9-2018

Blockchain based efficient and robust fair payment for outsourcing services in cloud computing

Yinghui ZHANG

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Ximeng LIU

Dong ZHENG

DOI: https://doi.org/10.1016/j.ins.2018.06.018

Citation

ZHANG, Yinghui; DENG, Robert H.; LIU, Ximeng; and ZHENG, Dong. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. (2018). *Information Sciences*. 462, 262-277. Research Collection School Of Information Systems.

Available at: https://ink.library.smu.edu.sg/sis_research/4213

Blockchain based Efficient and Robust Fair Payment for Outsourcing Services in Cloud Computing

Yinghui Zhang[a,b,c,d,*], Robert H. Deng[b], Ximeng Liu[b], Dong Zheng[a,d]

[a]*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, P.R. China*
[b]*School of Information Systems, Singapore Management University, Singapore*
[c]*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, P.R. China*
[d]*Westone Cryptologic Research Center, Beijing 100070, P.R. China*

Abstract

As an attractive business model of cloud computing, outsourcing services usually involve online payment and security issues. The mutual distrust between users and outsourcing service providers may severely impede the wide adoption of cloud computing. Nevertheless, most existing payment solutions only consider a specific type of outsourcing service and rely on a trusted third-party to realize fairness.

In this paper, in order to realize secure and fair payment of outsourcing services in general without relying on any third-party, trusted or not, we introduce BCPay, a blockchain based fair payment framework for outsourcing services in cloud computing. We first present the system architecture, specifications and adversary model of BCPay, then describe in detail its design. Our security analysis indicates that BCPay achieves *Soundness* and what we call *Robust Fairness*, where the fairness is resilient to eavesdropping and malleability attacks. Furthermore, our performance evaluation shows that BCPay is very efficient in terms of the number of transactions and computation cost. As illustrative applications of BCPay, we further construct a blockchain-based provable data possession scheme in cloud computing and a blockchain-based outsourcing computation protocol in fog computing.

Keywords: Blockchain, Cloud security, Fair payment, Provable data possession, Outsourcing computation, Authentication.

*Corresponding author.

Email addresses: `yhzhaang@163.com` (Yinghui Zhang), `robertdeng@smu.edu.sg` (Robert H. Deng), `snbnix@gmail.com` (Ximeng Liu), `zhengdong@xupt.edu.cn` (Dong Zheng)

The paper is published in Information Sciences (`https://doi.org/10.1016/j.ins.2018.06.018`) and Elsevier has the copyright. It can be cited as Zhang Y, Deng R H, Liu X, et al. Blockchain based Efficient and Robust Fair Payment for Outsourcing Services in Cloud Computing[J]. Information Sciences, 2018, 462: 262-277.

1. Introduction

As a promising computing paradigm, cloud computing has many attractive benefits, such as flexibility, high efficiency and high availability. It can provide a diversity of outsourcing services including storage and computations [3]. With the rapid development of cloud computing technologies, an increasing number of individuals and enterprises have uploaded their various data onto third-party cloud platforms either for ease of sharing or for cost savings. The cloud storage service of Dropbox currently has approximately 500 million registered users and 500 petabytes of user data [27]. Users can also subscribe to flexible computation resources from cloud service providers such as Google and Amazon. In order to facilitate the operation of computation, storage and networking services between end users and cloud computing data centers, fog computing further extends cloud computing to the edge of the network [9]. In fog computing, the outsourcing computation service is required because end users usually are resource-constrained. Obviously, outsourcing services play an important role in the development of cloud and fog computing.

Although cloud computing allows users to customize outsourcing services, its unique aspects also raise various security and privacy concerns [41, 29, 35, 32, 51, 34, 49, 50]. In cloud storage, for instance, users usually require assurance of data possession besides confidentiality of outsourced data. As for computation, users expect to get valid and correct computation results from the outsourcing service provider once the service fee is paid. Recently, great efforts have been made to realize provable data possession (PDP) [4, 6] and verifiable outsourcing computation [25, 33, 42, 13, 15]. However, most of the existing schemes do not consider the payment issues in outsourcing services. Take PDP as an example. In a challenge proof of PDP, if the server is malicious, a user's data may be lost without any compensation even if he/she has paid for the service. On the other hand, in the case of a malicious user, the server cannot earn the service fee from the user even if it enforces a valid and correct PDP service. Because of the distrust between the user and the server [37, 24, 47, 48, 18], the payment issues are sufficiently challenging for outsourcing services considering fairness.

In order to simultaneously address the payment and security issues, most of the existing schemes adopt the (default) traditional payment mechanism and rely on a trusted third-party such as a bank. For example, the Google cloud platform provides a series of cloud services including computing and data storage, and the registration requires a bank account [20]. In cloud computing, however, the traditional payment solution suffers several drawbacks. First, it is assumed that the bank is trusted by all the users and the server and it deals with all procedures in a fair manner. Second, the payment mechanism needs to be adapted to multiple banks used by different participants and has to be updated whenever they change, which will become a bottleneck of the payment system. Last but not least, users' privacy associated with bank accounts may be violated.

Recently, blockchain technologies have gained prominent popularity mostly due to its distributed nature and the lack of a central authority. In blockchain-based outsourcing services, the service fee is transferred directly between the user and the server and they do not have to trust any third-party. However, to the best of our knowledge, blockchain technologies have seldom been used in general for fair payment of outsourcing services in cloud and fog computing.

1.1. Our Contributions

To eliminate the third-party, trusted or not, while ensuring the fairness of payment against malicious users and outsourcing service providers, we introduce BCPay, a blockchain based fair payment framework for outsourcing services in cloud and fog computing. Our contributions are three-folds:

1. We first propose the system architecture, specifications and adversary model of BCPay, then describe its design details. We prove that BCPay enjoys *Soundness* and *Robust Fairness* where the latter implies that fairness is resilient to any attacks including eavesdropping and malleability attacks without relying on any third-party.

2. In BCPay, soundness and robust fairness are achieved by an *all-or-nothing checking-proof* protocol. In the protocol, it is ensured that the outsourcing service provider either earns the service fee and gets his/her guaranty back simultaneously or pays a penalty in the form of deposit to the user. Besides, our performance evaluation shows that BCPay is very efficient in terms of the number of involved transactions and computation cost.

3. To illustrate the applications of BCPay, we propose a blockchain-based PDP scheme in cloud computing and an outsourcing computation protocol suitable for fog computing.

1.2. Related Work

As an earlier and important application of blockchain technologies, Bitcoin was announced under the pseudonym Satoshi Nakamoto [39]. To facilitate the wide use of blockchain technologies, Buterin [10] proposed Ethereum, a next-generation smart contract and decentralized application platform. Later, Andrychowicz et al. [2] proposed a bitcoin-based timed commitment scheme, in which the committer has to reveal his/her secret before a specific time, or to pay a fine. With bitcoin-based timed commitments in place, they further constructed protocols for secure multiparty lotteries. In order to realize more general computation, Andrychowicz et al. [1] proposed a simultaneous Bitcoin-based timed commitment scheme. Subsequently, they presented a two-party computation protocol, which modifies the Bitcoin specifications to resist malleability attacks. Similar ideas were developed independently by Bentov et al. [8]. Note that all these bitcoin-based schemes cannot realize what we call all-or-nothing property which is required in outsourcing services. Specifically, the all-or-nothing property ensures that the outsourcing service provider either earns the service fee and gets his/her guaranty back simultaneously or pays a penalty to the user. The line of work on outsourcing service consists of outsourcing storage and outsourcing computation.

As for outsourcing storage, based on RSA homomorphic tags, Ateniese et al. [4] proposed the first PDP scheme, which allows users to challenge the cloud server for a proof that the integrity of their data is not violated. Recently, homomorphic signature and encryption technologies have obtained many attentions [40, 45]. In the same year, Juels et al. [30] defined and explored proofs of retrievability, which enables the cloud server to produce a concise proof that a user can retrieve a target file. Later, Ateniese et al. [7] presented a PDP scheme based on identification protocols supporting public verification. Data dynamics are further considered in [5, 43, 46]. On the other hand, outsourcing computation enables resource-limited end users in fog computing to complete computationally expensive tasks with the help of fog nodes (a.k.a. workers). This introduces the potential of cheating by untrusted participants in a commercial setting. To protect the rights and interests of users, the concept of ringer [26] is introduced to verify the validity of outsourcing computation results. In order to improve efficiency, Du et al. [22] presented a commitment-based scheme to prevent workers from cheating. Gennaro et al. [25] proposed a verifiable outsourcing computation scheme while protecting the input and output privacy. Carbunar et al. [12] proposed several outsourcing computation solutions that simultaneously ensure correct remuneration for computation tasks completed on time and prevent workers' laziness. Chen et al. [16] considered outsourcing computation with such workers that may not send the computation results on time. Chen et al. [14] further proposed a conditional e-payment system based on a restrictive partially blind signature scheme. Song et al. [42] proposed a solution to verifiable outsourcing of polynomial evaluation. Additionally, verifiable computation over large database is studied in [17].

In the above schemes, however, either the payment issue is not taken into account or the traditional payment framework is adopted, which needs a trusted third-party to realize fair payment. To solve these problems, blockchain technologies have been introduced to outsourcing services. Compared to traditional payment technologies, the independence from central authorities is the key advantage of blockchain-based solutions. Ateniese et al. [6] introduced accountable storage based on an extension of invertible Bloom filters, and showed how to combine it with Bitcoin based zero-knowledge proofs. However, the combination involves a trusted third-party called Bitcoin arbitrator. Huang et al. [28] proposed a blockchain-based outsourcing computation scheme, in which a trusted third-party is still required. Obviously, all these schemes [6, 28] fail to truly realize blockchain-based decentralized outsourcing services. Campanelli et al. [11] defined the notion of zero-knowledge contingent service payment to realize service payment based on blockchains. They constructed two high-level protocols and presented a concrete realization based on the proof of retrievability service. However, the proposed protocols are only conceptual and lack design details, of which the efficiency remains to be improved because a witness indistinguishable protocol [23] is used as a building block. Based on game theory and Ethereum smart contracts, Dong et al. [21] proposed a protocol for checking the correctness of computation in cloud computing. However, it is assumed that users are honest and two clouds cannot collude. On the other hand, in order to improve the transaction throughput and latency in blockchains, current efforts focus on off-chain payment channels which can be combined in a payment-channel network to enable a number of payments without accessing the blockchain. Khalil et al. [31] presented a solution which allows an arbitrary set of users in the payment-channel network to securely rebalance their channels. Malavolta et al. [36] formalized the security and privacy notions in a payment-channel network including balance security and value privacy. In this paper, we propose a general blockchain-based payment solution for outsourcing services, which can efficiently address the threat of cheating from malicious participants and offer guarantees that the service has been correctly enforced.

1.3. Organization

The rest of the paper is organized as follows. Some preliminaries are given in Section 2. We then present the system architecture, specifications and adversary model in Section 3. The proposed framework BCPay together with its security analysis are presented in Section 4. Section 5 shows the performance evaluation of BCPay. In Section 6, we present several applications of BCPay. Finally, concluding remarks are made in Section 7.

2. Preliminaries

In this section, we first list some notations and then briefly review blockchains and Bitcoin-based timed commitments.

2.1. Notations

In Table 1, we present notations mainly used in BCPay.

Table 1: Notations used in BCPay.

$\mathcal{C}$	The client	$I_{i,j}$	The hash value of the j-th node with height i in $\mathcal{T}_\ell$
$\mathcal{S}$	The server		
H	A hash function	σ_{root}	The ECDSA signature of the root of $\mathcal{T}_\ell$
r_S	The secret of $\mathcal{S}$		
h_S	The hash value $H(r_S)$	chal	A challenge-related hash value set used in the service checking
t	A time-lock		
$\mathcal{T}_\ell$	A service data tree	chal_0	A challenge-related variable set used in the service checking
ℓ	The height of $\mathcal{T}_\ell$		
(pk_A, sk_A)	An ECDSA key pair of A	$\mathsf{ChalIndex}$	A challenge-related index set used in the service checking
data_0	Service-related local data		
data_1	The outsourcing data	$\max_B$	The maximal delay between broadcasting a transaction and including it on the blockchain
$\mathsf{chaldata}$	A challenge (data indexes)		
D_i	The i-th data block in data_1		

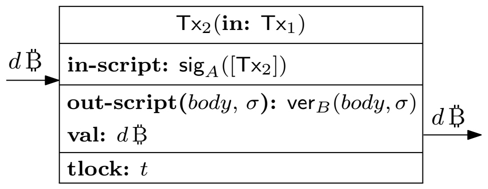

Tx_2(**in:** Tx_1)
d฿
in-script: $\mathsf{sig}_A([\mathsf{Tx}_2])$
out-script($body$, σ): $\mathsf{ver}_B(body, \sigma)$
val: d฿
d฿
tlock: t

Figure 1: An example of transaction.

2.2. Blockchain

The blockchain is an essential technology behind many cryptocurrencies, with Bitcoin and Ethereum as the two most widely used ones. The idea of the blockchain is that the longest chain is accepted as the proper one. In the following, we describe blockchain in terms of the Bitcoin currency system, including addresses and transactions.

As an important ingredient of the Bitcoin system, the ECDSA signature is associated with a public-secret key pair (pk, sk). Technically, an address is a hash of a public key pk. To keep the exposition as simple as possible, we use pk to represent an address. Suppose a user A has a key pair (pk_A, sk_A), then $\mathsf{sig}_A(m)$ denotes the ECDSA signature on a message m associated with sk_A, and $\mathsf{vec}_A(m, \sigma)$ denotes the result of the verification of the ECDSA signature σ on the message m with regard to pk_A. The most general form of a Bitcoin transaction Tx_x is

$$((y_1, a_1, \sigma_1), \cdots, (y_n, a_n, \sigma_n), (v_1, \pi_1), \cdots, (v_m, \pi_m), t).$$

The inputs of Tx_x are triples $(y_1, a_1, \sigma_1), \cdots, (y_n, a_n, \sigma_n)$, where y_i is the hash of some previous transaction Tx_{y_i}, a_i is an index of the output of Tx_{y_i} and σ_i is called an input script. The outputs of Tx_x are a list of pairs $(v_1, \pi_1), \cdots, (v_m, \pi_m)$, where v_i is the value of the i-th output of Tx_x and π_i is an output script. In particular, t is a time-lock, which means that Tx_x is valid only if time t is reached. In Ethereum, similar mechanisms can be realized based on the Ethereum Alarm Clock [38]. Furthermore, the body of Tx_x is denoted as

$$[\mathsf{Tx}_x] = ((y_1, a_1), \cdots, (y_n, a_n), (v_1, \pi_1), \cdots, (v_m, \pi_m), t),$$

which is equal to Tx_x without the input script. The transaction Tx_x is valid if $\pi'_i([\mathsf{Tx}_x], \sigma_i)$ evaluates to true for $1 \leq i \leq n$, where π'_i is the output script of the a_i-th output of Tx_{y_i}. The scripts are written in the Bitcoin scripting language, which is a stack based, not Turing-complete language. In Figure 1, as an example of transactions, the user A aims to transfer d฿ from Tx_1 to the user B after time t based on Tx_2, where the output script is an ECDSA signature verification. Similar to [2, 1], to keep the exposition simple we present our results assuming that the transaction fees are zero.

2.3. Bitcoin-based Timed Commitment

In BCPay, the bitcoin-based timed commitment scheme [2] is used, which is also adopted by [6, 28]. The commitment scheme is denoted by $\mathsf{CS}(\mathcal{S}, \mathcal{C}, d, t, s)$ and is

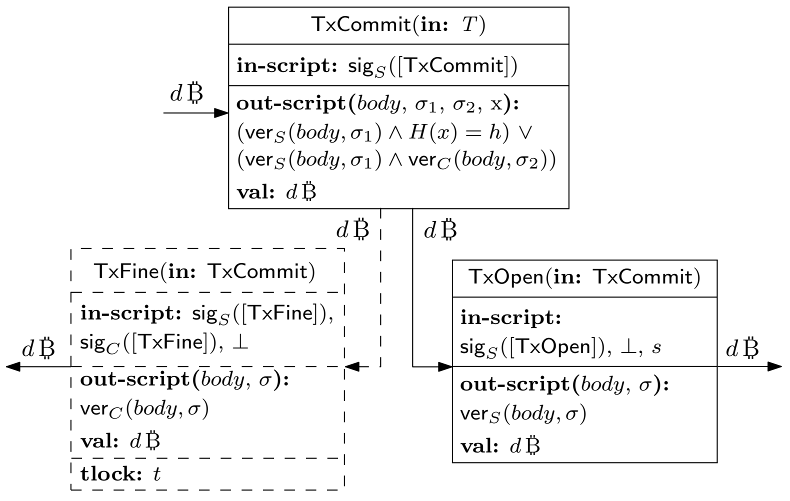

TxCommit(in: T)
in-script: $\mathsf{sig}_S([\mathsf{TxCommit}])$
out-script($body$, σ_1, σ_2, x):
$(\mathsf{ver}_S(body,\sigma_1) \wedge H(x)=h) \vee$
$(\mathsf{ver}_S(body,\sigma_1) \wedge \mathsf{ver}_C(body,\sigma_2))$
val: d฿
d฿
TxFine(in: TxCommit)
in-script: $\mathsf{sig}_S([\mathsf{TxFine}])$, $\mathsf{sig}_C([\mathsf{TxFine}])$, $\perp$
out-script($body$, σ):
$\mathsf{ver}_C(body,\sigma)$
val: d฿
tlock: t
TxOpen(in: TxCommit)
in-script: $\mathsf{sig}_S([\mathsf{TxOpen}])$, $\perp$, s
out-script($body$, σ):
$\mathsf{ver}_S(body,\sigma)$
val: d฿

Figure 2: The transactions involved in bitcoin-based timed commitments.

executed between $\mathcal{S}$ and $\mathcal{C}$, where the outsourcing service provider $\mathcal{S}$ acts as a committer and the outsourcing service client $\mathcal{C}$ acts as a receipt. Concretely, $\mathcal{S}$ commits to a secret s and has to open the commitment before a specific time t to get his/her deposit of value d฿ back. Otherwise, the deposit will be given to $\mathcal{C}$. The commitment scheme consists of three phases: the commitment phase $\mathsf{CS.Commit}(\mathcal{S},\mathcal{C},d,t,s)$, the opening phase $\mathsf{CS.Open}(\mathcal{S},\mathcal{C},d,t,s)$ and the punishment phase $\mathsf{CS.Fine}(\mathcal{S},\mathcal{C},d,t,s)$. Note that the punishment phase is performed only if the opening phase is not correctly performed. Three transactions $\mathsf{TxCommit}$, TxOpen and TxFine, as shown in Figure 2, are involved in the commitment phase, the opening phase and the punishment phase, respectively. In Figure 2, the omitted arguments of scripts are denoted by $\perp$ and H is a hash function. Please refer to [2] for more details.

3. System Architecture, Specifications and Adversary Model

In this section, we first present the system architecture and specifications of BCPay. Then, the adversary model and design goals of BCPay are described in detail.

3.1. System Architecture of BCPay

The system architecture of BCPay is illustrated in Figure 3, and it involves clients (i.e., users), servers (i.e., outsourcing service providers) and a blockchain. In the rest of this paper, we use $\mathcal{C}$ and $\mathcal{S}$ to denote a client and a server, respectively. Suppose $\mathcal{C}$ plans to subscribe to an outsourcing service sv from $\mathcal{S}$. To keep the presentation compact, we only show the main procedures of BCPay in Figure 3. The procedures (1), (2), (3.1) and (3.2) are used to implement sv. The procedures (4), (5), (6.1) and (6.2) are used to check the sv implementation and the checking result is reflected in the service payment (7) or the service claim (8). In BCPay, a public blockchain is considered, such as the Bitcoin blockchain and the Ethereum blockchain. The entities $\mathcal{C}$ and $\mathcal{S}$ are detailed as follows:

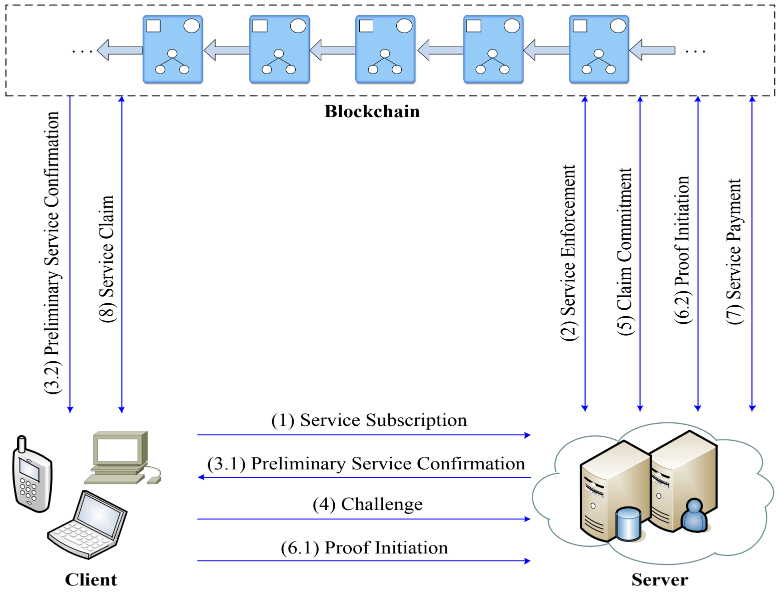


Figure 3: The system architecture of BCPay.

- *Client* $\mathcal{C}$: As a user, $\mathcal{C}$ subscribes to an outsourcing service sv from $\mathcal{S}$. After sv is enforced by $\mathcal{S}$, $\mathcal{C}$ can get a preliminary service confirmation from $\mathcal{S}$ based on the blockchain. In order to check the implementation of sv before the payment, $\mathcal{C}$ sends a challenge to $\mathcal{S}$. $\mathcal{S}$ first makes a claim commitment to ensure that $\mathcal{C}$ will get enough compensation in the form of deposits if $\mathcal{S}$ is malicious. Then, $\mathcal{C}$ and $\mathcal{S}$ jointly initiate the service implementation proof by specifying some requirements of sv. If $\mathcal{S}$ fails to provide a valid service proof that the service implementation meets the requirements before a specific time, $\mathcal{C}$ can claim enough deposits by himself from $\mathcal{S}$.

- *Server* $\mathcal{S}$: As an outsourcing service provider, $\mathcal{S}$ aims to earn service fees from $\mathcal{C}$ by enforcing services subscribed by $\mathcal{C}$. Upon receiving the service subscription request from $\mathcal{C}$, $\mathcal{S}$ completes the enforcement of sv based on the blockchain and sends to $\mathcal{C}$ a preliminary confirmation message. Then, $\mathcal{S}$ makes the claim commitment after receiving the challenge from $\mathcal{C}$. Once the joint proof initiation is finished, $\mathcal{S}$ provides a valid service implementation proof to get the service fee from $\mathcal{C}$ in the service payment phase before the specific time.

3.2. Specifications of BCPay

BCPay consists of five phases: the system setup phase, the service implementation phase, the service checking phase, the service payment phase and the service claim phase. The first four phases are compulsory and the service claim phase is performed by $\mathcal{C}$ only if $\mathcal{S}$ is malicious[2]. The details of the specifications of BCPay are as follows:

3.2.1. System Setup Phase

$\mathcal{C}$ and $\mathcal{S}$ initialize some parameters such as unredeemed transactions on the blockchain to be used in the subsequent phases.

3.2.2. Service Implementation Phase

The outsourcing service sv is implemented in this phase. Three procedures, service subscription, service enforcement and preliminary service confirmation, are sequentially performed as below.

- *Service Subscription:* $\mathcal{C}$ subscribes to sv from $\mathcal{S}$ by sending service-related data to $\mathcal{S}$.

- *Service Enforcement:* In this procedure, sv is enforced by $\mathcal{S}$. Upon receiving the subscription data from $\mathcal{C}$, $\mathcal{S}$ enforces sv. Then, $\mathcal{S}$ generates a digital signature according to the enforcement of sv and stores the signature on the blockchain. Finally, $\mathcal{S}$ sends a confirmation message to $\mathcal{C}$ that helps $\mathcal{C}$ to obtain the signature from the blockchain.

- *Preliminary Service Confirmation:* After obtaining the signature from the blockchain, $\mathcal{C}$ considers that sv has been preliminarily implemented, where "preliminarily" means that the sv implementation will be checked by $\mathcal{C}$ before the payment.

3.2.3. Service Checking Phase

This phase is used by $\mathcal{C}$ and $\mathcal{S}$ to jointly initiate the service checking. In this phase, the service requirements are specified. Three sequential sub-phases, challenge generation phase, claim commitment phase and proof initiation phase, are performed as below.

- *Challenge Generation Phase:* In order to check the sv implementation, $\mathcal{C}$ sends a challenge to $\mathcal{S}$ besides reaching an agreement beforehand on service-related parameters such as the compensation and penalty of $\mathcal{S}$ in the case of service failure.

- *Claim Commitment Phase:* This phase is used by $\mathcal{S}$ to make a commitment that once the sv implementation does not meet the requirements specified in the *Proof Initiation Phase* and the malicious $\mathcal{S}$ refuses to compensate $\mathcal{C}$ in the *Service Payment Phase* before a specific time, $\mathcal{C}$ is able to claim enough deposits of $\mathcal{S}$ by himself/herself as a penalty in the *Service Claim Phase* after the specific time.

[2]Strictly speaking, we mean $\mathcal{S}$ fails to provide a valid service implementation proof.

- *Proof Initiation Phase:* This phase is used by $\mathcal{C}$ and $\mathcal{S}$ to realize the service checking by temporarily freezing a joint deposit consists of service fee and guaranty respectively from $\mathcal{C}$ and $\mathcal{S}$, in which the requirements of sv are agreed upon. After this phase, honest $\mathcal{C}$ can ensure that either a valid sv is achieved in the *Service Payment Phase* by paying the service fee or enough deposits are claimed in the *Service Claim Phase* no matter how $\mathcal{S}$ behaves. On the other hand, honest $\mathcal{S}$ can ensure that if the sv implementation is valid, he/she will earn the service fee no matter how $\mathcal{C}$ behaves.

3.2.4. Service Payment Phase

This phase is performed by $\mathcal{S}$ to earn the service fee from $\mathcal{C}$ by proving that the sv implementation meets the requirements. Certainly, $\mathcal{C}$ can ensure that the service fee is paid only if the sv implementation is what is expected.

3.2.5. Service Claim Phase

Only if $\mathcal{S}$ fails to prove that the sv implementation meets the requirements of $\mathcal{C}$ before a specific time, BCPay comes to the *Service Claim Phase.* This phase is used by $\mathcal{C}$ to claim enough deposits from $\mathcal{S}$ no matter how $\mathcal{S}$ behaves.

3.3. Adversary Model and Design Goals of BCPay

In BCPay, both $\mathcal{C}$ and $\mathcal{S}$ can be malicious and they are of mutual distrust. Concretely, malicious $\mathcal{C}$ aims to enjoy the outsourcing service sv provided by $\mathcal{S}$ without paying the service fee while malicious $\mathcal{S}$ tries to get the service fee from $\mathcal{C}$ without implementing the service sv as specified in the requirements of $\mathcal{C}$. As for the blockchain, its contents are publicly available and both $\mathcal{C}$ and $\mathcal{S}$ can verify the authenticity of data in the blockchain.

In addition, no private channels are required in BCPay. Hence, eavesdropping attacks and malleability attacks should be taken into consideration. In these attacks, the adversary aims to undermine the fairness in BCPay.

- *Eavesdropping Attacks:* The adversary can eavesdrop on the public channel to see the transactions sent by the honest party, before they appear on the blockchain.

- *Malleability Attacks:* Based on the eavesdropping, the adversary tries to make some transactions invalid by modifying their hash values without changing the semantics.

In BCPay, our security goals mainly include soundness and robust fairness as follows[3].

- *Soundness:* If both $\mathcal{C}$ and $\mathcal{S}$ are honest, then $\mathcal{C}$ can obtain the required service implementation and $\mathcal{S}$ can gain the corresponding service fee.

[3]Because the design of BCPay does not change the underlying blockchains, traditional attacks on blockchains, such as 51% attacks and Sybil attacks, are not considered in BCPay.

- *Robust Fairness:* The fairness means that it is infeasible for the malicious $\mathcal{C}$ to enjoy the outsourcing service sv provided by $\mathcal{S}$ without paying the service fee and it is infeasible for the malicious $\mathcal{S}$ to get the service fee paid by $\mathcal{C}$ without providing a valid sv implementation proof in terms of the requirements of $\mathcal{C}$ before a specific time. Particularly, if malicious $\mathcal{S}$ fails to provide such a proof, $\mathcal{C}$ is able to get enough compensation or penalty from $\mathcal{S}$. Robust fairness means that the fairness is resilient to eavesdropping attacks and malleability attacks, without needing a third-party.

Furthermore, from the standpoint of efficiency, both the number of involved transactions and computation cost should be considered.

- *Number of Transactions:* The number of transactions involved in BCPay should be as small as possible.

- *Computation Cost:* The computation cost of BCPay should be as low as possible considering resource-constrained users.

4. BCPay: Blockchain-based Fair Payment Framework

In this section, we first present the main idea of BCPay, and then describe the design details of BCPay together with its security results.

4.1. Challenge and Main Idea

According to the adversary model and design goals in Section 3.3, the main challenge to design BCPay is *Robust Fairness* besides efficiency. The basic idea for realizing *Robust Fairness* is as follows.

In the service implementation phase, $\mathcal{S}$ constructs a Merkle tree based on the data from $\mathcal{C}$ and generates a signature on the root of the tree. The signature is then stored on the blockchain, which cannot be changed later, and acts as a "root of trust" in the service checking and payment. The ingredient of ensuring fairness is an **all-or-nothing** checking-proof protocol $\mathcal{CP}_{\mathrm{AON}}$. The idea of $\mathcal{CP}_{\mathrm{AON}}$ lies in two aspects:

1. $\mathcal{S}$ is able to earn the service fee from $\mathcal{C}$ and get his/her guaranty back if and only if he/she provides a valid service implementation proof, denoted as $\mathsf{ServiceProof}$;

2. If $\mathcal{S}$ fails to provide such a proof before a specific time t, $\mathcal{C}$ is able to claim from $\mathcal{S}$ either enough compensation together with his/her service fee refund or enough fines in the form of deposit.

In order to achieve these goals, in BCPay, $\mathcal{C}$ and $\mathcal{S}$ jointly create a deposit transaction $\mathsf{TxProofInit}$, which consists of the service fee from $\mathcal{C}$ and the guaranty from $\mathcal{S}$. In the normal case, $\mathsf{TxProofInit}$ can be completely redeemed by $\mathcal{S}$ based on his/her signature and $\mathsf{ServiceProof}$, and hence the *Soundness* is realized. If $\mathcal{S}$ cannot provide $\mathsf{ServiceProof}$, $\mathsf{TxProofInit}$ can be completely redeemed by $\mathcal{C}$ based on his/her signature and a secret r_S from $\mathcal{S}$. If r_S is replaced with the signature of $\mathcal{S}$, BCPay may suffer from malleability attacks. Because BCPay does not use private channels, $\mathsf{ServiceProof}$ may be eavesdropped by $\mathcal{C}$ before honest $\mathcal{S}$ gets the service fee. As a result, malicious $\mathcal{C}$ can redeem $\mathsf{TxProofInit}$ before honest $\mathcal{S}$, which violates (1) mentioned above. To overcome this problem, in BCPay, $\mathcal{S}$ just makes r_S public after redeeming $\mathsf{TxProofInit}$. Certainly, in this case, malicious $\mathcal{S}$ will not publicize r_S even if he/she fails to provide $\mathsf{ServiceProof}$, and hence $\mathcal{C}$ cannot redeem $\mathsf{TxProofInit}$ to claim compensation, which violates (2) mentioned above. To tackle this issue, in BCPay, $\mathcal{S}$ is required to make a commitment to r_S based on a deposit transaction $\mathsf{TxClaimCommitment}$. The commitment must be opened by $\mathcal{S}$ before time t to redeem $\mathsf{TxClaimCommitment}$. Otherwise, $\mathcal{C}$ can redeem $\mathsf{TxClaimCommitment}$ himself as a punishment to $\mathcal{S}$ after time t. Note that, the order among the involved transactions and the use of r_S make BCPay malleability-resistant.

In addition, to ensure the efficiency of BCPay, we aim to introduce small and constant number of transactions in a service implementation checking and proof. In fact, based on the "root of trust" constructed by $\mathcal{S}$ in the service implementation phase, $\mathcal{C}$ is able to specify the service requirements in terms of the authentication path of the Merkle tree. That is, the service implementation checking can be accomplished in one round $\mathcal{CP}_{\text{AON}}$. Hence, the efficiency of BCPay is assured.

4.2. Design Details of BCPay

As we know, the Bitcoin script is simple, stack-based and purposefully not Turing-complete. Unlike the Bitcoin protocol, the Ethereum is a programmable blockchain and it allows users to create their own operations of any complexity they wish [10, 44, 19]. In other words, the Ethereum blockchain is more flexible than the Bitcoin blockchain. However, in order to achieve easy understanding and keep the exposition simple, we present BCPay following the style of Bitcoin transactions in the same way as [2, 1, 6, 28]. Now, we present the details of BCPay.

4.2.1. System Setup Phase

Let H be a cryptographic hash function, such as SHA-256. A secure symmetric encryption algorithm should be chosen for specific services if necessary, such as the PDP service. For simple exposition, we assume $\mathcal{C}$ and $\mathcal{S}$ choose their own ECDSA public-secret key pairs, denoted by (pk_C, sk_C) and (pk_S, sk_S), respectively. $\mathcal{S}$ prepares an unredeemed transaction $\mathsf{Tx}_{\text{sig}}^{S}$ of value d_{sig} ₿, which can be redeemed with sk_S.

4.2.2. Service Implementation Phase

In order to realize the outsourcing service sv, the following three procedures are performed.

- *Service Subscription:* $\mathcal{C}$ preprocesses service-related local data data_0 and sends the result data_1 to $\mathcal{S}$ for subscribing to sv. Note that the preprocessing is specified by

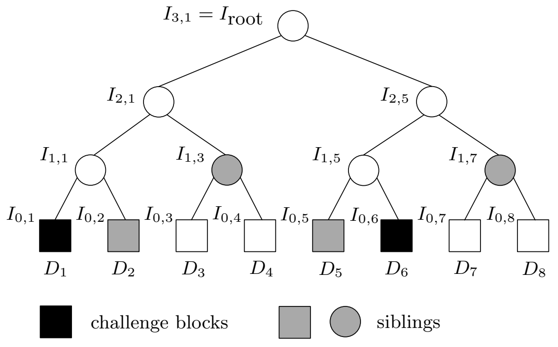


Figure 4: The example of $\mathcal{T}_3$.

concrete outsourcing services. For example, PDP involves encryption and hashing. Without loss of generality, suppose data_1 consists of $n = 2^\ell$ data blocks and $\mathsf{data}_1 = \{D_1, D_2, \cdots, D_{2^\ell}\}$.

- *Service Enforcement:* Upon receiving the subscription data data_1 from $\mathcal{C}$, $\mathcal{S}$ first enforces sv based on data_1. In order to prove the sv implementation to $\mathcal{C}$ and earn the service fee in the subsequent phases, a Merkle tree $\mathcal{T}_\ell$ is built by $\mathcal{S}$ after the service enforcement, where ℓ denotes the height of the tree and the leaf nodes have a height of 0. In $\mathcal{T}_\ell$, each interior node has a hash value. For $1 \leq i \leq \ell$, the j-th node of height i has a value

$$I_{i,j} = H(I_{i-1,j} \parallel I_{i-1,j+2^{i-1}}),$$

  where $I_{i-1,j}$ and $I_{i-1,j+2^{i-1}}$ represent the hash values of the left child and the right child of $I_{i,j}$, respectively. Furthermore, if $i = \ell$, $I_{i,j} = I_{\ell,1}$ is the root node, which is also denoted by I_{root}. If $1 \leq i < \ell$ and $I_{i,j}$ is a left child, then its right sibling is $I_{i,j+2^i}$. Otherwise, $I_{i,j}$ is a right child and its left sibling is $I_{i,j-2^i}$. If $i = 0$, $I_{i,j} = I_{0,j}$ represents the j-th leaf and $I_{0,j} = D_j$. As an example, $\mathcal{T}_3$ is shown in Figure 4. Subsequently, $\mathcal{S}$ computes a signature $\sigma_{\text{root}} = \mathsf{sig}_{\mathcal{S}}(I_{\text{root}})$, and stores σ_{root} on the blockchain by broadcasting a service signature transaction $\mathsf{TxServiceSig}$ shown in Figure 5. Here, σ_{root} is publicly output by $\mathsf{TxServiceSig}$ based on the opcode $\mathsf{OP\_RETURN}$ of Bitcoin transactions.[4] Finally, $\mathcal{S}$ sends the transaction ID to $\mathcal{C}$.

- *Preliminary Service Confirmation:* Upon receiving the transaction ID from $\mathcal{S}$, $\mathcal{C}$ first locates $\mathsf{TxServiceSig}$ on the blockchain and gets σ_{root} from $\mathsf{OP\_RETURN}$. Then, $\mathcal{C}$ computes I_{root} based on data_1. If $\mathsf{vec}_{\mathcal{S}}(I_{\text{root}}, \sigma_{\text{root}}) = \mathsf{true}$, $\mathcal{C}$ thinks sv has been preliminarily implemented. According to context of the concrete service under consideration, $\mathcal{C}$ could immediately delete data_1 or store data_1 till a successful service

[4]In the Ethereum blockchain, each transaction has a data field `data`, which can also be used to store σ_{root} on the blockchain.

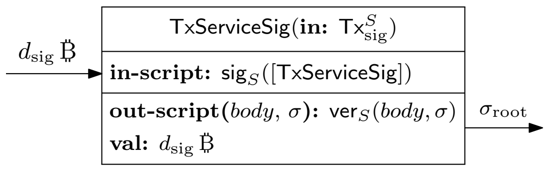

$\mathsf{TxServiceSig}(\textbf{in: } \mathsf{Tx}_{\mathrm{sig}}^{S})$
d_{sig} ฿
in-script: $\mathsf{sig}_S([\mathsf{TxServiceSig}])$
out-script$(body, \sigma)$**:** $\mathsf{ver}_S(body, \sigma)$
σ_{root}
val: d_{sig} ฿

Figure 5: The service signature transaction TxServiceSig.

checking proof. In any case, $\mathcal{C}$ should store ℓ as metadata, which will be used to specify the service requirements.

4.2.3. Service Checking Phase

In this phase, $\mathcal{C}$ and $\mathcal{S}$ jointly initiate the service checking based on three sequential sub-phases: the *Challenge Generation Phase*, the *Claim Commitment Phase* and the *Proof Initiation Phase*. Suppose there is an unredeemed transaction Tx_0^S of value d_0 ฿, which can be redeemed by $\mathcal{S}$ and is used as the penalty of $\mathcal{S}$ in the case of service failure.

- *Challenge Generation Phase:* To check the sv implementation, $\mathcal{C}$ sends a challenge $\mathsf{chaldata}$ to $\mathcal{S}$, which specifies the data blocks to be challenged in $\mathcal{T}_\ell$. Suppose

$$\mathsf{chaldata} = (k_1, k_2, \cdots, k_c),$$

which sequentially specifies data blocks $\{D_{k_j}\}_{1 \le j \le c}$. For each $k \in \mathsf{chaldata}$, denote by path_k the path from the leaf node $I_{0,k}$ to the root I_{root} of $\mathcal{T}_\ell$, and by $\mathsf{AuthenPath}_k$ the authentication path of $I_{0,k}$. To be specific, $\mathsf{AuthenPath}_k$ consists of $I_{0,k}$ and the sibling nodes corresponding to $I_{0,k}$ and the interior nodes on path_k. Define

$$\mathsf{AuthenPath} = \bigcup_{k \in \mathsf{chaldata}} \mathsf{AuthenPath}_k - \bigcup_{k \in \mathsf{chaldata}} (\mathsf{path}_k - I_{0,k}).$$

Denote by chal the ordered version of $\mathsf{AuthenPath}$ such that a node with a smaller first index and a smaller second index is placed in the front. Formally, given $I_{i_1,j_1}, I_{i_2,j_2} \in \mathsf{chal}$, I_{i_1,j_1} is in front of I_{i_2,j_2} if $i_1 < i_2$ or $(i_1 = i_2 \wedge j_1 < j_2)$. In addition, denote the challenge index set by $\mathsf{ChalIndex} = \{(i,j)\}_{I_{i,j} \in \mathsf{chal}}$. For example, in Figure 4, $\mathsf{chaldata} = (1, 6)$, and

$$\begin{aligned}
\mathsf{path}_1 &= \{I_{0,1}, I_{1,1}, I_{2,1}, I_{3,1}\},\\
\mathsf{path}_6 &= \{I_{0,6}, I_{1,5}, I_{2,5}, I_{3,1}\},\\
\mathsf{AuthenPath}_1 &= \{I_{0,1}, I_{0,2}, I_{1,3}, I_{2,5}\},\\
\mathsf{AuthenPath}_6 &= \{I_{0,6}, I_{0,5}, I_{1,7}, I_{2,1}\},\\
\mathsf{chal} &= \{I_{0,1}, I_{0,2}, I_{0,5}, I_{0,6}, I_{1,3}, I_{1,7}\},\\
\mathsf{ChalIndex} &= \{(0,1), (0,2), (0,5), (0,6), (1,3), (1,7)\}.
\end{aligned}$$

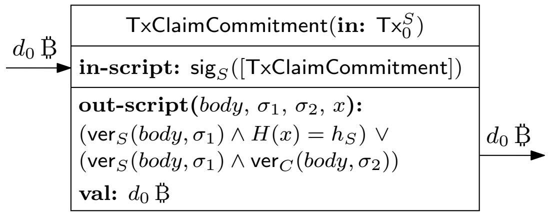

d_0 ₿
TxClaimCommitment(**in:** Tx_0^S)
in-script: sig_S([TxClaimCommitment])
out-script($body$, σ_1, σ_2, x)**:**
$(\mathsf{ver}_S(body, \sigma_1) \wedge H(x) = h_S) \vee$
$(\mathsf{ver}_S(body, \sigma_1) \wedge \mathsf{ver}_C(body, \sigma_2))$
val: d_0 ₿
d_0 ₿

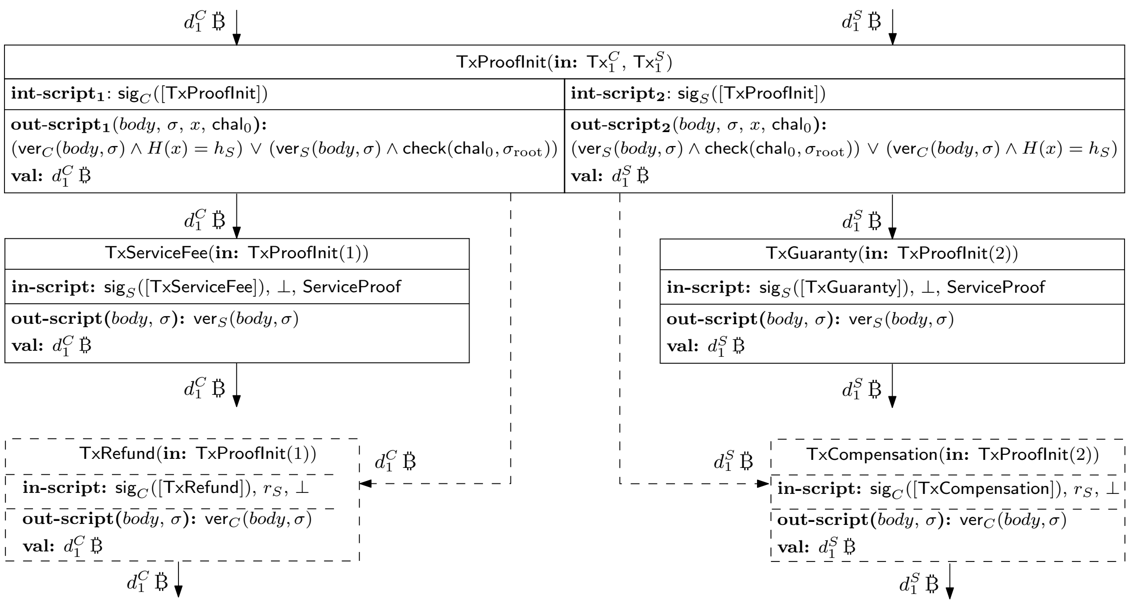
Figure 6: The claim commitment transaction TxClaimCommitment.

Note that ChalIndex can be computed by $\mathcal{C}$ based on the metadata ℓ without knowing chal. Furthermore, suppose there are unredeemed transactions Tx_1^S of value d_1^C ₿ and Tx_1^S of value d_1^S ₿, which can be redeemed by $\mathcal{C}$ and $\mathcal{S}$, respectively. In order to force $\mathcal{S}$ to compensate $\mathcal{C}$ before a specific time once sv fails, let $d_0 \geq d_1^C + d_1^S$. Here, d_1^C ₿ and d_1^S ₿ denote the service fee of $\mathcal{C}$ and the compensation of $\mathcal{S}$ in the case of service failure, respectively.

- *Claim Commitment Phase:* Upon receiving chaldata, $\mathcal{S}$ performs $\mathsf{CS.Commit}(\mathcal{S}, \mathcal{C}, d_0, t, r_S)$, where t is a specific time and $r_S \in_R \{0,1\}^*$. Specifically, $\mathcal{S}$ posts a deposit transaction TxClaimCommitment of value d_0 ₿ on the blockchain, which makes a commitment that once the sv implementation does not meet the requirements specified in the *Proof Initiation Phase* and malicious $\mathcal{S}$ refuses[5] to compensate $\mathcal{C}$ in the *Service Payment Phase* before time t, $\mathcal{C}$ is able to claim d_0 ₿ of $\mathcal{S}$ by himself/herself as a penalty in the *Service Claim Phase* after time t. After TxClaimCommitment is included on the blockchain, $\mathcal{S}$ creates the body of the punishment transaction TxFine, which will be used by $\mathcal{C}$ to claim the penalty, signs it and sends the signed body sig_S([TxFine]) to $\mathcal{C}$. The details of TxClaimCommitment are shown in Figure 6, where $h_S = H(r_S)$. TxOpen and TxFine will be detailed in the *Service Payment Phase* and the *Service Claim Phase*, respectively. Certainly, if the sv implementation is valid, $\mathcal{S}$ will eventually get his/her deposit back no matter how $\mathcal{C}$ behaves.

- *Proof Initiation Phase:* If TxClaimCommitment is included on the blockchain with enough confirmations and the signature sig_S([TxFine]) is received, $\mathcal{C}$ initiates the service proof request based on ChalIndex and σ_{root}, which can be obtained from the blockchain. Generally speaking, $\mathcal{C}$ chooses a single variable x and a variable set $\mathsf{chal}_0 = \{x_{i,j}\}_{(i,j)\in\mathsf{ChalIndex}}$, which can be chosen by $\mathcal{S}$ based on chaldata and $\mathcal{T}_\ell$. Also, $\mathcal{C}$ and $\mathcal{S}$ jointly make a deposit transaction TxProofInit, which specifies the requirements of sv implementation and is finally posted on the blockchain by $\mathcal{S}$. The idea of joint deposit has been used in [2, 1]. The joint deposit in TxProofInit consists of the service fee d_1^C ₿ from $\mathcal{C}$ and the guaranty d_1^S ₿ from $\mathcal{S}$, where the guaranty is used as the compensation in the *Service Claim Phase*. Please find the

[5]Refusing to compensate means that $\mathcal{S}$ does not redeem TxClaimCommitment based on the opening transaction TxOpen before time t, that is, r_S is not revealed by $\mathcal{S}$ before time t.



d_1^C ฿
d_1^S ฿
TxProofInit(**in:** Tx_1^C, Tx_1^S)
int-script₁: sig_C([TxProofInit])
int-script₂: sig_S([TxProofInit])
out-script₁($body$, σ, x, chal_0): $(\mathsf{ver}_C(body,\sigma) \wedge H(x)=h_S) \vee (\mathsf{ver}_S(body,\sigma) \wedge \mathsf{check}(\mathsf{chal}_0,\sigma_{\text{root}}))$
val: d_1^C ฿
out-script₂($body$, σ, x, chal_0): $(\mathsf{ver}_S(body,\sigma) \wedge \mathsf{check}(\mathsf{chal}_0,\sigma_{\text{root}})) \vee (\mathsf{ver}_C(body,\sigma) \wedge H(x)=h_S)$
val: d_1^S ฿
TxServiceFee(**in:** TxProofInit(1))
in-script: sig_S([TxServiceFee]), $\perp$, ServiceProof
out-script($body$, σ): $\mathsf{ver}_S(body,\sigma)$
val: d_1^C ฿
TxGuaranty(**in:** TxProofInit(2))
in-script: sig_S([TxGuaranty]), $\perp$, ServiceProof
out-script($body$, σ): $\mathsf{ver}_S(body,\sigma)$
val: d_1^S ฿
TxRefund(**in:** TxProofInit(1))
in-script: sig_C([TxRefund]), r_S, $\perp$
out-script($body$, σ): $\mathsf{ver}_C(body,\sigma)$
val: d_1^C ฿
TxCompensation(**in:** TxProofInit(2))
in-script: sig_C([TxCompensation]), r_S, $\perp$
out-script($body$, σ): $\mathsf{ver}_C(body,\sigma)$
val: d_1^S ฿

Figure 7: The transactions involved in the service implementation checking and proof of BCPay

details of TxProofInit in Figure 7, in which $\mathsf{check}(\mathsf{chal}_0, \sigma_{\text{root}}) \triangleq \mathsf{vec}_S(I^*_{\text{root}}, \sigma_{\text{root}})$ and I^*_{root} is computed based on chal_0 in the same way as I_{root} is computed based on chal according to the construction of $\mathcal{T}_\ell$. Obviously, hashing and ECDSA signature verification are involved in the output script. More details of the service proof are given based on a checking-proof protocol $\mathcal{CP}_{\text{AON}}$ performed by $\mathcal{C}$ and $\mathcal{S}$, which is described in Figure 8 and additionally involves the *Service Payment Phase* and the *Service Claim Phase*. We call $\mathcal{CP}_{\text{AON}}$ an **all-or-nothing** protocol in the sense that either the service fee and the guaranty are redeemed by $\mathcal{S}$ at the same time or more deposit of $\mathcal{S}$ will be paid to $\mathcal{C}$.

4.2.4. Service Payment Phase

In this phase, if $\mathcal{S}$ can provide a valid proof ServiceProof before the specific time $t - 2\max_B$ to prove that the sv implementation meets the requirements, $\mathcal{S}$ can earn the service fee d_1^C ฿ of $\mathcal{C}$ and get his/her guaranty d_1^S ฿ back by redeeming TxProofInit based on TxServiceFee and TxGuaranty, respectively. The transactions TxServiceFee and TxGuaranty are shown in Figure 7. Furthermore, $\mathcal{S}$ performs $\mathsf{CS.Open}(\mathcal{S}, \mathcal{C}, d_0, t, r_S)$, in which $\mathcal{S}$ opens the claim commitment made in the *Claim Commitment Phase* by posting the opening transaction TxOpen on the blockchain before time t. The details of TxOpen are shown in Figure 9. Note that TxOpen redeems TxClaimCommitment and hence $\mathcal{S}$ can get his/her commitment deposit back. Finally, $\mathcal{S}$ quits.

4.2.5. Service Claim Phase

Suppose $\mathcal{S}$ fails to provide a valid service implementation proof ServiceProof in the *Service Payment Phase* before time $t - 2\max_B$, BCPay comes to the *Service Claim*

$\mathcal{CP}_{\mathrm{AON}}(\mathcal{C}, \mathcal{S}, \{\mathsf{Tx}_1^C, d_1^C\}, \{\mathsf{Tx}_1^S, d_1^S\}, \sigma_{\mathrm{root}}, h_S)$:

$\mathcal{C}$ and $\mathcal{S}$ do the following:

(1) Both $\mathcal{C}$ and $\mathcal{S}$ compute the body of the transaction TxProofInit using Tx_1^C and Tx_1^S as inputs.

(2) $\mathcal{C}$ signs the transaction TxProofInit and sends the signature $\mathsf{sig}_C([\mathsf{TxProofInit}])$ to $\mathcal{S}$. According to the definition of check, $\mathcal{C}$ does not need to know I_{root}.

(3) If $\mathcal{S}$ does not receive $\mathsf{sig}_C([\mathsf{TxProofInit}])$ before time $t - 4\max_B$, where $\max_B$ is the maximal delay between broadcasting a transaction and including it on the blockchain, then $\mathcal{S}$ redeems Tx_1^S and quits. Otherwise, $\mathcal{S}$ signs TxProofInit and broadcasts it.

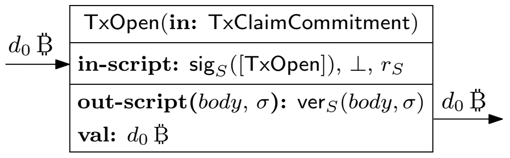
(4) $\mathcal{C}$ waits until TxProofInit is included on the blockchain. If TxProofInit is not included on the blockchain before time $t - 3\max_B$, $\mathcal{C}$ immediately redeems Tx_1^C and quits.

(5) $\mathcal{S}$ provides the service proof ServiceProof, and broadcasts TxServiceFee and TxGuaranty to earn the service fee d_1^C ₿ and get back the guaranty d_1^S ₿, respectively.

(6) If ServiceProof cannot pass check before time $t - 2\max_B$, $\mathcal{C}$ performs the *Service Claim Phase.*

(7) Otherwise, ServiceProof passes check before time $t - 2\max_B$, and hence $\mathcal{C}$ obtains a valid outsourcing service from $\mathcal{S}$. $\mathcal{C}$ quits and $\mathcal{S}$ opens his/her commitment.

Figure 8: The all-or-nothing checking-proof protocol $\mathcal{CP}_{\mathrm{AON}}$.



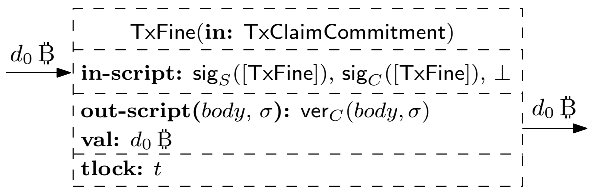
d_0 ₿
TxOpen(**in:** TxClaimCommitment)
in-script: $\mathsf{sig}_S([\mathsf{TxOpen}])$, $\perp$, r_S
out-script($body$, σ)**:** $\mathsf{ver}_S(body, \sigma)$
val: d_0 ₿
d_0 ₿

Figure 9: The opening transaction TxOpen.

Phase. In this phase, $\mathcal{C}$ is able to get enough deposit from $\mathcal{S}$ no matter how $\mathcal{S}$ behaves. Two cases should be taken into account.

- *Case 1.* $\mathcal{S}$ refuses to pay the compensation d_1^S ₿ to $\mathcal{C}$, that is, $\mathcal{S}$ does not open the claim commitment made in the *Claim Commitment Phase* and TxOpen is not included on the blockchain before time t. In this case, $\mathcal{C}$ performs $\mathsf{CS.Fine}(\mathcal{S}, \mathcal{C}, d_0, t, r_S)$, in which $\mathcal{C}$ gets the penalty d_0 ₿ by posting the punishment transaction TxFine on the blockchain, and then quits. The detail of TxFine is given in Figure 10.

- *Case 2.* $\mathcal{S}$ refuses to pay the penalty d_0 ₿ to $\mathcal{C}$, that is, $\mathcal{S}$ opens the claim commitment by posting the opening transaction TxOpen on the blockchain before time t. In this case, $\mathcal{C}$ gets both the refund d_1^C ₿ and the compensation d_1^S ₿ by immediately posting the refund transaction TxRefund and the compensation transaction TxCompensation on the blockchain, respectively. Then $\mathcal{C}$ quits. The details of TxRefund and TxCompensation are given in Figure 7.



d_0 ₿
TxFine(**in:** TxClaimCommitment)
in-script: $\mathsf{sig}_S([\mathsf{TxFine}])$, $\mathsf{sig}_C([\mathsf{TxFine}])$, $\perp$
out-script($body$, σ)**:** $\mathsf{ver}_C(body, \sigma)$
val: d_0 ₿
tlock: t
d_0 ₿

Figure 10: The punishment transaction TxFine.

4.3. Security Analysis

In this section, we present the results of security analysis of BCPay in Theorem 1 and Theorem 2. As mentioned before, eavesdropping attacks and malleability attacks are considered and no third-party is involved in BCPay.

Theorem 1. *Based on the collision-resistance of the adopted hash function H and the unforgeability of ECDSA, BCPay satisfies the property of soundness.*

Proof. Suppose both $\mathcal{C}$ and $\mathcal{S}$ are honest and they follow the procedures of BCPay. We show that even outside adversaries make eavesdropping attacks and malleability attacks, $\mathcal{C}$ and $\mathcal{S}$ will always obtain the required service implementation and the corresponding service fee at the end, respectively. As a matter of fact, in the service enforcement procedure of the service implementation phase, $\mathcal{S}$ computes a signature σ_{root} which is stored on the blockchain by broadcasting the service signature transaction $\mathsf{TxServiceSig}$. After a challenge is generated by $\mathcal{C}$ in the challenge generation phase, $\mathcal{S}$ makes a commitment based on $\mathsf{CS.Commit}$. Subsequently, $\mathcal{C}$ and $\mathcal{S}$ perform the all-or-nothing checking-proof protocol $\mathcal{CP}_{\text{AON}}$, in which only the proof initiation phase and the service payment phase are involved if both parties are honest. In the proof initiation phase, after $\mathcal{C}$ initiates the service proof based on σ_{root}, $\mathcal{C}$ and $\mathcal{S}$ make a joint deposit transaction $\mathsf{TxProofInit}$, which is finally posted on the blockchain by $\mathcal{S}$. In the service payment phase, $\mathcal{S}$ provides a service implementation proof $\mathsf{ServiceProof}$ to earn the service fee from $\mathcal{C}$ and get his/her current guaranty back by redeeming $\mathsf{TxProofInit}$ based on $\mathsf{TxServiceFee}$ and $\mathsf{TxGuaranty}$, respectively. According to the definitions of check and $\mathsf{ServiceProof}$ in Section 4.2, if a $\mathsf{ServiceProof}$, which is deduced by outside adversaries based on eavesdropping attacks and malleability attacks, can pass check, then either a hash collision is found or ECDSA is forgeable. In other words, if the adopted hash function is collision-resistant and ECDSA is unforgeable, it is ensured that check has the value true only if $\mathsf{ServiceProof}$ meets the service requirements specified in the proof initiation phase. Therefore, if $\mathcal{C}$ and $\mathcal{S}$ are honest and follow the procedures of BCPay, they will always obtain the required service implementation and the corresponding service fee, respectively. □

Theorem 2. *BCPay satisfies the property of robust fairness without needing a third-party if the adopted hash function H is collision-resistant and ECDSA is unforgeable.*

Proof. As mentioned in Section 3.3, no private channels are required in BCPay. So, eavesdropping attacks and malleability attacks may be made by a malicious party to undermine the fairness for the honest party. In the following, we first prove the robust fairness for $\mathcal{C}$ against malicious $\mathcal{S}$, and then consider the robust fairness for $\mathcal{S}$ in the case of malicious $\mathcal{C}$.

Case 1. Suppose $\mathcal{C}$ is honest and $\mathcal{S}$ is malicious. In this case, $\mathcal{S}$ aims to get the service fee from $\mathcal{C}$ without providing a valid service implementation proof in terms of the requirements specified by $\mathcal{C}$ before time $t - 2\max_B$. At the same time, $\mathcal{S}$ is reluctant to pay compensation and penalty to $\mathcal{C}$. Assume that $\mathcal{C}$ does not get a valid service implementation proof from $\mathcal{S}$ in terms of his/her requirements before time t, which means the service implementation proof $\mathsf{ServiceProof}$ is invalid. Hence, the joint deposit transaction $\mathsf{TxProofInit}$ cannot be redeemed by $\mathcal{S}$ based on $\mathsf{TxServiceFee}$ and $\mathsf{TxGuaranty}$ before time $t - 2\max_B$ in the service payment phase. According to the definitions of check and $\mathsf{ServiceProof}$ in Section 4.2, we know $\mathcal{S}$ cannot get the service fee d_1^C ₿ from $\mathcal{C}$ unless $\mathcal{S}$ is able to forge an ECDSA signature or find a collision of the hash function H. Furthermore, $\mathcal{S}$ may make malleability attacks by eavesdropping transactions on the public channel. However, the attacks are meaningless because the transactions involved in BCPay are posted on the blockchain in order and $\mathcal{C}$ is still able to claim enough compensation or penalty from $\mathcal{S}$. Please refer to Figure 7 and Figure 8 for more details.

Specifically, if $\mathcal{S}$ refuses to pay the compensation d_1^S ₿ to $\mathcal{C}$, which means $\mathcal{S}$ does not open the claim commitment made in the claim commitment phase by broadcasting TxOpen based on $\mathsf{CS.Open}$ before time t, $\mathcal{C}$ performs $\mathsf{CS.Fine}$, in which $\mathcal{C}$ gets the penalty d_0 ₿ with $d_0 \geq d_1^C + d_1^S$ by posting the punishment transaction TxFine on the blockchain. If $\mathcal{S}$ refuses to pay the penalty to $\mathcal{C}$, which means $\mathcal{S}$ opens the claim commitment by performing $\mathsf{CS.Open}$ to post TxOpen on the blockchain before time t, $\mathcal{C}$ can claim both the refund d_1^C ₿ and the compensation d_1^S ₿ by posting $\mathsf{TxRefund}$ and $\mathsf{TxCompensation}$ on the blockchain, respectively. Accordingly, in any case, if malicious $\mathcal{S}$ fails to provide a valid service implementation proof, $\mathcal{C}$ is able to claim enough compensation besides the service fee refund or penalty from $\mathcal{S}$ no matter how $\mathcal{S}$ behaves.

Generally speaking, the robust fairness for $\mathcal{C}$ is ensured in BCPay without needing a third-party if the hash function H is collision-resistant and ECDSA is unforgeable.

Case 2. Suppose $\mathcal{S}$ is honest and $\mathcal{C}$ is malicious. In this case, $\mathcal{C}$ aims to obtain a valid service implementation proof in terms of his/her requirements before time $t - 2\max_B$ without paying the corresponding service fee to $\mathcal{S}$. Assume that $\mathcal{S}$ provides a valid service implementation proof in terms of the requirements of $\mathcal{C}$ before time t. It follows that the service implementation proof $\mathsf{ServiceProof}$ is valid. According to the details of BCPay, $\mathcal{C}$ only puts service fees in the generation of the joint deposit transaction $\mathsf{TxProofInit}$, which can be successfully redeemed by $\mathcal{S}$ in the service payment phase based on $\mathsf{TxServiceFee}$ and $\mathsf{TxGuaranty}$ before time $t - 2\max_B$ only if $\mathsf{ServiceProof}$ is valid. In fact, malicious $\mathcal{C}$ may try to eavesdrop $\mathsf{TxServiceFee}$ and $\mathsf{TxGuaranty}$ on the public channel to get the service proof $\mathsf{ServiceProof}$ together with $\mathsf{sig}_S([\mathsf{TxServiceFee}])$ and $\mathsf{sig}_S([\mathsf{TxGuaranty}])$, respectively. After that, $\mathcal{C}$ mauls the joint deposit transaction $\mathsf{TxProofInit}$ to prevent $\mathcal{S}$ from earning the corresponding service fee. As we know, however, the service payment phase is behind the proof initiation phase in BCPay, hence this malleability attack is meaningless.

On the other hand, malicious $\mathcal{C}$ may try to claim compensation or penalty from $\mathcal{S}$ after ensuring that the service proof is valid in terms of his/her requirements. Obviously, it is infeasible for $\mathcal{C}$ to claim compensation from $\mathcal{S}$ because $\mathsf{TxGuaranty}$ has been posted on the blockchain. In particular, $\mathcal{C}$ cannot redeem $\mathsf{TxProofInit}$ before $\mathcal{S}$ unless he/she finds a collision of H or forges an ECDSA signature. According to the service payment phase of BCPay, $\mathsf{CS.Open}$ is immediately performed by $\mathcal{S}$ to open the claim commitment and hence to get the punishment deposit back before time t. From the property of transaction lock-time, it follows that $\mathcal{C}$ cannot get a penalty from $\mathcal{S}$ even if malleability attacks are made.

Therefore, the robust fairness for $\mathcal{S}$ is ensured in BCPay without needing a third-party if H is collision-resistant and ECDSA is unforgeable. $\square$

5. Performance Evaluation

In this section, we evaluate the performance of our proposed BCPay in terms of the number of involved transactions and computation cost.

5.1. Number of Transactions

As for BCPay, in the *Service Implementation Phase*, only one transaction TxServiceSig is required. In the *Service Checking Phase*, transactions TxClaimCommitment and TxProofInit are involved. In the *Service Payment Phase*, transactions TxOpen, TxServiceFee and TxGuaranty are needed. In the *Service Claim Phase*, either the transaction TxFine or transactions TxRefund and TxCompensation are created. Note that TxServiceFee and TxGuaranty can be replaced with one transaction because they only need signatures of the server. Similarly, TxRefund and TxCompensation can also be combined into one transaction. Accordingly, as shown in Figure 11, the number of involved transactions is small and constant and it is affected neither by the height of the data tree nor by the number of challenge data blocks.

5.2. Computation Cost

In BCPay, the most common operations are hashing and ECDSA signature operations. Considering that the computation cost of a hashing is far less than that of an ECDSA signature, we take ECDSA signature into account in the following. In our experiments, we evaluate the computation time of the ECDSA signature used in transactions on a virtual machine (3.6 GHz single-core processor and 6 GB DDR3-1600 RAM memory) based on Ubuntu 16.04 LTS and OpenSSL 1.0.2g. In particular, a specific elliptic curve called secp256k1 with the equation $y^2 = x^3 + 7$ is adopted, which is used by Bitcoin and can also be used in Ethereum. Additionally, in the following figures, we display the computation time with data trees of height 7, 10, 13, and 16, respectively. In any case, the number of challenge data blocks can reach 100 ($< 2^7$).

BCPay is very efficient because the computation cost is not related to the height of the data tree and the number of challenge data blocks. If the server is honest, the client only participates in creating the transaction TxProofInit in the *Service Checking Phase*, and hence only one ECDSA signature is needed. The computation time of the client is presented in Figure 12(a). On the other hand, if the server is malicious, the client only computes one ECDSA signature in the *Service Claim Phase*. The corresponding

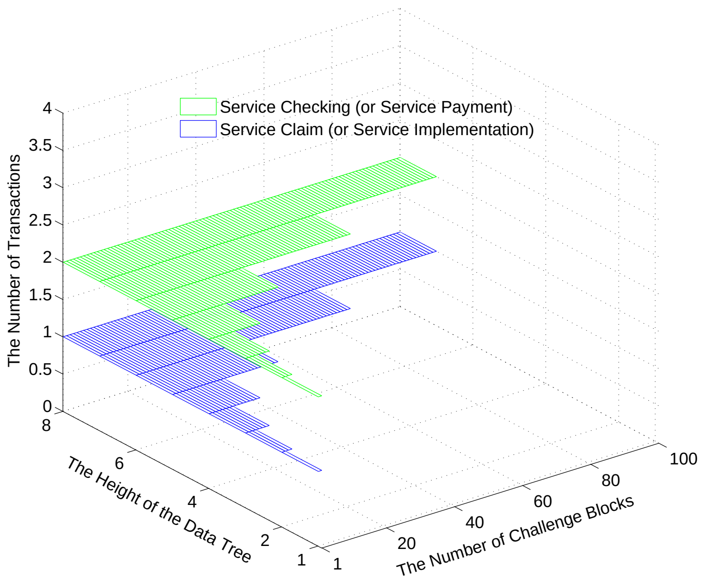


Figure 11: The number of transactions in BCPay.

claim time for the client is presented in Figure 12(b). In BCPay, the server creates TxServiceSig, TxClaimCommitment, TxOpen, TxProofInit, TxServiceFee and TxGuaranty. Note that, even if TxServiceFee and TxGuaranty are combined, the number of ECDSA signatures is not reduced. In addition, the creation of TxFine also needs a signature of the server. Therefore, the server has to perform 7 ECDSA signature operations in BCPay. Computation time of the server is presented in Figure 12(c).

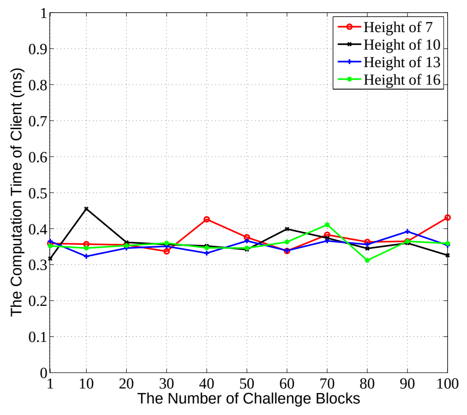
6. Decentralized Applications of BCPay

BCPay is a blockchain-based fair payment framework. In this section, we show how to realize two important decentralized applications based on BCPay.

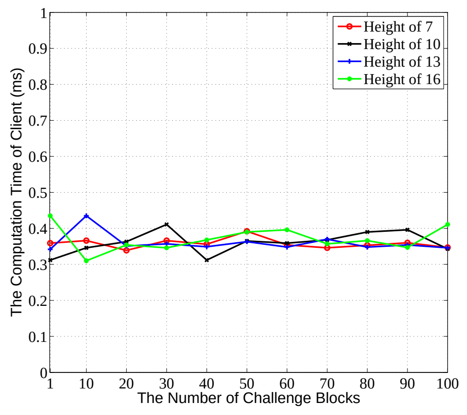
6.1. Blockchain-based PDP

In the case of $\mathsf{sv}=$ PDP, according to the details of BCPay, we only need to display the *Service Implementation Phase*, which is implemented based on the following three procedures.

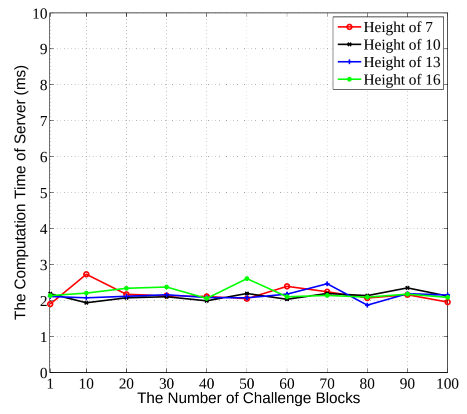
- *Service Subscription:* Let $\mathsf{data}_0 = \{F_1, F_2, \cdots, F_{2^\ell}\}$ be the plaintext data collection. $\mathcal{C}$ encrypts data_0 based on a symmetric encryption algorithm and sends the resulting ciphertext data collection data_1 to $\mathcal{S}$ for subscribing the PDP service. Suppose $\mathsf{data}_1 = \{D_1, D_2, \cdots, D_{2^\ell}\}$ in which D_k is the ciphertext of F_k for $1 \le k \le 2^\ell$.



(a) Computation time of the client with an honest server



(b) Claim time of the client with a malicious server



(c) Computation time of the server

Figure 12: Computation time in BCPay

- *Service Enforcement:* Upon receiving the subscription data data_1 from $\mathcal{C}$, $\mathcal{S}$ constructs a Merkle tree $\mathcal{T}_\ell$. Subsequently, $\mathcal{S}$ computes $\sigma_{\text{root}} = \mathsf{sig}_S(h_r)$, and stores σ_{root} on the blockchain by broadcasting $\mathsf{TxServiceSig}$ as shown in Figure 5. Finally, $\mathcal{S}$ sends the transaction ID to $\mathcal{C}$.

- *Preliminary Service Confirmation:* Upon receiving ID from $\mathcal{S}$, $\mathcal{C}$ first locates $\mathsf{TxServiceSig}$ on the blockchain and gets σ_{root}. Then, $\mathcal{C}$ computes h_r based on data_1. If $\mathsf{vec}_S(h_r, \sigma_{\text{root}})$ evaluates to true, $\mathcal{C}$ stores the height ℓ of the Merke tree. Based on his/her practical outsourcing strategies, such as redundant outsourcing, $\mathcal{C}$ immediately deletes data_1 or stores data_1 until a successful service checking proof.

Note that a challenge-response mechanism is needed in the traditional PDP. In blockchain-based PDP, $\mathcal{C}$ can challenge $\mathcal{S}$ based on the *Service Checking Phase* of BCPay for data integrity. $\mathcal{S}$ can response to $\mathcal{C}$ based on the *Service Payment Phase.* To further support data dynamics, the user only needs to store the structure of the Merkle tree as metadata in *Preliminary Service Confirmation.*

6.2. BCOC: Blockchain-based Outsourcing Computation

In this section, we show the application of BCPay in outsourcing computation, and propose a blockchain-based outsourcing computation scheme, denoted as BCOC. BCOC can be used in fog computing, where a fog user with limited resources wants to outsource distributed computation tasks to the fog node. For consistency, we use $\mathcal{C}$ and $\mathcal{S}$ to represent the fog user and the fog node, respectively. Based on the definition in [26], a distributed computation involves a function, a screener and a payment scheme. However, a trusted third-party is introduced in [26]. In BCOC, we realize both the screener and the payment based on blockchain and no third-party is required. Formally, let f be a one-way function from X to Y, denoted as $f : X \mapsto Y$. Suppose $y^* = f(x)$ for $x \in X$. Note that multiple such x may exist. Given f and y^* only, the objective of the computation is to discover all such x by exhaustive search of the domain X. According to the design details of BCPay, we show the outsourcing of inverting a hash function. Based on the original procedures of BCPay, $\mathcal{C}$ and $\mathcal{S}$ further perform the following.

- *System Setup Phase:* $\mathcal{C}$ specifies a task $\mathsf{task} = (f, X, y^*)$, where $X = \{x_1, x_2, \cdots, x_N\}$.

- *Service Implementation Phase:*

  - *Service Subscription:* $\mathcal{C}$ sends task to $\mathcal{S}$.
  - *Service Enforcement:* For $1 \le i \le N$, $\mathcal{S}$ computes $y_i = f(x_i)$. Without loss of generality, suppose

    $$\{x \in X | f(x) = y^*\} = \{x_1, x_2, \cdots, x_{2^\ell}\} \triangleq X^*,$$

    where $\ell \le \log N$. $\mathcal{S}$ constructs a Merkle tree based on X^* as before and sends ℓ to $\mathcal{C}$.

– *Preliminary Service Confirmation:* $\mathcal{C}$ stores ℓ.

- *Service Checking Phase:*
  - *Challenge Generation Phase:* As before.
  - *Claim Commitment Phase:* As before.
  - *Proof Initiation Phase:* $\mathcal{C}$ and $\mathcal{S}$ jointly create $\mathsf{TxProofInit}$ based on check and y^* by putting $H(x'_k) = y^*$ for $k \in \mathsf{chaldata}$ in the output script, where the value of x'_k is from x_k provided by $\mathcal{S}$ in the *Service Payment Phase*. That is, the service proof provided by $\mathcal{S}$ in the *Service Payment Phase* should satisfy the basic correctness requirement besides check.
- *Service Payment Phase:* $\mathcal{S}$ provides $\{x_k\}_{k\in\mathsf{chaldata}}$ besides $\mathsf{ServiceProof}$.
- *Service Claim Phase:* As before.

7. Conclusion

In this paper, we introduced BCPay, a blockchain based fair payment framework for outsourcing services in cloud computing. Specifically, we presented the system architecture, specifications and adversary model, and described the design details of BCPay. Our security analysis indicated that BCPay enjoys *Soundness* and *Robust Fairness*. Our performance analysis showed that BCPay is very efficient in terms of the number of involved transactions and computation cost. To illustrate the applications of BCPay, we presented a blockchain-based PDP scheme and a blockchain-based outsourcing computation protocol based on BCPay.

Acknowledgment

We are grateful to the editors and reviewers for their invaluable suggestions. This research is supported by the National Key R&D Program of China (2017YFB0802000), the AXA Research Fund, the National Natural Science Foundation of China (Nos. 61772418, 61472472, 61402366), the Natural Science Basic Research Plan in Shaanxi Province of China (No. 2015JQ6236). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications (No. 2016-02).

References

[1] Andrychowicz, M., Dziembowski, S., Malinowski, D., Mazurek, Ł., 2014. Fair two-party computations via bitcoin deposits. In: International Conference on Financial Cryptography and Data Security (FC). Springer, pp. 105–121.

[2] Andrychowicz, M., Dziembowski, S., Malinowski, D., Mazurek, Ł., 2014. Secure multiparty computations on bitcoin. In: IEEE Symposium on Security and Privacy (SP). IEEE, pp. 443–458.

[3] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58.

[4] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D., 2007. Provable data possession at untrusted stores. In: Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS). ACM, pp. 598–609.

[5] Ateniese, G., Di Pietro, R., Mancini, L. V., Tsudik, G., 2008. Scalable and efficient provable data possession. In: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks (SecureComm). ACM, pp. 1–10.

[6] Ateniese, G., Goodrich, M. T., Lekakis, V., Papamanthou, C., Paraskevas, E., Tamassia, R., 2017. Accountable storage. In: International Conference on Applied Cryptography and Network Security (ACNS). Springer, pp. 623–644.

[7] Ateniese, G., Kamara, S., Katz, J., 2009. Proofs of storage from homomorphic identification protocols. In: International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer, pp. 319–333.

[8] Bentov, I., Kumaresan, R., 2014. How to use bitcoin to design fair protocols. In: International Cryptology Conference (CRYPTO). Springer, pp. 421–439.

[9] Bonomi, F., Milito, R., Zhu, J., Addepalli, S., 2012. Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, pp. 13–16.

[10] Buterin, V., 2014. A next-generation smart contract and decentralized application platform. White paper, 1–36.

[11] Campanelli, M., Gennaro, R., Goldfeder, S., Nizzardo, L., 2017. Zero-knowledge contingent payments revisited: Attacks and payments for services. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, pp. 229–243.

[12] Carbunar, B., Tripunitara, M. V., 2012. Payments for outsourced computations. IEEE Transactions on Parallel and Distributed Systems 23 (2), 313–320.

[13] Chen, X., Li, J., Huang, X., Ma, J., Lou, W., 2015. New publicly verifiable databases with efficient updates. IEEE Transactions on Dependable and Secure Computing 12 (5), 546–556.

[14] Chen, X., Li, J., Ma, J., Lou, W., Wong, D. S., 2014. New and efficient conditional e-payment systems with transferability. Future Generation Computer Systems 37, 252–258.

[15] Chen, X., Li, J., Ma, J., Tang, Q., Lou, W., 2014. New algorithms for secure outsourcing of modular exponentiations. IEEE Transactions on Parallel and Distributed Systems 25 (9), 2386–2396.

[16] Chen, X., Li, J., Susilo, W., 2012. Efficient fair conditional payments for outsourcing computations. IEEE Transactions on Information Forensics and Security 7 (6), 1687–1694.

[17] Chen, X., Li, J., Weng, J., Ma, J., Lou, W., 2016. Verifiable computation over large database with incremental updates. IEEE transactions on Computers 65 (10), 3184–3195.

[18] Chen, X., Zhang, F., Susilo, W., Tian, H., Li, J., Kim, K., 2014. Identity-based chameleon hashing and signatures without key exposure. Information Sciences 265, 198–210.

[19] Community, E., 2016. Ethereum homestead documentation. Online document. URL `http://ethdocs.org/en/latest/index.html`

[20] Developers, G., 2017. Google cloud platform. Online document. URL `https://cloud.google.com/free/docs/frequently-asked-questions`

[21] Dong, C., Wang, Y., Aldweesh, A., McCorry, P., van Moorsel, A., 2017. Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, pp. 211–227.

[22] Du, W., Jia, J., Mangal, M., Murugesan, M., 2004. Uncheatable grid computing. In: Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS). IEEE Computer Society, pp. 4–11.

[23] Feige, U., Shamir, A., 1990. Witness indistinguishable and witness hiding protocols. In: Proceedings of the twenty-second annual ACM symposium on Theory of computing. ACM, pp. 416–426.

[24] Gao, C., Cheng, Q., He, P., Susilo, W., Li, J., 2018. Privacy-preserving naive bayes classifiers secure against the substitution-then-comparison attack. Information Sciences 444, 72–88.

[25] Gennaro, R., Gentry, C., Parno, B., 2010. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: Annual Cryptology Conference (CRYPTO). Springer, pp. 465–482.

[26] Golle, P., Mironov, I., 2001. Uncheatable distributed computations. In: Cryptographers' Track at the RSA Conference (CT-RSA). Springer, pp. 425–440.

[27] Hardson, K., 2017. Monitoring at dropbox. Online document. URL `https://www.usenix.org/conference/srecon17asia/program/presentation/hardson-hurley`

[28] Huang, H., Chen, X., Wu, Q., Huang, X., Shen, J., 2018. Bitcoin-based fair payments for outsourcing computations of fog devices. Future Generation Computer Systems 78, 850–858.

[29] Huang, Z., Liu, S., Mao, X., Chen, K., Li, J., 2017. Insight of the protection for data security under selective opening attacks. Information Sciences 412, 223–241.

[30] Juels, A., Kaliski Jr, B. S., 2007. Pors: Proofs of retrievability for large files. In: Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS). ACM, pp. 584–597.

[31] Khalil, R., Gervais, A., 2017. Revive: Rebalancing off-blockchain payment networks. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, pp. 439–453.

[32] Li, B., Huang, Y., Liu, Z., Li, J., Tian, Z., Yiu, S.-M., 2018. Hybridoram: practical oblivious cloud storage with constant bandwidth. Information Sciences. Online publication. URL `doi.org/10.1016/j.ins.2018.02.019`

[33] Li, J., Huang, X., Li, J., Chen, X., Xiang, Y., 2014. Securely outsourcing attribute-based encryption with checkability. IEEE Transactions on Parallel and Distributed Systems 25 (8), 2201–2210.

[34] Li, J., Zhang, Y., Chen, X., Xiang, Y., 2018. Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security 72, 1–12.

[35] Li, T., Li, J., Liu, Z., Li, P., Jia, C., 2018. Differentially private naive bayes learning over multiple data sources. Information Sciences 444, 89–104.

[36] Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M., Ravi, S., 2017. Concurrency and privacy with payment-channel networks. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, pp. 455–471.

[37] Meng, W., Tischhauser, E., Wang, Q., Wang, Y., Han, J., 2018. When intrusion detection meets blockchain technology: a review. IEEE Access 6, 10179–10188.

[38] Merriam, P., 2015. Ethereum alarm clock. Online document. URL `http://docs.ethereum-alarm-clock.com/en/latest/`

[39] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system, 1–9. Online document. URL `http://bitcoin.org/bitcoin.pdf`

[40] Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J., Tang, Y., 2018. An id-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access 6, 20632–20640.

[41] Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y., 2018. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications 106, 117–123.

[42] Song, W., Wang, B., Wang, Q., Shi, C., Lou, W., Peng, Z., 2017. Publicly verifiable computation of polynomials over outsourced data with multiple sources. IEEE Transactions on Information Forensics and Security 12 (10), 2334 – 2347.

[43] Wang, Q., Wang, C., Ren, K., Lou, W., Li, J., 2011. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE transactions on parallel and distributed systems 22 (5), 847–859.

[44] Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151, 1–32. Online document. URL `http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf`

[45] Xu, J., Wei, L., Zhang, Y., Wang, A., Zhou, F., Gao, C.-z., 2018. Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. Journal of Network and Computer Applications 107, 113–124.

[46] Yan, H., Li, J., Han, J., Zhang, Y., 2017. A novel efficient remote data possession checking protocol in cloud storage. IEEE Transactions on Information Forensics and Security 12 (1), 78–88.

[47] Zhang, X., Tan, Y.-A., Liang, C., Li, Y., Li, J., 2018. A covert channel over volte via adjusting silence periods. IEEE Access 6 (1), 9292–9302.

[48] Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., You, I., 2017. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences 379, 42–61.

[49] Zhang, Y., Li, J., Chen, X., Li, H., 2016. Anonymous attribute-based proxy re-encryption for access control in cloud computing. Security and Communication Networks 9(14), 2397–2411.

[50] Zhang, Y., Zheng, D., Chen, X., Li, J., Li, H., 2016. Efficient attribute-based data sharing in mobile clouds. Pervasive and Mobile Computing 28, 135–149.

[51] Zhang, Y., Zheng, D., Deng, R. H., 2018. Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal. Online publication. URL `https://ieeexplore.ieee.org/document/8334589/`