain.

$$PuK = (Y_1, Y_2, .., Y_n) \text{ where each } Y \in G$$

The size of PoA is directly proportional to the size of the anonymity set. Note that PoA is linear with respect to the number of public keys in the anonymity set. A reduction in proof size is possible by reducing the precisions. The Bitcoin addresses which are performing send action are suitable candidates for the anonymity set. The public key $Y_i = g^{x_i}$ where $x_i \in SK$, the set of secret keys for $i = 1$ to n.Consider the set S_B, the set of all Bitcoin addresses for which the exchange knows the private key such that $S_B \in PuK$. A Boolean set $s_i \in \{0,1\}$ is used to denote the accounts controlled by the exchange. We set the s_i value to one whenever E knows the secret key x_i corresponds to the public key Y_i. In Bitcoin no account can exist with a negative balance. For the balance $B(Y_i)$ the exchange's total asset is calculated as,1.Using range proof check whether the committed value lies in the interval $[0, 2^{51}]$.

$$TA = \sum_{i=1}^{n} s_i.B(Y_i), \forall i \in [1,n] \tag{1}$$

Compute B_i to form a DH tuple such that,2

$$B_i = g^{B(Y_i)}, \forall i \in [1,n] \tag{2}$$

The exchange E publishes the commitments for $s_i.B(Y_i)$, s_i and x_i as follows,

$$C_i = B_i^{s_i}.h^{r_i} \tag{3}$$

$$L_i = Y_i^{s_i}.h^{k_i} \tag{4}$$

The other way,

$$L_i = g^{x_i.s_i}.h^{k_i} \tag{5}$$

$$L_i = g^{x_i}.h^{k_i} \tag{6}$$

Where $r, k \in_R Z_q$ and $i \in [1,n]$

A commitment C_A for the total asset of the exchange is computed by performing homomorphic addition [41] of C_i.

$$C_A = \prod_{i=1}^{n} C_i = \prod_{i=1}^{n} B_i^{s_i} h^{r_i} = g^{TA} \times h^{\sum_{i=1}^{n} r_i} \tag{7}$$

It needs to prove in zero knowledge that the C_A computed in 7 is valid as well as knowledge of the exchange about the secret values s_i, r_i, k_i and x_i used in 1, 3, 5 and 6.From 3, 4 and 6 the verifier is convinced with the fact that when s_i is set to 1, the exchange is having the secret key x_i corresponds to the public key Y_i. It can be proven by dividing 4 by 6, results in $Y_i = g^{x_i}$. The protocol defined for PoA in NIZK is as follows,

Public Parameters: $G, g, h, C_i, L_i, B_i, Y_i$
Where $C_i = B_i^{s_i}.h^{r_i}$ $L_i = Y_i^{s_i}.h^{k_i}$ $B_i = g^{B(Y_i)}$ and $Y_i = g^{x_i}$
CRS Generation:$\rho \leftarrow (1^n), u, v$ and s where $u = g^{\rho}, v = h^{\rho}$ and s is the hash key

Prover Algorithm For $i \in [1,n]$

1.P chooses the random values $\alpha, \beta, \gamma, \delta$ and $t \in_R Z_q$
2.Calculates the a values

$$A_{1i} = B_i{}^{\alpha} h^{\beta}$$
$$A_{2i} = Y_i{}^{\alpha} h^{\gamma}$$
$$A_3 = g^{\delta} h^{\gamma}$$

3.Calculate the commitment for a
$Com_i = (C_{1i}, C_{2i}, C_{3i}, C_{4i}, C_5, C_6)$

$$C_{1i} = g^t / u^{A_{1i}} \quad C_{2i} = h^t / v^{A_{1i}} \quad C_{3i} = g^t / u^{A_{2i}}$$
$$C_{4i} = h^t / v^{A_{2i}} \quad C_5 = g^t / u^{A_3} \quad C_6 = h^t / v^{A_3}$$

4.Find the hash of the committed value Com_i
$e_i = H_s(Com_i) = H_s(C_{1i}, C_{2i}, C_{3i}, C_{4i}, C_5, C_6)$

5.Calculate the Z values,

$$Z_{1i} = \alpha + (e_i s_i)$$
$$Z_{2i} = \beta + (e_i r_i)$$
$$Z_{3i} = \gamma + (e_i k_i)$$
$$Z_{4i} = \delta + (e_i x_i)$$

6.Publish the values $(A_{1i}, A_{2i}, A_3, Z_{1i}, Z_{2i}, Z_{3i}, Z_{4i}, Com_i)$
Verifier Algorithm

Verifier accepts if,

$$B_i^{Z_{1i}} h^{Z_{2i}} = C_i^{e_i} A_{1i}$$
$$Y_i^{Z_{1i}} h^{Z_{3i}} = L_i^{e_i} A_{2i}$$
$$g^{Z_{4i}} h^{Z_{3i}} = L_i^{e_i} A_3$$

Compute commitment for Total asset of exchange,

$$C_A = \prod_{i=1}^{n} C_i$$

Using the protocol PoA the exchange proves its knowledge about the secret values s_i, r_i, k_i and x_i. We make use of a standard $\sum$ protocol to complete the proof. Since the protocol is HVZK (Honest Verifier Zero Knowledge), it conceals the total assets. The proof for the same is given below. The proof size is reduced by choosing common exponentiation for A_{1i}, A_{2i} and A_3 $\forall i \in [1,n]$. Using PoA the exchange proves its knowledge about the secret values.The PoA uses $\sum$ protocol to prove that each $s_i \in \{0,1\}$ which is known to the exchange.The protocol is made non-interactive using non-programmable random oracle model.It is therefore enough to prove that the protocol is honest verifier zero knowledge.

Theorem: For the publicly known values g, h, Y_i, B_i, C_i, L_i $\forall i \in [1,n]$,the $\sum$ protocol in PoA with Non Programmable Random Oracle is HVZK of the quantities $s_i \in \{0,1\}$and

$v_i, t_i, x_i \in Z_q \forall i \in [1,n]$ satisfying conditions (2),(4)and (6)$\forall i \in [1,n]$

Completeness: If the prover P and the verifier V follow the PoA protocol for the public inputs (g,h,Y_i,L_i,C_i,B_i) and the secret inputs (s_i,x_i,r_i,k_i) then V always accept the proof.

Proof: It is immediate. The exchange knows the public values from the block chain and it knows the secret values, for the random values α,β and γ and the hashed committed value e_i , it computes the proofs by following the protocol, thus V accepts.

Adaptive soundness According to definition 2.3 PoA protocol holds adaptive soundness.The $\sum = (P,V)$ be a sigma protocol for a relation R, with a perfect binding commitment *com* and the hash function $H : \{0,1\}^n \longleftarrow \{0,1\}^*$ in the non-programmable random oracle model.Then PoA with $\sum$ is a non interactive system holds adaptive soundness for the language L in CRS.

Proof: For any function f, the relation $R = \{(x, f(x))\}$ is equivocal on the pair $(x, O(x))$,where O represents the non-programmable random oracle model.If O is accessible by an adversary A ,then it is infeasible to get the string x such that $(x, O(x)) \in R$.Consider $x \notin L$ then according the soundness property of the $\sum$ protocol, for each $a, \exists e \in \{0,1\}^n$ such that, for some z the verifier is accepting (a,e,z).
Define the hash function with secret key s , $H_s(x,com) = e$,where there exists the values (a,r,z) such that $com = com(a:r)$ and the verifier $V(x,a,e,z) = 1$.Since $x \notin L$ and *com* is perfectly binding, only one e value exists which fulfils this property.Thus concludes that H is the required function.Since H is the function for the relation $R = \{(x,com), H(x,com\})$ which is equivocal .That is no polynomial time adversary can find a pair (x,com) such that $O(x,c) = H(x,c)$ .So by contradiction, for a PPT function f and a cheating prover P satisfies $V(f(\rho_n),\rho_n,P(\rho_n)) = 1$ with probability P (ρ is calculated as $GenCRS(1^n) \rightarrow \rho$).

Honest Verifier Zero Knowledge (HVZK): For a PPT simulation S the inputs $(g,h,Y_i,B(Y_i),L_i,C_i)$ and $e_i \in_R Z_q$ for $i \in [1,n]$ produce a transcript with same distribution as that of the transcript generated between the prover and the honest verifier.

Proof: For a given simulator, the real value and the simulated value follows uniform distribution for $e_i \in_R Z_q$. For random $\alpha,\beta,\gamma,\delta$ values, the z values are uniform in Z_q. Since the distribution are the same, the real and the simulated transcripts hold equal probability. The simulator does the follows,
For $i = 1$ to n

1.Select $Z_{1i}, Z_{2i}, Z_{3i}, Z_{4i}$ and $e_i \in_R Z_q$
2.Assign

$$A_{1i} \leftarrow B_i^{Z_{1i}}.h^{Z_{2i}}.C_i^{-e_i}$$
$$A_{2i} \leftarrow Y_i^{Z_{1i}}.h^{Z_{3i}}.L_i^{-e_i}$$
$$A_3 \leftarrow g^{Z_{4i}}.h^{Z_{3i}}.L_i^{e_i}$$

3.Publish the transcript,$(A_{1i}, A_{2i}, A_3, e_i, Z_{1i}, Z_{2i}, Z_{3i}, Z_{4i})$

PoA admits only one to one mapping between public keys and the Bitcoin addresses. Used Bitcoin addresses are members of the anonymity set. Thus the exchange proves its total assets using PoA. If the exchange is well enough to calculate the proof of liabilities, a commitment for its total liabilities, it is easy to prove that the exchange is solvable.

4 Results and Discussions

The protocol is designed in the non programmable random oracle(NPRO) model to obtain the non-interactive nature. The FS transform is sound only in the random oracle model.Hence considered non programmable random oracle model using hybrid commitments for proving the assets in a non-interactive way. The PoA with NPRO is straight forward to parallelize, since almost all parts of the protocol is linear in nature. This will improve the running time of the protocol. The protocol appears to be perfectly separable with unique and independent component for each address in the address set.Much computation is not required apart from the commitment calculation compared to Dagher et al.'s scheme . A total of six components are part of the final commitment out of that two are calculated only once.Anonymously the user can check whether his balance is added to the total liabilities.The hash function used in the proposed protocol provides integrity for the commitment which is lacking in the Dangher et al. scheme. The commitments helps in balancing the non-interactive nature of the protocol.Since the protocol is HVZK, it conceals about the exchange's total assets,the secret value x_i and s_i.
The protocol performance is tested with the prototype implemented in java 1.8.All cryptographic executions are achieved using the standard java library called BouncyCastle.We tested with an anonymity set of $1000-5000$ public keys .The protocol is versatile even for huge anonymity set.The proof size and the computation time of the protocol is compared with the interactive protocol proposed by Dagher et .al without considering the CRS generation are shown in figure2 and in figure3.The proof size includes the construction and verification time.The outcome shows that the proposed protocol gives better performance compared to interactive protocol since for large exchanges network latency plays a major role in completing the proof.

5 Conclusion

Bitcoin is going to be the potential candidate for common medium of exchange all over the world.The wide

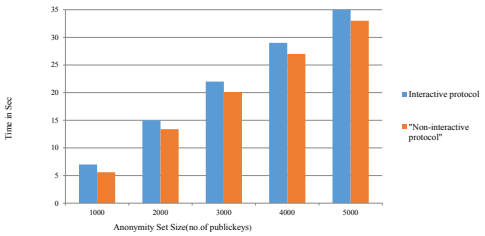

Fig. 2: Execution Time Comparison

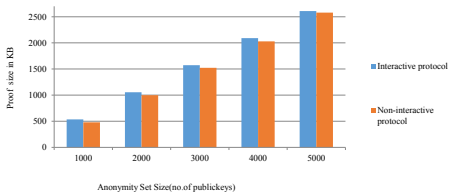

Fig. 3: Proof Size Comaprison

acceptance of bitcoin increases its value in the current economy.The trading of various goods will be achieved using bitcoin.This may reduce the demand for using exchanges, as the requirement for using fiat currency against bitcoin reduces.However, cryptoexchanges come into existence for trading among various cryptocurrencies.So the requirement for preserving the privacy of the users still exists and that demands the proposed scheme.The PoA protocol enables the exchange to prove its assets in zero knowledge to any verifier. Dangher et al.scheme is made non-interactive using non-programmable random oracle model using the hybrid commitment scheme.We have seen the pros and cons in using FS transform in the random oracle model .The PoA protocol with non programmable random oracle helps in publishing the proof without any verifier interaction. The exchange's privacy is preserved without any complex computation. For better efficiency, it is advisable to choose smaller anonymity set instead of the set of all public keys in the Bitcoin block chain. Protection of the secret keys is of utmost importance, failing which will lead to exchange bankruptcy. Access control of the keys needs to be practiced to conducting the proof in a regular span of time. By using an alternate $\sum$ protocol, non-interactive zero knowledge proof is achieved in the non-programmable random oracle model.

Acknowledgement

The first author acknowledges the valuable suggestions from the co-author for furnishing the article.
The authors are grateful to the anonymous referees for a careful checking of the details and for helpful comments that improved this paper.

References

[1] M.Belenkiy,E-cash, In Handbook of financial Cryptography and Security, CRC, 4-48 (2011)
[2] R.Parhonyi, Micropayment Systems, In Handbook of financial Cryptography and Security, CRC, 161-183(2011)
[3] S.Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Consulted **1**, 2012(2008)
[4] T.Okamoto and K.Ohta, Universal electronic cash, In CRYPTO 91, **576** of LNCS, 324-337(1992)
[5] Joseph Bonneaue, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A.Kroll, Edward W.Felten, SoK:Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, IEEE Symposium on Security and Privacy 2015, 104-121(2015)
[6] S.Eskandari, D.Barrera, E.Stobert and J.Clark, A first look at the usability of bitcoin key management, In workshop on Usable Security (2015)
[7] C.Herley and P.C van Oorschot, A research Agenda Acknowledging the Persistence of Passwords, IEEE Security and Privacy, **10(1)**, 28-36(2012)
[8] Litke .P and Stewart .J, Cryptocurrency-stealing maiwarelandscape, Technical Report, Dell SecureWorks Counter Threat Unit (2014).
[9] Goldfeder .S , Gennaro .R, Kalodner .H, Bonneau .J, Felten E.W, Kroll J.A and Narayanan .A, Securing bitcoin wallets via a new DSA/ECDSA threshold signature scheme Proceedings of Applied Cryptography and Network Security, 156-174 (2016).
[10] Ro .S, A Bloomberg TV Host Gifted Bitcoin on Air And It Immediately Got Stolen, Business Insider (2013).
[11] Wilcox.Z, Proving your bitcoin reserves2014, https://iwilcox.me.uk/2014/proving-bitcoin-reserves.
[12] Merkle R.C, Secrecy,Authentication and Public Key Systems , Ph.D.theis, Stanford University (1979).
[13] Gaby G. Dagher, Benedikt Bunz, Joseph Bonneau, Jerry Clark, Dan Boneh, Provisions: Privacy preserving proofs of solvency for Bitcoin Exchanges, ACM CCS 2015, 720-731 (2015)
[14] Androulaki.E, Karame G.O, Roeschlin.M, Scherer.T and Capkun.S, Evaluating User Privacy in Bitcoin, In Financial Cryptography and Data Security, 34-51 (2013)
[15] Damgard .I, On the Existence of Bit Commitments Schemes and Zero Knowledge Proofs, In CRYPTO'89, Springer-Verlag(LNCS **435**), 17-27 (1989)
[16] Dodis. Y, Shoup.V and Walfish.S, Efficient Constructions of Composable Commitments and Zero knowledge Proofs, In CRYPTO 2008, Springer (LNCS **5157**), 515-535(2008)

[17] Caetti.R, Goldreich.O and Halevi.S, The Random Oracle methodology, Revisited, In the 30th STOC'98, 209-218 (1998)
[18] Rafael Pass, On deniability in the common reference string and the random oracle model, In advances in Cryptology-CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, 316-337 (2003).
[19] Alfredo De Santis, Silvio Micali and Giuseppe Persiano, Non-interactive zero knowledge proof systems ,In advances in cryptology-CRYPTO7,A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, pp.52-72 (1987).
[20] Silvio Micali, Computationally sound proofs, SIAM Journal on Computing, **30(4)**, 1253-1298 (2000).
[21] Meiklejohn. S, Pomarole .M, Jordan .G,Levchenko.K , McCoy .D,Voelker G.M and Savage.S, A fistful of bitcoins: characterizing payments among men with no names , Stefan Savage Communications of the ACM, **59(4)**, 86-93 (2013)
[22] Conference of State Bank Supervisors, State Regulatory Requirements for Virtual Currency Activities Model Regulatory Framework (2015)
[23] Feige.U and Shamir.A, Witness indistinguishable and witness hiding protocols, In ACM STOC'90 , 416-426(1990)
[24] Damgard .I, Catalano and Ivan Visconti, Hybrid commitments and their applications to zero-knowledge proof systems, Theoretical Computer Science, **374(1-3)**, 229-260(2007)
[25] Yehuda Lindell, An efficient transform from Sigma protocols to NIZK with CRS and non-programmable random oracle, In theory of cryptography-12thThoery of Cryptography conference, TCC 2015 Proceedings, Part 1,93-109 (2015)
[26] Pedersen T.P, Non-interactive and information-theoretic secure verifiable secret sharing ,: Advances in Cryptology CRYPTO 91, 129-140 (1991)
[27] Boneh. D,1998 Decisional Diffie-Hellman Problem, In Proceedings of the 3rd Algorithmic Number Theory Symposium (Springer LNCS), **1423**, 48-63 (1998)
[28] Damgard .I, Commitment Schemes are Zero Knowledge Protocols, Proceedings of Lectures on Data Security, Springer (LNCS), 63-86 (1999)
[29] Jarecki.S and Shmatikov.V, Efficient Two-Party Secure Computation on Committed Inputs, In EUROCRYPT 2007, Springer (LNCS **4515**), 97-114(2007)
[30] Lindell .Y and Pinkas.B, Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer, In Journal of Cryptology, **25(4)**, 680-722 (2012)
[31] Yehuda Lindell , Fast Cut-and-Choose Based Protocols for Malicious and Convert Adversaries, In CRYPTO 2013, Springer (LNCS **8043**), 1-17 (2013)
[32] Schoenmakers .B and Tuyls.P, Practical Two-Party Computation Based on the Conditional Gate, In ASIACRYPT 2004, Springer(LNCS **3329**), 119-136(2004).
[33] Damgard.I, On $\sum$ Protocols2010, http://www.daimi.au.dk/ ivan/sigma.pdf.
[34] Goldreich.O and Kalai .Y, Definitions and Properties of Zero-Knowledge Proof Systems, Journal of Cryptology,**7(1)**, 1-329(1994)
[35] Shafi Goldwasser and Michael Sipser, Private coins versus public coins in interactive proof systems, Proceedings of ACM STOC'86, 58-68 (1986)
[36] Amos Fiat and Adi Shamir, How to prove yourself:Practical solutions to identification and signature problems, In Advances in Cryptology,CRYPTO '86, 186-194 (1986)
[37] Michele Ciampi, Giuseppe Persiano, LuisaSinscalchi and Ivan Visconti, A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracle, 13th International Conference TCC 2016-A, Springer (LNCS **9563**), 83-1139(2016)
[38] Damgard .I, Efficient Concurrent Zero-Knowledge in the Auxiliary String Model , In EUROCRYPT 2000, Springer (LNCS **1807**), pp.418-430 (2000)
[39] Dodis.Y, Shoup.V and Walfish.S, Efficient Constructions of Composable Commitments and Zero-Knowledge Proofs, In CRYPTO 2008, Springer(LNCS 5157), 515-535 (2008)
[40] Pass.R, On Deniability in the Common Reference String and Random Oracle Model, In CRYPTO 2003, Springer(LNCS **2729**), 316-337 (2003)
[41] Monique Ogburn, Claude Turner and PushkarDahal, Homomorphic Encryption, Procedia Computer Science **20**, 502-509 (2013)

Maya Mohan received her M.Tech degree in Computer Science and Engineering from NIT, Trichy. Currently doing her research in information security under Anna University, Chennai. She is working as Assistant Professor in Department of Computer Science and Engineering, NSSCE, Palakkad, Kerala. Her research interests are in the areas of cryptography, zero knowledge proofs and network security.She has published research articles in reputed international journals including mathematical and engineering sciences.

M. K. Kavitha Devi is Associate Professor of department of Computer Science and Engineering. She received her B.E. and M.E. in Computer Science and Engineering in 1994 and 2004 respectively .She obtained her Ph.D. in Information and Communication Engineering from Anna University chennai in 2011 . Her research interests are Recommender Systems, Cloud Computing, Theoretical Computation,Information Security and Steganalysis. She has more than 50 publications in reputed International Conferences and refereed Journals. She is an active reviewer in refereed Journals including IEEE, Springer, and Elsevier.She is a pride recipient of the Best Computer Science Faculty Award of ASDF Global in year 2014. She was the editor for the National Conference proceedings of NCSMAC 2016. She is currently guiding 10 Ph.D. scholars in her research area.