Peer-to-peer Electronic Cash Using Identity Based Signcryption

Dany Eka SAPUTRA, Sarwono SUTIKNO, and Suhono Harso SUPANGKAT

School of Electrical Engineering and Informatics,
Institut Teknologi Bandung, Bandung, Indonesia
dekastra@gmail.com

Abstract: Indonesia e-cash system faced with some challenges. Lack of proper network infrastructure impedes the distribution of e-cash throughout the country. Most existing e-cash scheme designed for usage with proper network infrastructure, mainly for validating the transaction. Existing peer-to-peer e-cash scheme also require proper network infrastructure, either for public key request or deposit the received e-cash. This paper proposed a novel e-cash scheme by building its e-cash data as chain of transaction (block chain) using identity-based signcryption as its security mechanism. The combination of block chain and identity-based signcryption make the e-cash peer-to-peer, transferable, and able to operate on ad hoc network. The Markov chain evaluation show that the proposed scheme can achieve security against forgery and double spending.

Keywords: electronic cash, peer-to-peer, identity-based cryptosystem, signcryption.

1. Introduction

The usage of electronic cash (hence referred to e-cash) in Indonesia has not evenly distributed throughout the nation. The Central Bank of Indonesia records that the total e-cash transaction in 2017 reaches IDR 12 trillion [1], which almost equal to the Indonesia's 2017 GDP of IDR 13 trillion [2]. However, that amount only contribute to 0.2% of Indonesia's money supply in the same year [3]. The uneven distribution of e-cash can be seen from the number of e-cash instrument in 2017. The Central Bank of Indonesia records approximately 90 million unit of e-cash is circulated in 2017, which is only 34% of Indonesia populations.

The condition of Indonesia's internet network contributes to the uneven distribution of e-cash. Most of Indonesia e-cash system is an online system, the system needs to contact the issuer of e-cash at the time of transaction. An annual survey from Indonesia Internet Service Provider Association (APJII) in 2017 shows that the internet penetration level in Indonesia has reach 54.46% [4]. However, 58.08% of internet user are in Java region, while other regions only contribute around 5-20% to the total user. Because the network infrastructure itself is not evenly distributed, the e-cash can only be used in certain area of Indonesia.

The e-cash scheme can be categorized into two general paradigms: the centralized and decentralized (distributed) paradigm [5]. The difference between the two lies in the existence of single authorization entity in the system (usually known as Trusted Third Party/TTP or the Issuer). Indonesia e-cash scheme fall into the centralized paradigm. All scheme in Indonesia has its own TTP and most of it is online scheme.

It is more suited to implement decentralized e-cash in Indonesia, which does not have a TTP in its scheme. Scheme such as [6] [7] [8] [9], does not require TTP to operate. Thus, eliminating the needs to contact TTP at the time of transaction. However, decentralized e-cash can not be implemented in Indonesia as an exchange tool in a legal transaction under the current regulation. Beside regulation aspect, these decentralized schemes are network dependent. The scheme still requires the network to broadcast it transaction to all the user for validation. For example, TTP in Zerocash [9] is only needed for creating the user's key pair. The rest of the operation does not need the TTP. However, Zerocash is built on top of Bitcoin [6]. Instead of contacting the TTP for validation, it broadcast the transaction data to most of the user, so the transaction will be validated and recorded in the block chain.

Received: April 20th, 2017. Accepted: June 20th, 2018
DOI: 10.15676/ijeei.2018.10.2.13

There are several offline schemes under centralized paradigm, which does not require TTP's presence at the time of transaction. Scheme such as [10] [11] [12] enables an user to use e-cash in a transaction with a merchant without the involvement of TTP for transaction validation. The schemes provide protection against double spending, which is a crucial point for an offline scheme. Although these schemes seem perfect to tackle Indonesia e-cash problem, it still unsuited under lack of network infrastructure. After the transaction, the merchant needs to contact the TTP to deposit the received e-cash. This process exchanges the e-cash with real cash for the merchant. If the merchant does not deposit the e-cash, he/she can not use the e-cash for another purpose. Under this condition, the scheme still requires proper network infrastructure to operate.

Several centralized schemes do not need to deposit their e-cash after transaction. Scheme with transferable e-cash [13] enables the receiver to immediately use the received e-cash in another transaction. The transferable property could reduce the need of using proper network infrastructure in e-cash scheme operation. However, transferable e-cash usually uses public key cryptography as its main security mechanism. Public key cryptosystems must be operated with proper network infrastructure, especially when requesting a user public key.

The existing schemes mainly build with the assumption of there is a proper network infrastructure. Therefore, the existing schemes is not suitable to Indonesia implementation. A new scheme of e-cash needs to be designed for a condition without proper network infrastructure. A scheme can operate under ad hoc network when it has both the transferable and peer-to-peer property and implementing offline cryptosystem. From the previous explanation, many of existing schemes does not meet this requirement.

The proposed scheme aims to fulfill the gap in e-cash research for implementation in Indonesia, as explained above. It is built to minimize the need for proper network infrastructure (an ad hoc network between the user and the merchant still needed for transaction). The goal is achieved by using two methods. First, to eliminate the need to contact TTP at transaction time, the scheme deploys the identity-based signcryption as its signature scheme. Second, the scheme is built as transferable e-cash to minimize the need to deposit the received e-cash, so the receiver can use the e-cash in another transaction.

2. Proposed Electronic Cash Scheme

The development of the proposed scheme uses reference from the General Money Model [14]. The scheme uses the term from the model to determine data used in this scheme, such as holder function and value function. The scheme defines the medium (m) of e-cash as a chain of transaction block. A transaction block (T_i) is a tuple of data that define a transaction. The transaction block is defined as:

$$T_i = \left(ID_{h'}, v, H(T_{i-1}), Sigc_h^{h'}\left(ID_{h'}, v, H(T_{i-1})\right)\right) \quad (1)$$

where $ID_{h'}$ is the identity string (public key) of opposing party in a transaction, v is the value of e-cash in a holder possession after a transaction with opposing party ($v \in \mathbb{Z}^+$), $H(T_{i-1})$ is hash value of previous transaction of a holder, and $Sigc_h^{h'}$ is signcryption [15] of block data using both party's keys. The proposed scheme uses identity-based signcryption [16] as its signature scheme. Identity-based cryptosystem does not require a Certificate Authority (CA) to operate. By using this scheme, there is no need to contact the CA at the time of transaction to conduct digital signature operation.

In Equation 1, it is stated that each transaction block contain data from previous transaction. Each transaction block form chain with each other. This concept of chain is similar to the concept of chain in Bitcoin [6]. Figure 1 describe the transaction block chain. Each time a holder conducts a transaction with another holder, a block is added at the end of their chain. The first block (T_0)is a special block that created by the issuer when a user requests an e-cash. Each holder keeps their own chain as a medium to store value. The scheme's value function can be defined as:

$$\mathrm{vf}(m) = T_i \quad (2)$$

Each transaction block represents the value function which map money value to a holder. The latest block in the chain represent the current valid value function. Model in [14] also defines a holder function, a function that map each medium to its holder. In this scheme, holder function is represented by signcryption ($Sigc_h^{h'}$):

$$\mathrm{hf}(m) = Sigc_h^{h'} = Signcrypt(T_i, ID_{h'}, S_h) \quad (3)$$

whit S_h is medium holder's private key. By using this holder function, an entity can define who is the legitimate holder of a medium.

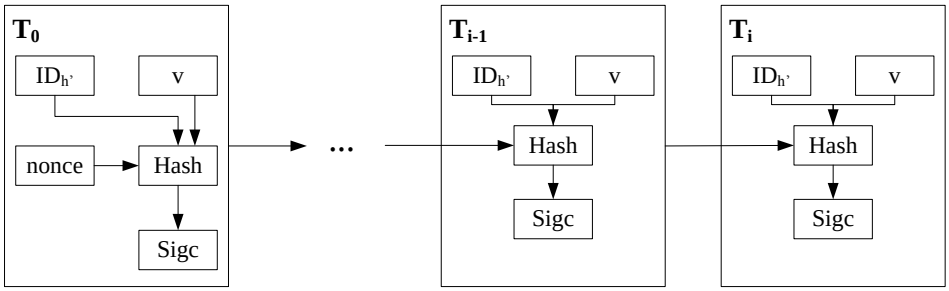

Figure 1. Transaction Block Chain

To preserve the integrity of transaction block chain, a holder keeps another data called hash root. Hash root is a chain of hash in form of a tree, also known as Merkle Tree [17]. Similar concept is used by Bitcoin [6] to shorten their transaction data in the block chain. In this scheme, the hash root is defined as:

$$H_{root} = \left(H_{root-1} \parallel H(T_i)\right) \quad (4)$$

Symbol ‖ is used to define a concatenation A Hash root is a hash value of previous hash root with the hash value of the recent transaction block. The property of Merkle Root enables us to verify if for any T_i in a chain is an element of H_{root} ($T_i \in H_{root}$).

The proposed scheme works under Centralized Paradigm [5], which has a single authority that oversee the entire system. This authority is called Trusted Third Party (TTP), responsible for issuing key pair to holder, issue new e-cash, and mediating dispute between holder. However, TTP will not be involved in a transaction. The responsibility to verify a transaction is delegated to each holder involved in transaction.

The proposed scheme differentiate holder between the using holder and the receiving holder. The holder that use e-cash in transaction is called Payer. While holder that receive the e-cash is called Payee. Payer is symbolized by h, while Payee is represented by symbol h'. The relationship between each holder and TTP can be seen in Figure 2.

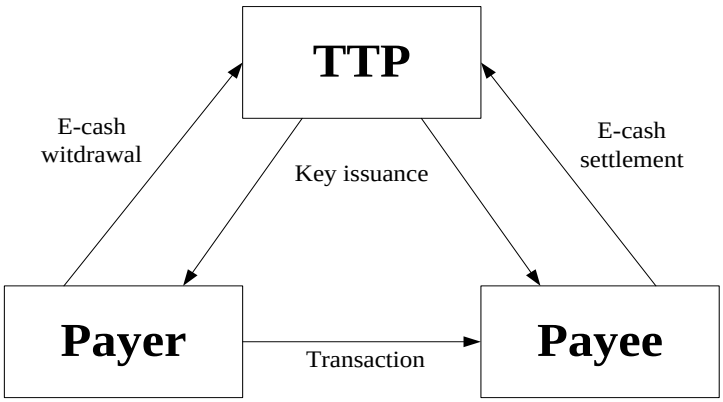

Figure 2. Relationship between entities

The proposed scheme consists of 6 protocols: SETUP, EXTRACT, WITHDRAW, TRANSACTION, DISPUTE, and SETTLEMENT. Each protocol is used to achieve specific goal related to a process in e-cash usage. Each protocol involves specific entities in its process. In describing each protocol, the process of decrypt and verify the signcryption is not explained in detail. However, the parameters needed in this process are still defined as part of the system setup. The next part of this paper describes each protocol in more detail.

A. SETUP Protocol

The SETUP protocol is used by the TTP to establish the e-cash system. In this process, TTP set the system parameters and set TTP public and private keys. The system parameter mainly used to establish variables used in signcryption, therefore the protocol is adopting the SETUP algorithm in [16] with some additional steps to add variables. The SETUP protocol is conducted as follow:

1) Select additive group G_1 and multiplicative group G_2. Both groups are cyclic group of prime orders of q.
2) Select P as a generator of G_1.
3) Select a pairing function $\hat{e}: G_1 \times G_1 \rightarrow G_2$ which satisfy bilinear and non-degenerate condition.
4) Select hash function $H_1: \{0,1\}^* \rightarrow {G_1}^*$, $H_2: \{0,1\}^* \rightarrow \mathbb{Z}_q$, $H_3: {\mathbb{Z}_q}^* \rightarrow \{0,1\}^n$, and a secure hash algorithm H_4, where $n \in \mathbb{Z}$ is length of message to be signcrypted.
5) Choose a random $t \in {\mathbb{Z}_q}^*$ and keep as system's private key.
6) Calculate $Q_{TA} = t.P$ as system's public key.
7) Set system parameter Param $= (P, \hat{e}, H_1, H_2, H_3, H_4, Q_{TA})$ and publish the parameter.
8) Run EXTRACT protocol to achieve TTP's public and private key.

All variables in system parameter, except for H_4, are parameters for making and verifying the signcryption. These parameters are not explicitly used in next protocols. They are used implicitly if the protocol uses signcryption.

B. EXTRACT Protocol

EXTRACT protocol generates key pair for user. This protocol executes the extract algorithm in [16]. New user contact TTP to execute this protocol and receives public and private key. EXTRACT protocol can also be used to renew private key, in case of user lost his/her private key. A user's public key is symbolized by ID_u, where subscript u denote the owner of key. While user's private key is symbolized by S_u.

C. WITHDRAW Protocol

This protocol is conducted by Payer and TTP. It goals is to generate new e-cash for Payer or adding e-cash value of existing Payer. In this protocol, there is a small step difference between new Payer or existing Payer. For existing Payer, all existing transaction chain is extracted from Payer's device before adding new value. At the end of protocol, both new and existing Payer will receive new transaction block which replace old transaction chain. We called this new transaction block as Genesis Block (T_0). We can see in Figure 1, Genesis Block always placed in the beginning of each transaction block chain.

WITHDRAW protocol is conducted in these steps, with the summary of this protocol can be seen in Figure 3.

1) For existing Payer, send $(H_{root}, T_0, T_1, \dots, T_i)$ to TTP, where subscript i denote the last transaction in Payer medium.
2) TTP check the validity of $(H_{root}, T_0, T_1, \dots, T_i)$. If valid proceed to next step, else reject the request and abort protocol.
3) Payer (new & existing) request new e-cash of value v to TTP.
4) TTP calculate new e-cash value $v_h = v_o + v$, where v_o is old e-cash value for existing Payer. For new Payer $v_o = 0$.

5) TTP choose a nonce N_0 and calculate $H_0 = H_4(ID_{TTP} \parallel v_h \parallel N_0)$.
6) TTP form genesis block $T_0 = \left(ID_{TTP}, v_h, N_0, Sigc^h_{TTP}(H_0)\right)$.
7) T_0 is sent to Payer.
8) Payer replace his/her transaction block chain (if any) with T_0, and calculate $H_{root} = H_4(T_0)$.

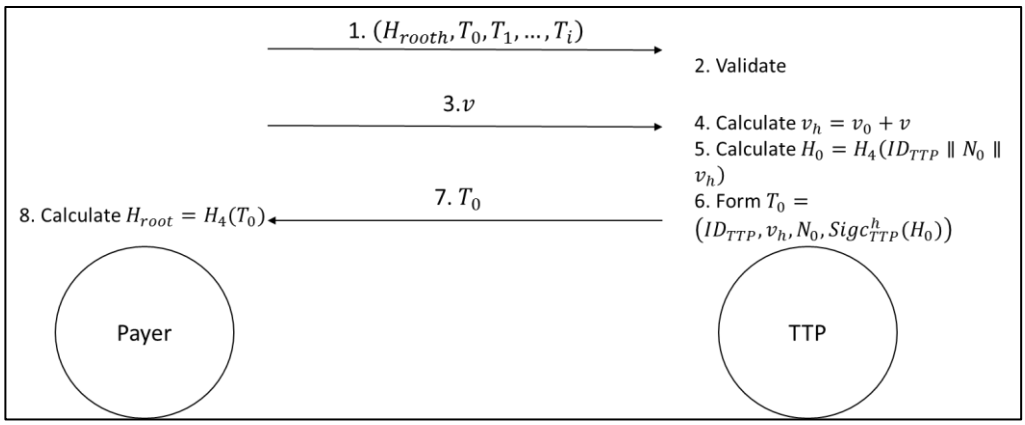

Figure 3. WITHDRAW Protocol

D. TRANSACTION Protocol

TRANSACTION protocol regulates the process of transferring e-cash from Payer to Payee. This protocol is conducted between Payer and Payee as peer-to-peer connection without the need to contact TTP. Payer and Payee validate each other transaction block chain as part of protocol. This protocol is conducted with these steps (See Figure 4):

1) Payee sent his/her identity string (public key) $ID_{h'}$ to Payer.
2) Payer sent $Sigc^{h'}_h(T_{h-1}, ID_h, N_h, H_{rooth})$ to Payee, where N_h is nonce choosen by Payer.
3) Payee open and validate $Sigc^{h'}_h$, if valid send $Sigc^h_{h'}(T_{h'-1}, (N_h - 1), H_{rooth'})$.
4) Payer open and validate $Sigc^h_{h'}$, if valid calculate new Payee's new e-cash value $v_{h'} = v_{h'-1} + v$, where v is the value of e-cash transferred between Payer and Payee.
5) Payer calculate $H(T_{h'}) = H_4\left(ID_h \parallel v_{h'} \parallel H_4(T_{h'-1})\right)$ and send $Sigc^{h'}_h\left(H(T_{h'})\right)$ ke Payee.
6) Payee validate $Sigc^{h'}_h\left(H(T_{h'})\right)$. Then set new transaction block $T_{h'} = \left(ID_h, v_{h'}, H(T_{h'}), Sigc^{h'}_h\left(H(T_{h'})\right)\right)$.
7) Payee calculate new hash root $H_{rooth'} = H_4\left(H_{rooth'-1} \parallel H_4(T_{h'})\right)$.
8) Payee calculate new e-cash value for Payer $v_h = v_{h-1} + v$.
9) Payee calculate $H(T_h) = H_4\left(ID_{h'} \parallel v_h \parallel H_4(T_{h-1})\right)$ and send $Sigc^h_{h'}\left(H(T_h)\right)$ to Payer.
10) Payer validate $Sigc^h_{h'}\left(H(T_h)\right)$, then set new transaction block $T_h = \left(ID_h, v_h, H(T_h), Sigc^h_{h'}\left(H(T_h)\right)\right)$.
11) Payer calculate new hash root $H_{rooth} = \left(H_{rooth-1} \parallel H_4(T_h)\right)$.

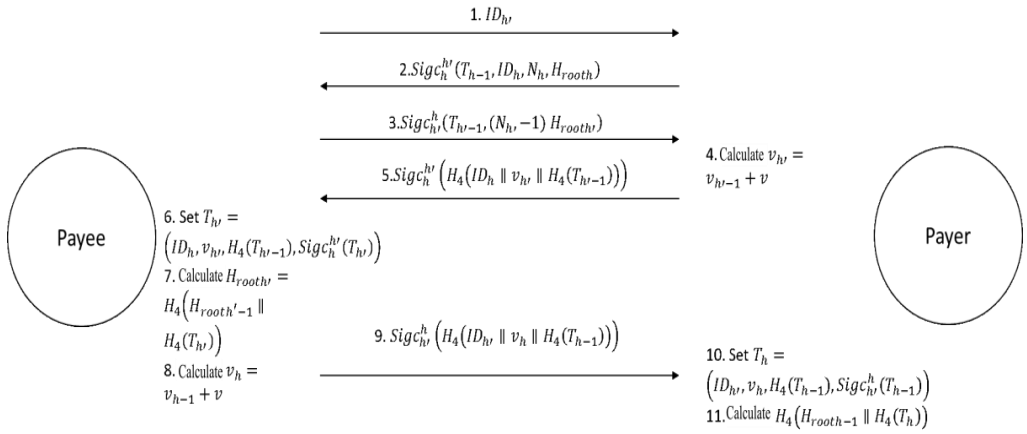

Figure 4. TRANSACTION Protocol

E. DISPUTE Protocol

When Payer and Payee have a dispute over a past transaction, TTP will mediate the transaction using DISPUTE protocol. There are 2 scenarios of dispute covered in this protocol. First is a user deny a transaction in which he/she was legally involved, if effect demand that transaction deemed invalid. Second scenario is when a user unknowingly involved in a non-exist transaction and want to prove that the transaction is invalid. To solve this dispute, TTP will use these steps.

1) TTP extract the disputed transaction block and hash root from each user in dispute $(T_h, T_{h'} H_{rooth}, H_{rooth'})$.
2) TTP check $H_4(T_u) \in H_{rooth}$.
3) TTP validate $Sigc_u^{u'}$.
4) To settle first scenario of dispute and retain non-repudiation, the result must satisfy $(H_4(T_u) \in H_{rootu}) \wedge \left(validate\left(Sigc_u^{u'}\right) = (ID_{u'}, S_u)\right)$.
5) To settle second scenario of dispute and retain non-repudiation, the result must satisfy $(H_4(T_u) \notin H_{rootu}) \vee \left(validate\left(Sigc_u^{u'}\right) \neq (ID_{u'}, S_u)\right)$.

F. SETTLEMENT Protocol

SETTLEMENT protocol is used when a user wants to exchange his/her e-cash into cash. This protocol is the reverse of WITHDRAW protocol. SETTLEMENT protocol is conducted by a user and TTP. The step is as follow (see Figure 5).

1) User sent $(H_{root}, T_0, T_1, \ldots, T_i)$ to TTP
2) TTP validate the hash root and transaction chain. If any variable is not valid, TTP will abort the process. Otherwise, proceed to next step.
3) User sent value to be settled v to TTP.
4) TTP calculate new balance for user, $v_u = v_o - v$ where $v \leq v_o$.
5) TTP calculate hash $H_0 = H_4(ID_{TTP} \parallel N_0 \parallel v_u)$.
6) TTP forms genesis block $T_0 = \left(ID_{TTp}, v_u, N_0, Sigc_{TTP}^{u}(H_0)\right)$.
7) TTP send T_0 to user.
8) User replace his/her transaction block chain with genesis block T_0, and calculate new hash root $H_{root} = H_4(T_0)$.

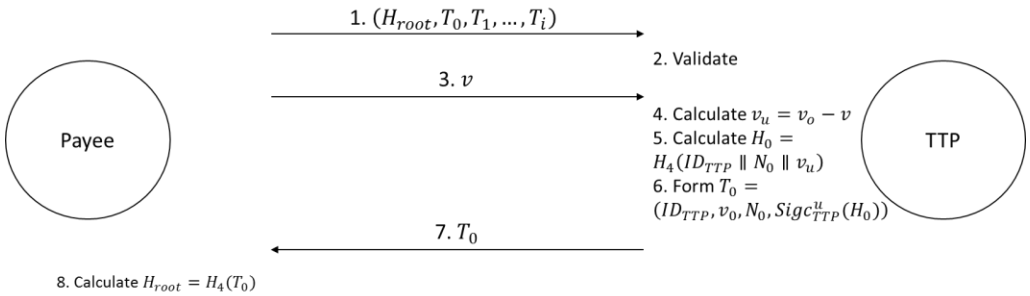

Figure 5. SETTLEMENT protocol

3. Analysis of E-cash Scheme

A. Protocol Performance Analysis

The security of the proposed scheme relies on the security of the signcryption scheme. For an adversary to be able to forge or to double spend T_i, he/she must be able to forge the signcryption used in T_i. The security of identity-based signcryption has been proved in [16] to fulfill the *existential unforgeability of identity-based signcryption under adaptive chosen message attack* definition.

A protocol performance evaluation is conducted by using Markov Chain technique. This action aims to prove that the TRANSACTION protocol in the proposed scheme does not have deadlock and will always ends in its ending state. The Markov Chain technique can also prove that the probability of forgery and double spending is acceptable. This evaluation method is similar with the work of Dreier et al. [18] where they evaluate the security of e-cash by using Pi-Calculus. However, their definition of forgery and double spending is slightly differed from what used in this paper. This paper uses the definition defined in [14] that define the forgery and double spending separately. The forgery definition used in [18] is part of double spending in this paper's definition.

The evaluation process only analyzes the TRANSACTION protocol because it is the only protocol which TTP is not involved, thus having the greatest risk. To prove that the proposed scheme is secure and correct, it needs to prove that the transaction of e-cash can be conducted securely. To conduct the evaluation, the protocol is transformed into a state diagram, shown in Figure 6.

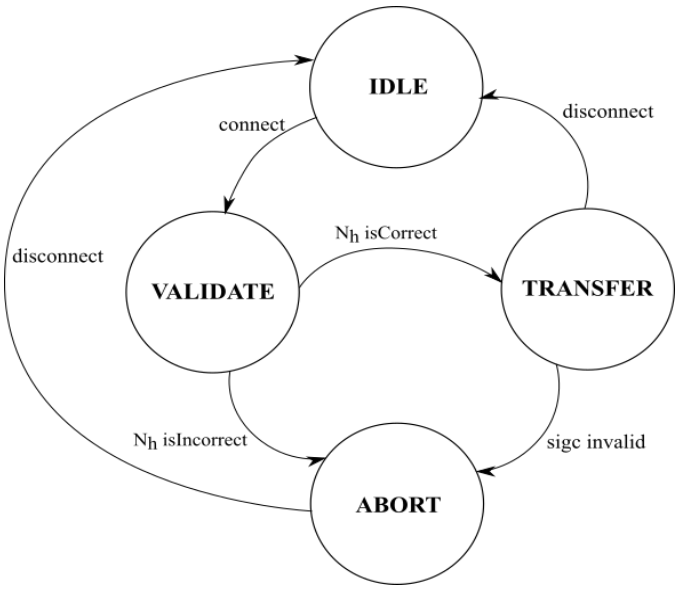

Figure 6. State diagram of TRANSACTION protocol

From the state diagram in Figure 6, transition matrix can be made. The transition matrix describes the probability of transition between states. By using the transition matrix, it is possible to calculate the probability of TRANSACTION protocol ends in its designated states, whether in IDLE or ABORT, after the normal number of steps. The transition matrix (tm) for TRANSACTION protocol can be described as follow.

$$tm = \begin{array}{c} \\ I \\ V \\ T \\ A \end{array} \begin{array}{c} \begin{array}{cccc} I & V & T & A \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1-a & a \\ 1-b & 0 & 0 & b \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array} \tag{5}$$

Variable a and b represent the probability of VALIDATE and TRANSFER state change into ABORT state. The values of a and b are derived from the success probability to forge a signcryption. If the probability to forge a signcryption (ε) is low ($\varepsilon \approx 0$), then it more likely that the state will ends in ABORT state. Thus, the value of variable a and b become close to 1 ($a, b \approx 1$).

In a case where both payer and payee are honest, there is no signcryption forgery. Under this condition it can be assumed that the probability to change into ABORT state is approximately zero ($a, b \approx 0$). In normal condition, the protocol will end in 3 steps. After 3 steps, the transition matrix from Equation 5 become as follow:

$$tm = \begin{array}{c} \\ I \\ V \\ T \\ A \end{array} \begin{array}{c} \begin{array}{cccc} I & V & T & A \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \tag{6}$$

The normal TRANSACTION protocol starts at IDLE state, and it will end in IDLE state again after 3 steps. From Equation 6, the probability of state's chain of I-V-T-I (the normal chain) is 1. It means that the protocol is always ends in IDLE state under normal condition. If there is any dishonest party (either payer or payee) involved in a transaction, then the probability of state transfer is not 1.

According to [16], the success probability to forge the signcryption can be calculated by method presented in [19]. In the proof, it is stated that the probability to existentially forge an identity-based signature is approximately low enough ($\varepsilon \approx 0.037$). By inserting the probabilistic value into the transition matrix in Equation 5 ($(1-a) = (1-b) = \varepsilon$), we find that after 2 steps the protocol ends in ABORT state with probability ≈ 0.963. In the same number of steps, the probability that the protocol will assume to change to the normal state (i.e. the adversary can change state from VALIDATE to TRANSFER) is 0.037. If the Markov chain probability after 3 steps is calculated, the protocol will end in IDLE state with probability of 0.964 and in ABORT state with probability of 0.035. The IDLE state has greater probability than ABORT state because there are 2 chain that can link to that result, the I-V-A-I chain and I-V-T-I chain. However, the I-V-A-I chain is having greater probability to occurs than the I-V-T-I chain. From the Markov chain calculation, the protocol will always end in either IDLE or ABORT state after 3 steps. It can be concluded that the protocol will ends in the designed state. From the calculation, the probability to forge a signcryption, hence forge a fake e-cash or double spend the e-cash and ends the transaction normally, is quite low.

B. Comparison of Properties

The proposed scheme must be able to solve the problem in Indonesia e-cash implementation. To fulfil this condition, the proposed scheme must have several e-cash functional properties (peer-to-peer and transferable) and mandatory security properties (forgery prevention and double spending prevention) [14]. The proposed scheme has the required properties which cannot be fulfilled by another scheme. The comparison of properties is conducted with two other schemes.

The first scheme is Abouelseoud's work that employ identity-based signcryption for e-cash [20] which based on work of Chaum's blind signature [21]. The second scheme is Zerocash [9] which works on top of Bitcoin [6]. The comparison of these schemes can be seen in Table 1.

Table 1. Comparison of Properties

Properties	Proposed Scheme	Abouelseoud Scheme [20]	Zerocash [9]
Paradigm	Centralized	Centralized	Decentralized
Peer-to-peer	Yes	No	Yes*
Transferable	Yes	No	Yes
Forgery prevention	Yes	Yes	Yes
Double spending prevention	Yes	Yes	Yes

*under Bitcoin mechanism

Although the scheme proposed by Abouelseoud uses identity-based signcryption, it has different purpose. The scheme focuses on generating new blind signature that does not require PKI in the process of signing the e-cash. The scheme works as online scheme where the TTP is required during time of transaction. The exchanged e-cash need to be deposited back to the TTP since it does not have transferable properties. Despite the implementation of identity-based signature, the scheme proposed by Abouelseoud still depends on proper network infrastructure. Zerocash has all the required properties to be implemented in Indonesia, except it operates under decentralized paradigm. Although the scheme is peer-to-peer at the time of transaction, the transaction needs to be broadcasted to most of Zerocash user to be recorded. If it is not recorded by most of Zerocash user, the transaction is invalid. Under this condition, the operation of Zerocash scheme still need the proper network infrastructure.

The proposed scheme can achieve what the other scheme cannot. The scheme is peer-to-peer, the transaction is conducted by Payer and Payee without the need to contact another party for validation, record, or public key request. The transferable property in the proposed scheme also means that the e-cash received by a Payee can be used in another transaction without the need to deposit the e-cash first. In these conditions, the need of proper network infrastructure is minimized.

4. Conclusion

The proposed scheme can solve Indonesia problem of e-cash implementation. By using identity-based signcryption and block chain, the proposed scheme able to have peer-to-peer and transferable property. Both properties ensure that the proposed scheme can works without proper network infrastructure. Even without proper network infrastructure, the proposed scheme is proven secure against forgery and double spending. Since the proposed scheme work under the supervision of a TTP, the scheme is centralized. All these conditions are perfect for Indonesia implementation.

Compared to Abouelseoud's scheme and Zerocash, the proposed scheme has its advantages. Abouelseoud's scheme does not have transferable and peer-to-peer property, even though it deploys the same identity-based signcryption. While Zerocash can fulfill the transferable property and peer-to-peer, it works under decentralized paradigm. The proposed scheme works under centralized paradigm, so it can fit the regulation in Indonesia perfectly.

5. References

[1] Bank Indonesia, "Statistik Sistem Pembayaran," 2017. [Online]. Available: http://www.bi.go.id/. [Accessed 21 May 2017].

[2] BPS, "Ekonomi Indonesia Triwulan IV-2017 Tumbuh 5,19 persen," Badan Pusat Statistik, 2018. [Online]. Available: https://www.bps.go.id/pressrelease/2018/02/05/1519/ekonomi-indonesia-triwulan-iv-2017--tumbuh-5-19-persen.html. [Accessed 9 July 2018].

[3] BPS, "Uang Beredar (Milyar Rp), 2003-2018," Badan Pusat Statistik, 2018. [Online]. Available: https://www.bps.go.id/dynamictable/2015/12/22/1074/uang-beredar-miliar-rupiah-2003-2017.html. [Accessed 9 July 2018].

[4] APJII, "Infografis Penetrasi & Perilaku Pengguna Internet Indonesia," Indonesia Internet Service Provider Association, 2017.

[5] D. E. Saputra and S. H. Supangkat, "A study of electronic cash paradigm," in *Information Technology Systems and Innovation (ICITSI), 2014 International Conference on*, 2014. pp 273-278.

[6] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system,* 2008.

[7] I. Miers, C. Garman, M. Green and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Security and Privacy (SP), 2013 Sympossium on*, 2013. pp. 397-411.

[8] G. Danezis, C. Fournet, M. Kohlweiss and B. Parno, "Pinocchio coin: building zerocoin from succinct pairing-based proof system," in *Proceeding of the First ACM workshop on Language support on privacy-enhancing technologies*, 2013. pp. 27-30.

[9] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, 2014. pp. 459-474.

[10] C.-I. Fan and V. S.-M. Huang, "Provably secure on/off-line electronic cash for flexible and efficient payment," *IEEE Transaction on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* vol. 40, no. 5, pp. 567-579, 2010.

[11] H. Oros and C. Popescue, "A secure and efficient off-line electronic payment system for wireless network," *International Journal of Computers Communication & Control,* vol. 5, no. 4, pp. 551-557, 2010.

[12] C. Wang, H. Sun, H. Zhang and Z. Jin, "An improved off-line electronic cash scheme," in *Computational and Information Science (ICCIS), 2013 Fifth International Conference on*, 2013. pp. 438-441.

[13] O. Blazy, S. Canard, G. Fuchsbauer, A. Gouget, H. Sibert and J. Traoré, "Achieving optimal anonymity in transferable e-cash with a judge," in *International Conference on Cryptology in Africa*, 2011. pp. 206-223.

[14] D. E. Saputra, S. Sutikno and S. H. Supangkat, "General Model for Secure Electronic Cash Scheme," *International Journal of Network Security,* in press.

[15] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption)," in *Annual International Cryptology Conference*, 1997. pp. 165-179.

[16] J. Malone-Lee, "Identity-based signcryption," *IACR Cryptology ePrint Archive,* p. 98, 2002.

[17] R. C. Merkle, "A certified digital signature," in *Conference on the Theory and Application of Cryptology*, 1989. pp. 218-238.

[18] J. Dreier, A. Kassem and P. Lafourcade, "Formal analysis of e-cash protocol," in *e-Business and Telecommunications (ICETE), 2015 12th International Joint Conference on*, 2015. pp. 65-75.

[19] F. Hess, "Efficient identity based signature schemes based on pairings," in *International Workshop on Selected Areas in Cryptography*, 2002. pp. 310-324.

[20] Y. Abouelseoud, "New blind signcryption schemes with application to e-cash systems," in *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on*, 2014. pp. 1-6.

[21] D. Chaum, "Blind Signature for Untraceable Payment," *Advance in Cryptology - CRYPTO '82*, pp. 199-203, 1983.

Dany Eka Saputra received B.Eng. in Aeronautics and Astronautics from Institut Teknologi Bandung in 2007. He also obtained his M.Eng. in Electrical Engineering from the same institution in 2012. Currently, he is taking his Doctoral study in Electrical Engineering and Informatics in Institut Teknologi Bandung. He also a faculty member Department of Informatics in STMIK "AMIKBANDUNG". His main interest is information security and cryptography. His other interest includes game technology and protocol engineering.

Sarwono Sutikno received B.Eng. in Electronics from Institut Teknologi Bandung in 1984. He then received his Dr.Eng. in Integrated System from Tokyo Institute of Technology in 1994. Currently, he is an Associate Professor at School of Electrical Engineering and Informatics, Institut Teknologi Bandung. An active member of ISACA with certification in CISM, CISSP, CISA, and CSX-F. His main interest is information security, embedded secure system, and cryptography.

Suhono Harso Supangkat received his B.Eng. in Electrical Engineering from Institut Teknologi Bandung in 1986. He received his Dr.Eng. in Information System Science from Tokyo University of Electro-Communication in 1998. Currently, he is a Professor at School of Electrical Engineering and Informatics, Institut Teknologi Bandung. His main interest is smart city system and technology. Actively promoting smart city concept and technology from 2012.