View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Scholarworks@UTRGV Univ. of Texas RioGrande Valley

University of Texas Rio Grande Valley

ScholarWorks @ UTRGV

Computer Science Faculty Publications and Presentations

College of Engineering and Computer Science

3-2020

Supporting Blockchain-Based Cryptocurrency Mobile Payment With Smart Devices

Lei Xu
The University of Texas Rio Grande Valley, lei.xu@utrgv.edu

Lin Chen
University of Houston

Zhimin Gao
University of Houston

Larry Carranco
University of Houston

Xinxin Fan
IoTeX

See next page for additional authors

Follow this and additional works at: https://scholarworks.utrgv.edu/cs_fac

 Part of the Computer Sciences Commons

Recommended Citation

Xu, Lei; Chen, Lin; Gao, Zhimin; Carranco, Larry; Fan, Xinxin; and University of Houston, Nolah Shah, "Supporting Blockchain-Based Cryptocurrency Mobile Payment With Smart Devices" (2020). *Computer Science Faculty Publications and Presentations*. 16.
https://scholarworks.utrgv.edu/cs_fac/16

This Article is brought to you for free and open access by the College of Engineering and Computer Science at ScholarWorks @ UTRGV. It has been accepted for inclusion in Computer Science Faculty Publications and Presentations by an authorized administrator of ScholarWorks @ UTRGV. For more information, please contact justin.white@utrgv.edu, william.flores01@utrgv.edu.

Authors
Lei Xu, Lin Chen, Zhimin Gao, Larry Carranco, Xinxin Fan, and Nolah Shah University of Houston

This article is available at ScholarWorks @ UTRGV: https://scholarworks.utrgv.edu/cs_fac/16

Supporting Blockchain based Cryptocurrency Mobile Payment with Smart Devices

Lei Xu, Lin Chen, Zhimin Gao, Larry Carranco, Xinxin Fan, Nolan Shah, Nour Diallo, and Weidong Shi

***Abstract*—The smart device owning rate such as smart phone and smart watch is higher than ever before and mobile payment has become one of the major payment methods in many different areas. At the same time, blockchain based cryptocurrency is becoming a non-negligible type of currency and the total value of all types of cryptocurrency has reached USD 200 billion. Therefore, it is a natural demand to support cryptocurrency payment on mobile devices. Considering the poor infrastructure and low penetration of financial service in developing countries, this combination is especially attractive. The high storage cost and payment processing latency are the two main obstacles for mobile payment using cryptocurrency. We propose two different schemes for cryptocurrency mobile payment, one involves a centralized bank and the other one does not require any centralized party. We also provide a solution for the bank to meet KYC (know your customer)/AML (anti money laundering) compliance requirements when it is involved in cryptocurrency mobile payment processing.**

I. Introduction

Mobile payment (MP) uses personal smart devices such as smart phones as the tool to make payment and receive money, which is especially attractive in underdeveloped areas where the majority of people only have access to the Internet through their phones.

Most existing mobile payment systems depend on a centralized party, e.g., banks and carriers, face the following challenges: (i) One major obstacle that prevents people in these areas from fully enjoying the benefits of mobile payment is the low penetration rate of financial service. According to the World Bank, 59% of adults in developing economies do not have an account at a financial institution. (ii) For those who can obtain a bank account, it is not cheap to use the bank for transactions processing. Credit companies and banks charge fees for payment processing. The electronic payments acquiring/processing revenue for the U.S. market itself is expected to achieve $ 14.3 billion [1]. (iii) Using bank based mobile payment also exposes the consumers to the potential risk of inflation, which is especially serious in underdeveloped and developing countries.

The emergence of cryptocurrency using blockchain provides an alternative way to support mobile payment. A blockchain is a decentralized ledger that is maintained by all participants, which can be used to store all transactions information of the cryptocurrency to prevent double spending and track ownership. Bitcoin is the first successful cryptocurrency built on top of blockchain, which was proposed by Nakamoto in 2008 [9]. Most blockchain based cryptocurrency systems have three major benefits: openness, predictable supply, and lower transaction cost.

Considering the wide adoption of mobile devices and the advantages of blockchain based cryptocurrency, the combination of these two technologies provides a unique opportunity to improve the everyday life for people in underdeveloped areas. However, several technique challenges need to be addressed to support cryptocurrency mobile payment. For example, smart devices usually have limited storage capacity and cannot save the whole blockchain, and most public blockchains are built using PoW and have relatively high latency. Storage and communication cost can be reduced using cryptography accumulator [14] or trusted full nodes, and we focus on the reduction of latency in this paper.

Our contributions. In this paper, we consider two different scenarios of mobile payment with blockchain based cryptocurrency: (i) The merchant has a traditional bank account and the bank can facilitate the payment process; (ii) Neither the payer nor the merchant has a traditional bank account and they have to work together to finish the payment. We propose two protocols that can be used to handle mobile payment for these scenarios that allow the user to better control the payment and are more flexible for daily use. We also design a framework to help the financial institution to meet the KYC (know your customer)/AML (anti money laundering) compliance requirements when it is involved in cryptocurrency payment processing.

II. Background and Challenges

In this section, we briefly introduce background information that is related to mobile payment, blockchain, and cryptocurrency.

Mobile payment. Mobile payments cover many types of transactions which fall into two categories: transactions with a remote merchant or proximity payments at the merchant site. There are different ways to implement mobile payment, such as NFC based mobile payment, using QR code for payment, and audio signal based approach. There are many commercial mobile payment products on the market, including Alipay, Square, Google Wallet, and Apple Pay. These products may use different communication channels to finish the payment but they also share some similarities: (i) The mobile device stores credentials like checking account and credit card information; (ii) The real payment is processed by the bank.

Cryptocurrency systems. Cryptocurrency, or electronic cash, was developed at least at early 90's. The basic requirement of all cryptocurrency systems is prevention of double-spending, i.e., one cannot spend the same currency twice, and cryptocurrency schemes with extra features are also developed, such as untraceability and anonymization. All these schemes rely on a centralized party, usually the bank, to achieve the design goals.

Blockchain technology. In a nutshell, a blockchain is a sequence of blocks and provides a decentralized book keeping mechanism. Blocks are linked together using hash values, and any type of records can be embedded into the block. Depending on the way the blockchain is constructed, a proof field is used to stores different information to demonstrate the validity of this block. Each participant of the system maintains his/her own local copy of the blockchain, and they follow a pre-defined consensus protocol to determine the next block to be added.

Blockchain technology has found many applications [6], [5], [13], [11], and is used to build cryptocurrency systems without relying on a centralized party. The basic idea is to embed transactions into blocks and store the complete transaction history on the blockchain. Because of the public accessibility and the immutability feature, every participant can detect double-spending him/herself, and the consensus mechanism guarantees that as long as the majority of participants are honest, every double-spending transaction will be rejected. More specifically, a blockchain based cryptocurrency system has two basic functions: currency creation and currency transfer. We only consider public blockchain based cryptocurrency system in this paper as it is harder to be take over by a small group of malicious participants.

III. Fine-grained Payment Schemes

Most existing blockchain based cryptocurrency systems like Bitcoin use a simple payment structure. Each user is equipped with a public/private key pair, where the public key serves as the wallet address to identify the user and the private key is used to authorize transactions, which only include the amount and receiver's identity. We propose two fine-grained payment primitives that allow a user to manage transactions in a more flexible way and are more suitable for the mobile environment. We also provide two concrete use cases of these primitives in Section IV.

Payment using delegation. The first primitive is delegation based payment, which allows a user to leverage a semi-trusted third party to help her/him to manage payments.

When a user first joins the system, he/she generates a key pair (pk_m, sk_m). The user can delegate the right of transaction generation by submitting the following record to the system:

$$delegation \leftarrow (pk_d, pk_m, policy, sig_{sk_m}(pk_d||policy)),$$

where pk_d is the delegatee's public key in the system, $policy$ describes what privileges are given, and $sig_{sk_m}(pk_d||policy)$ is the delegator's digital signature of the record. $policy$ can be defined as $[range^*||count^*||time^*||receiver^*]^*$, where $range$ is a number that defines the amount of cryptocurrency the delegatee can use for transactions, $count$ sets up the limitation that how many times the delegatee can issue transactions, $time$ is the time period that the delegation is valid, and $receiver$ is the address that the delegatee can send cryptocurrency to.

When a miner receives a record of delegation request, s/he checks its validity and tries to include it in a block if everything is consistent, e.g., the signature is valid and the delegator wallet has enough balance. After the block containing the payment delegation record is confirmed on the blockchain, only the delegatee can launch transactions using his/her own private key on behalf of the delegator until the delegation expires. Miners of the blockchain system will check transactions created by the delegatee to make sure they are consistent with the *policy*.

The user can also set up multiple delegatees in the system to further improve the flexility by submitting more than one delegation request record, and each delegator can handle a specific type

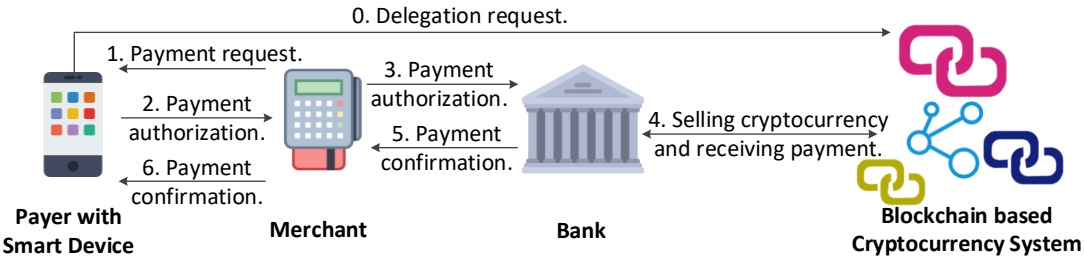

Fig. 1: Overview of the protocol of supporting blockchain based cryptocurrency with a third party. On the merchant side, it does not need to change existing system like POS machine to accept mobile payment using cryptocurrency.

of payments. To avoid potential risk of double-spending, the system checks whether two delegation requests are compatible in the worst case, i.e., the delegator has enough balance to cover all payment that these two delegatees can make according to the pre-defined policies.

With delegation, the latency of payment on a public blockchain can be reduced as the receiver does not need to wait for a payment record to be confirmed on the blockchain. There is still a latency for the blockchain to confirm the record but the receiver can accept the payment immediately as the delegatee is trusted and will not submit conflicted payment records.

Two-step payment. The second primitive for mobile payment using cryptocurrency is two-step payment mechanism. Following the basic idea of Bitcoin Lightening network, we divide the payment into two phases, pre-payment and confirmation. The sender first creates a pre-payment record in the following form:

$$\textit{prepay} \leftarrow (\textit{value}, \textit{receiver}^{+}, \textit{notary}^{*}, \textit{critera}, pk_S, sig_{sk_S}(\textit{value}||\textit{receiver}^{+}||\textit{notary}^{*}||\textit{criteria})).$$

Here *value* is the amount of cryptocurrency that the user wants to send, $\textit{receiver}^{+}$ is a list of one or more potential receivers' wallet addresses, $\textit{notary}^{*}$ is a list of zero or more notaries who can endorse the transaction, and *criteria* defines when the transaction should be accepted, e.g., the majority of notaries support the transaction, one third of notaries plus a certain one support the transaction. pk_S/sk_S is the public/private key of the sender and $sig_{sk_S}(value||receiver^{*}||notary^{*}||critera)$ is the digital signature of the record.

When the sender decides to finalize a *prepay* transaction, s/he first selects a receiver pk_R, generates a message $(prepay, pk_R, sig_{sk_S}(prepay||pk_R))$ and then shares with the receiver. The receiver appends his/her digital signature $sig_{sk_R}(prepay, pk_R)$ and asks all notaries listed in $prepay$ to sign the message, and the final result is the confirmation record:

$$\textit{confirm} \leftarrow (prepay, pk_R, sig_{sk_S}(prepay||pk_R), sig_{sk_R}(prepay||pk_R), sig_{notary}(prepay||pk_R)),$$

where $sig_{notary}(prepay, pk_R)$ is a set of signatures generated by users included in notary list, which is part of *prepay*.

This two-steps payment scheme enables 1-to-many payment, i.e., the pre-payment record does not need to bind with a specific receiver. This is especially useful in everyday usage as the user does not know in advance which merchant s/he will deal with. At the same time, the scheme reduces payment latency as notaries guarantee the validity of a payment scheme even if it has not been confirmed on the blockchain yet.

IV. Two Scenarios of Mobile Payment with Cryptocurrency

In this section, we discuss two major mobile payment scenarios using cryptocurrency based on the schemes given in Section III.

A. Case 1: Mobile Payment for Merchant without a Cryptocurrency Account

It is usually easier for a merchant to open a bank account than an individual, but the merchant may not have an account of cryptocurrency. Therefore, it is useful for the mobile payment scheme with lightweight smart devices to support this scenario to accelerate the adoption of MP with cryptocurrency.

Note that this procedure is similar to existing products such as Bitpay. The major difference is that the payer can enforce a fine-grained control of the transactions that the bank can launch.

MP protocol for case 1. We assume that everyone has been properly initialized and the communication between different parties is secured using TLS/SSL. The MP protocol works as follows:

1: Delegation setup. Using the delegation protocol described in Section III, the payer authorizes the

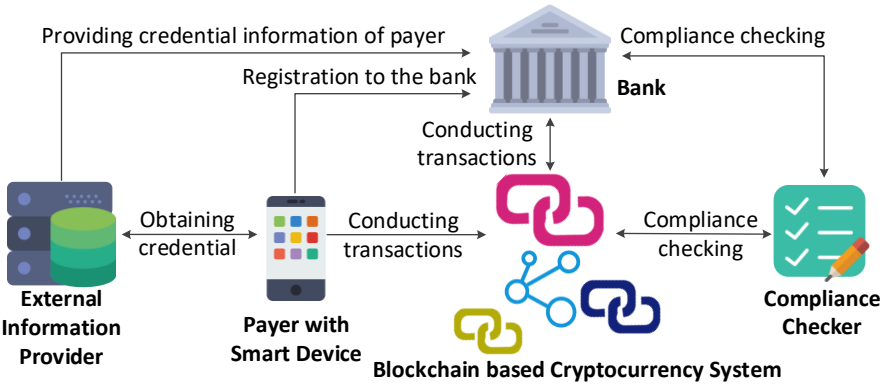

Fig. 2: Supporting KYC and AML for mobile payment using cryptocurrency when a bank is involved.

bank as the delegator to sell a certain amount of cryptocurrency on behalf of him/herself.

2: Payment request initialization. The merchant sends the payment request to the payer, which includes identity of the merchant, the value of the payment, and the merchant's digital signature that protects the authenticity/integrity of the request.
3: Payment preparation. The sender first checks the payment request for value and merchant identity, then generates a request to ask the bank to sell a certain amount of cryptocurrency and pay the merchant fiat currency.
4: Payment submission. As the payer designates the bank as the delegatee, the bank can issue a transaction on the blockchain based cryptocurrency system to sell cryptocurrency for fiat currency, which is then deposited to the merchant account. If the payment is not consistent with the conditions included in the delegation, the blockchain will not accept the bank issued transaction and the payment fails.
5: Payment confirmation. The merchant checks his/her bank account. If he/she receives the correct amount of fiat currency, the payment is finished.

The above protocol can address blockchain storage and payment processing latency:

- Storage and communication. The smart device relies on the bank for all blockchain related operations. Because the bank usually has strong enough servers to work as a full node who keeps a local copy of the complete transaction history and reliable network connecting to other participants of the blockchain system, it has the capability to verify the validity of transactions by itself.
- Latency. Since the bank works as a delegatee of the payer, it can guarantee the success of the selling operation as there will not be a double-spending. Therefore, the bank can deposit the correct amount of fiat currency to the merchant account before the selling transaction is confirmed in the blockchain based cryptocurrency system.

One potential risk that the proposed protocol cannot address in this scenario is liquidity. Since the merchant only accepts fiat currency, there must be a liquidity provider who is willing to help the payer to convert the cryptocurrency to fiat currency. If there is not enough liquidity, the payment will fail.

Regulatory compliance. When a financial institution is involved in the mobile payment, even if it is cryptocurrency, the system needs to consider regulatory requirements such as KYC and AML [2]. Although blockchain can be used as the storage infrastructure to store KYC related information [7], [8], in a purely decentralized and open system, it is very difficult or even impossible to obtain accurate information of each participant to fulfill all requirements at the first place [3]. Therefore, we propose to add another layer on top of the existing blockchain based cryptocurrency system for KYC and AML compliance. Fig. 2 demonstrates the overall framework for KYC/AML compliance layer.

According to the requirements, the payer with smart device needs to contact external information provider to obtain credential information of him/herself. External information providers also help the payer to bind the credentials with his/her identity used in the cryptocurrency system by maintaining a database that stores the relationship between the identity and credentials. When the payer registers with the bank using the new identity with bound credential, the bank can check with external information providers to learn whether the new identity has correct credentials attached. With the new identity, the bank can help the payer and

merchant to finish transactions. The compliance checker monitors transactions on the blockchain and within the bank system and can link them with credential information of involved parties to make sure that all KYC/AML requirements are satisfied.

B. *Case 2: Mobile Payment for Merchant with a Cryptocurrency Account*

When both the payer and the merchant have cryptocurrency accounts, the two-step payment protocol can be applied and only three players are involved: the payer with a smart device to make payment, the merchant with a cryptocurrency account, and the blockchain based cryptocurrency system. Fig. 3 demonstrates the sketch of MP using cryptocurrency without a centralized bank using the two-step payment protocol.

MP protocol for case 2. The MP protocol for case 2 leverages the two-step payment mechanism described in Section III, which works as follows:

1: Pre-payment. The payer generates a set of pre-payment records according to his/her preferences and submits them to the blockchain.
2: Payment request initialization. The merchant sends the payment request to the payer, which includes identity of the merchant, the value of the payment, and the merchant's digital signature that protects the authenticity/integrity of the request. The merchant can also share his/her preferred list of notaries with the payer.
3: Payment submission. The payer selects an adequate pre-payment record according to information received from the merchant, and collaborate with the merchant to prepare the message to finish the selected pre-payment. The message is then send to notaries listed in the pre-payment record to confirm.
4: Payment confirmation. Notaries sign the message and submit it to the blockchain based cryptocurrency system. The signed message is also sent to the merchant. The merchant does not need to wait for this transaction to be confirmed on the blockchain if he/she trusts those notaries as a group.

The payer knows pre-payment records he/she generated so he/she does not need to query the blockchain to obtain these information. For the merchant, he/she only needs to verify the confirmed payment record which is signed by a group of notaries. Therefore, neither of them needs to keep a full copy of the blockchain.

The payment processing latency is shifted to the first step, i.e., pre-payment creation. After the pre-payment record is confirmed on the blockchain, corresponding notaries can quickly sign the payment request and the merchant does not need to wait for the signed payment confirmation record to be confirmed on the blockchain.

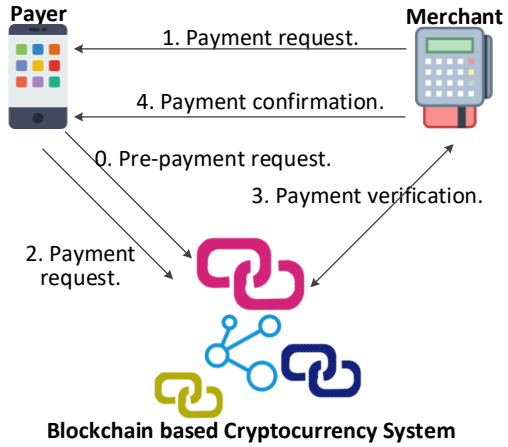

Fig. 3: Reducing latency in cryptocurrency mobile payment using smart devices without a centralized bank. The strategy is to use a two-step payment to shift the latency.

V. Related Works

A variety of blockchain based cryptocurrency systems have been proposed since Nakamoto introduced Bitcoin. Some of these systems simply replace the mining mechanism of Bitcoin (e.g., Litecoin uses a memory intensive mining function instead of SHA-256, Primecoin requires the miner to find a prime number as the proof-of-work [4]), and others provide new features beside a simple cryptocurrency (e.g., Zcash [12] and Dash enable privacy preserving transaction where sender/receiver and amount information is hidden, Ethereum provides a smart contract platform). These systems do not consider latency and storage cost, and hard to be adopted by mobile payment.

While there are some decentralized token exchange platform (e.g., Nxt and Circle), exchange between cryptocurrency and fiat currency still heavily depends on centralized platforms, which usually require to fully control the user's account. While this reduces latency and the risk of the exchange itself, it requires the exchange platform to be well protected.

One direction to reduce latency is to use new methods to maintain the blockchain itself, such as permissioned blockchain with Byzantine fault tolerant protocol and graph based chain structure like IOTA. Another direction is to design new transaction structures. Bitcoin Lightening network [10] is a successful example along this direction, which divides a transaction into multiple steps and allows participants to conduct off-chain transactions.

VI. Results Discussion and Future Works

In this paper, we proposed two cryptocurrency protocols that are useful for mobile payment, the delegation protocol and the transaction protocol with low latency. These two protocols allow the user to better control his/her cryptocurrency account and are more flexible for daily use. We also discuss their applications in two common cryptocurrency mobile payment scenarios and provide a mechanism to enforce and check KYC/AML compliance. These schemes have the potential to greatly promote the adoption of both mobile payment and cryptocurrency, and benefit people in underdeveloped areas. The proposed schemes also have some limitations such as relying on a centralized party in the delegation protocol and vulnerability to notaries collusion.

Future works on blockchain based cryptocurrency mobile payment include: (i) Proof of concept. We plan to implement a fully functional prototype on main stream smart phone platforms to validate it performance. (ii) Stabilization of cryptocurrency. Most existing blockchain based cryptocurrency systems are used as investing instruments other than currencies and their prices fluctuate strongly. However, this is not favorable from a general user's perspective. We plan to explore new technologies to make the value of the cryptocurrency more steady. (iii) Transaction cost reduction. We also plan to develop a formal framework to analyze the relationship between incentive mechanism and miners' behaviour, and utilize the results to reduce the transaction cost.

About the Authors

Lei Xu (xuleimath@gmail.com) is a research scientist at Conduent Labs. His research interests include blockchain, cloud security, and applied cryptography.

Lin Chen (chenlin198662@gmail.com) is a research assistant professor at University of Houston. His research interests include blockchain, stochastic optimization, parameterized algorithms and complexity.

Zhimin Gao (mtion@msn.com) is currently working as a post-doctoral fellow at University of Houston. His research interests include blockchain, high performance computing and cloud computing.

Larry Carranco (lcarranco@gmail.com) is an undergraduate student of Computer Science Department, University of Houston. His research interests include blockchain and supply chain.

Xinxin Fan (xinxin@iotex.io) is currently working as the Chief Cryptography Officer at IoTeX. His research interesting include cryptography and blockchain technology.

Nolan Shah (nolanshah212@gmail.com) is an undergraduate student of Computer Science Department, University of Houston. His research interests include blockchain, machine learning, and VoIP security. Email:

Nour Diallo (noudiallo@gmail.com) is a master student of Computer Science Department, University of Houston. His research interests include blockchain and mobile payment.

Weidong (Larry) Shi (wshi3@central.uh.edu) is employed as an associate professor by University of Houston. He is involved in Borders, Trade, and Immigration Institute and he is the organizer of Houston's meetup group on blockchain.

References

[1] R. Byrne and J. Hanson, "Innovation and disruption in u.s. merchant payments," 2014.

[2] J. S. Cermeño, "Blockchain in financial services: Regulatory landscape and future challenges for its commercial application," *BBVA Research, Madrid, Spain*, 2016.

[3] M. Gill and G. Taylor, "Preventing money laundering or obstructing business? financial companies' perspectives on 'know your customer'procedures," *British Journal of Criminology*, vol. 44, no. 4, pp. 582–594, 2004.

[4] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," 2013.

[5] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[6] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry [future directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 19–23, 2017.

[7] Y. Lootsma, "From fintech to regtech: The possible use of blockchain for KYC," 2017.

[8] D. Martens, A. v. Tuyll van Serooskerken, and M. Steenhagen, "Exploring the potential of blockchain for kyc," *Journal of Digital Banking*, vol. 2, no. 2, pp. 123–131, 2017.

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

[10] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," *draft version 0.5*, vol. 9, p. 14, 2016.

[11] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.

[12] 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*. IEEE, 2014, pp. 459–474.

[13] L. Xu, L. Chen, Z. Gao, Y. Lu, and W. Shi, "Coc: Secure supply chain management system based on public ledger," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*. IEEE, 2017, pp. 1–6.

[14] L. Xu, L. Chen, Z. Gao, S. Xu, and W. Shi, "Epbc: Efficient public blockchain client for lightweight users," in *SERIAL 17: ScalablE and Resilient InfrAstructures for distributed Ledgers*. ACM, 2017.