Zef: Low-latency, Scalable, Private Payments

Mathieu Baudet*
mathieu.baudet@linera.io
Liner

Mahimna Kelkar*
mahimna@cs.cornell.edu
Cornell University

Alberto Sonnino*
alberto@mystenlabs.com
University College London and Mysten Labs

George Danezis*
george@mystenlabs.com
University College London and Mysten Labs

ABSTRACT
Zef is the first Byzantine-Fault Tolerant (BFT) protocol to support payments in anonymous digital coins at arbitrary scale. Zef achieves its performance by forgoing the expense of BFT consensus and using instead Byzantine Consistent Broadcast as its core primitive. Zef is asynchronous, low-latency, linearly-scalable, and powered by partially-trusted sharded authorities. Zef introduces opaque coins represented as off-chain certificates that are bound to user accounts. In order to hide the values of coins when a payment operation consumes or creates them, Zef uses cryptographically hiding commitments and NIZK proofs. Coins creation and spending are unlinkable through the Coconut [28] blind and randomizable threshold anonymous credentials scheme. To control storage costs associated with coin replay prevention, Zef allows safe accounts deletion once the account is deactivated. Our extensive benchmarks on AWS confirm textbook linear scalability and demonstrate a confirmation time under one second at nominal capacity. Compared to existing anonymous payment systems based on a blockchain [22, 34], this represents a latency speedup of three orders of magnitude, with no theoretical limit on throughput.

KEYWORDS
privacy-preserving payments, bft, consensus-less

1 INTRODUCTION
Anonymous payment systems have been an exciting research area in cryptography since Chaum’s seminal work [12] on e-cash. Early e-cash schemes [11, 12, 27] however required a centralized issuer to operate, usually in the form of a trusted commercial bank, which hampered their adoption. In recent years, the advent of networks like Bitcoin has sparked renewed interest in privacy-preserving decentralized payment systems. Several anonymous payment systems [7, 21, 22] are now deployed as permissionless blockchains.

Compared to traditional global payment infrastructures (aka. RTGS systems [6]), however, decentralized anonymous payment systems have not yet reached performance levels able to sustain large-scale adoption. For instance, due to high computational costs, only 2% of Zcash [34] transactions typically take full advantage of the privacy features offered by the platform [1]. Recently proposed Byzantine fault-tolerant (BFT) consensus-less protocols such as FastPay [5] forgo consensus and use weaker broadcast-based primitives to offer low-latency transfers of assets. This makes them suitable for deployment as a high-performance sidechain of an existing blockchain, but do not provide any privacy guarantee.

Zef achieves the best of both worlds: the privacy of anonymous payment systems like Zcash and the performance of consensus-less systems like FastPay. Furthermore, Zef authorities can be sharded to accommodate arbitrary throughput and innovates in its storage design solving one of the major costs of current anonymous payment systems. Zef is thus the first linearly-scalable BFT protocol for anonymous payments with sub-second confirmation time.

Zef implements digital coins that are opaque and unlinkable (in short anonymous) by combining: (i) randomized commitments and Non-Interactive Zero-Knowledge (NIZK) proofs (e.g., [21]) to provide opacity, that is, to hide payment values, together with (ii) blind and randomizable signatures (e.g., [28]) to provide unlinkability, meaning that the relation between senders and receivers is hidden. The natural approach to preventing double spending in anonymous systems requires authorities to keep track of all the coins that have been spent. Eventually, maintaining such an ever-growing spent list is bound to create performance and storage bottlenecks. Both Monero and Zcash nevertheless follow this approach, suggesting theoretical limitations in throughput and/or system lifetime. In contrast, in a non-anonymous payment system such as Bitcoin, it is sufficient to keep track of the currently unspent coins—known as Unspent Transaction Outputs (UTXOs). A key contribution of Zef is to remove the need for authorities to maintain a list of spent coins. Zef proposes a new concept of accounts supporting both (i) account-oriented operations, such as transferring ownership, receiving funds repeatedly, and creating unique identifiers, and (ii) UTXO-like operations, such as spending and deactivating accounts. Deactivated accounts may be safely cleaned up from the local storage of each authority. Importantly, all the features introduced by Zef still rely exclusively on client-driven broadcast (reliable or not) and do not require a consensus protocol.
Contributions. (1) We propose Zef—a consensus-less system for scalable account operations. Accounts are addressed by unique, non-replayable identifiers (UIDs) and support a variety of operations such as account creation, deactivation, transparent payments, and ownership transfer. Importantly, all account operations in Zef, including generation of system-wide unique identifiers, are linearly scalable, consensus-free, and require only elementary cryptography (hashing and signing). (2) We describe and analyze the first asynchronous BFT protocol for opaque, unlinkable payments with linear (aka “horizontal”) scalability and sub-second latency. (3) We open-source a prototype implementation of Zef in Rust and evaluate both the scalability and the latency of anonymous payments.

2 BACKGROUND AND RELATED WORK

FastPay. FastPay [5] was recently proposed as a sidechain protocol for low-latency, high-throughput payments in the permissioned model with asynchronous communication.

- Sidechain protocol: FastPay is primarily meant as a scalability solution on top of an existing blockchain with smart contracts (e.g., Ethereum [31]).
- Permissioned model (Byzantine-Fault Tolerance): $N = 3f + 1$ replicas called authorities are designated to operate the system and process the clients’ requests. A fixed set of at most $f$ authorities may be malicious (i.e. deviate from the protocol).
- Low latency: Authorities do not interact with each other (e.g. running a mempool or a consensus protocol). Client operations succeed predictably after a limited number of client/authorities round trips. Notably, in FastPay, a single round-trip with authorities suffices to both initiate a payment and obtain a certificate proving that the transfer is final.
- Scalable: Each authority operates an arbitrary number of logical shards, across many physical hosts. By design, each client request is processed by a single shard within each authority. Within an authority, communication between shards is minimal and never blocks a client request.
- Asynchronous communication: Malicious nodes may collude with the network to prioritize or delay certain messages. Progress is guaranteed when messages eventually arrive.

In a nutshell, the state of the Fastpay accounts is replicated on a set of authorities. Each account contains a public key that can authorize payments out, a sequence number and a balance. Account owners authorize payments by signing them with their account key and including the recipient amount and payment value. An authorized payment is sent to all authorities, who countersign it if it contains the next sequence number; there are enough funds; and, it is the first for this account and sequence number. A large enough number (to achieve quorum intersection) of signatures constitute a certificate for the payment. Obtaining a certificate ensures the payment can eventually be executed (finality). Anyone may submit the certificate to the authorities that check it and update the sender account and recipient balance.

FastPay does not rely on State-Machine Replication (SMR) in the sense that it does not require authorities to agree on a single global state—as one could expect from a traditional sidechain. Doing so, the protocol avoids performance considerations commonly associated with SMR. Notably, FastPay does not incur the end-to-end latency cost of gathering, disseminating, and executing large blocks of transactions, a de-facto requirement for high throughput with SMR solutions [13, 17, 29, 32].

Despite the benefits listed above, until now, the FastPay protocol has been limited to transparent payments, that is, without any privacy guarantees. In fact, to ensure fund availability in worst-case scenarios, FastPay requires all past money transfers to be publicly available in clear text. This contrasts negatively with traditional retail payments (e.g. credit cards) where individual transactions remain within a private banking network. Another technical limitation of FastPay is that unused accounts cannot be deleted. In a privacy-sensitive setting where users would never re-use the same account twice, this means that storage cost of accounts would grow linearly with the number of past transactions. Appendix C provides a deeper system comparison of FastPay and Zef.

Existing private payment schemes. Compared to payment channels (e.g. [25]), safety in FastPay and Zef does not require any upper bound on network delays and clients to stay connected (aka. a synchrony assumption [15]). Furthermore, the reliability of the lighting network depends on the existence of pairwise channels, with the success of a payment between two random nodes being at most 70%\(^1\). In contrast, coins delegated to a FastPay instance are always immediately transferable to any recipient that possesses a public key (resp. an account identifier in Zef).

Several privacy-preserving payment systems have been proposed in the past, each based on a blockchain consensus and therefore not linearly scalable: Zcash, based on Zerocash [7], uses a zero-knowledge proof of set inclusion which is expensive to compute instead of an efficient threshold issuance credential scheme. As a result most transactions are shielded, leading to a degradation in privacy [18]. Monero [22] uses ring signatures to ensure transactions benefit from a small anonymity set. However, intersections attacks and other transaction tracing heuristics are applicable. This results in an uneven degree of privacy [23].

Furthermore, the safety in those systems requires any upper bound on network delays and clients to stay connected (aka. a synchrony assumption [15]), while Zef operates asynchronously.

3 SYSTEM OVERVIEW

Zef is a consensus-less protocol designed to support high-volume, low-latency payments, both anonymous and transparent, on top of a primary blockchain. Zef introduces a new notion of accounts, indexed by a unique identifier (UID) so that deactivated accounts can have their data safely removed.

Authorities and quorums. We assume a primary blockchain which supports smart contracts (e.g., Ethereum [31]). In a typical deployment, we expect Zef to be “pegged” to the primary chain through a smart contract, thereby allowing transfers of assets in either direction [3]. The Zef smart contract holds the reserve of assets (e.g., coins) and delegates their management to a set of external nodes called authorities. For brevity, in the rest of this paper, we focus on the Zef system and omit the description of transfers between

\(^1\)https://diar.co/volume-2-issue-25/
the primary blockchain and Zef. The mechanics of such transfers is similar to “funding” and “redeeming” operations in FastPay [5].

Zef is meant to be Byzantine-Fault Tolerant (BFT), that is, tolerate a subset of authorities that deviate arbitrarily from the protocol. We assume an asynchronous network that may collude with malicious authorities to deliver messages in arbitrary order. The protocol makes progress when message are eventually delivered.

We assume that authorities have shared knowledge of each other’s signing public keys. Each authority is also assigned a voting power, which indicates how much control the authority has within the system. \( N \) denotes the total voting power, while \( f \) denotes the power held by adversarial authorities. In the simplest setting where each authority has a voting power of 1 unit, \( N \) denotes the total number of authorities and \( f \) denotes the number of adversarial authorities tolerated by the system. In general, unequal voting powers may be used to reflect different stakes locked by the authorities on the main blockchain. Similar to standard protocols, we require \( 0 \leq f < \frac{N}{3} \). The system parameters \( N \) and \( f \), as well as the public key and voting power of each authority are included in the Zef smart contract during setup.

We use quorum to refer to a set of signatures by authorities with a combined voting power of at least \( N - f \). An important property of quorums, called quorum intersection, is that for any two quorums, there exists an honest authority \( \alpha \) that is present in both.

Cryptographic primitives. We assume a collision-resistant hash function hash as well as a secure public-key signature scheme. Informally, a random commitment \( cm = \text{com}_M(\phi) \) is an expression that provides a commitment over the value \( \phi \) (in particular, is collision-resistant) without revealing any information on \( \phi \), as long as the random seed \( r \) is kept secret. A signing scheme supports blinding and unblinding operations iff (i) a signature of a blinded message \( B = \text{blind}(M; u) \) with blinding factor \( u \) can be turned into a valid signature of \( M \) by computing the expression \( \text{unblind}(B; u) \), and (ii) provided that \( u \) is a secret random value, an attacker observing \( B \) learns no information on \( M \).

Blind signatures will be used for anonymous coins in Section 5 together with an abstract notion of Non-Interactive Zero-Knowledge (NIZK) proof of knowledge. We will also further assume that a public key \( pk\text{all} \) is set up between authorities in such a way that any quorum of signatures on \( M \) may be aggregated into a single, secure threshold signature of \( M \), verifiable with \( pk\text{all} \). (See Appendix B for a concrete instantiation.)

Clients, requests, certificates, and coins. Clients to the Zef protocol are assumed to know the public configuration of the system (see above) including networking addresses of authorities. Network interactions are always initiated by a client request. We distinguish account-based requests, i.e., those targeting a specific account, noted \( R \), from free requests \( R^\ast \). In what follows, all requests are account-based unless mentioned otherwise. Free requests will be used for coin creation in Section 5.

As illustrated in Figure 1, clients may initiate a particular operation \( O \) on an account that they own as follows: (i) broadcast a request \( R \) containing the operation \( O \) and authenticated by the client’s signature to the appropriate logical shard of each authority \( \alpha \); and (ii) wait for a quorum of responses, that is, sufficiently many answers so that the combined voting power of responding authorities reaches \( N - f \).

An authority responds to a valid request \( R \) by sending back a signature on \( R \), called a vote, as acknowledgment (1). After receiving votes from a quorum of authorities, a client forms a certificate \( C \), that is, a request \( R \) together with a quorum of signatures on \( R \). In the rest of this paper, we identify certificates on a same value \( V \) and simply write \( C = \text{cert}[V] \) when \( C \) is a certificate on \( V \). Depending on the nature of value \( V \) (e.g., anonymous coins in Section 5) and implementation choices, the quorum of signatures in \( C \) may be aggregated into a single threshold signature \( \sigma \).

We further distinguish regular operations from locking operations. A request \( R \) typically contains a regular operation \( O \) meant to be executed once. The certificate \( C = \text{cert}[R] \) is meant to be broadcast back to authorities as a confirmation (2), thereby triggering the one execution of \( O \) (3) and allowing the account behind \( R \) to process further requests. A confirmation certificate \( C \) also acts as a proof of finality, that is, a verifiable document proving that the transaction (e.g., a payment) can be driven to success. In the case of payments, recipients obtain and verify the certificate themselves before accepting the payment. In contrast, locking operations cannot be confirmed and executed. If a request \( R \) contains a locking operation, a certificate on \( R \) is called a locking certificate and written \( L = \text{cert}[R] \). Such certificate \( L \) serves as a proof that the account is locked and cannot process further account operations.

A third type of certificates associates a coin to an account identifier. Section 5 introduces anonymous coins of the form \( A = \text{cert}[(id, cm)] \) for some commitment \( cm \) on the value \( o \) of the coin. Appendix A also introduces transparent coins \( T = \text{cert}[(id, v, r)] \).

Accounts and unique identifiers. Zef accounts are replicated across all authorities. For a given authority \( \alpha \), we use the notation \( X(\alpha) \) to denote the current view of \( \alpha \) regarding some replicated data \( X \). At a high level, Zef improves upon the notion of a FastPay account and provides the following important features:

- A Zef account is addressed by an unique identifier (or UID for short) designed to be non-replayable. We use \( \text{id}, \text{id}_1, \ldots \) to denote account identifiers.
- Every account includes an optional public key \( pk^{\text{id}}(\alpha) \) to authenticate their owner, if any. When \( pk^{\text{id}}(\alpha) = \perp \), the account is said to be inactive.
Identifiers are created whenever the owner of an account id requests a fresh identifier, for themselves or for a third-party. In practice, we define the next available identifier as the concatenation of the account address id and its current sequence number $\alpha = \text{next_sequence}^{id}(\alpha)$.

Zef makes it possible to safely and verifiably transfer the control of an account to another user by changing the key $pk^{id}(\alpha)$. An account can be deactivated by setting $pk^{id}(\alpha) = \perp$. This operation is final and effectively consumes the assets controlled by the account. Because identifiers id are never reused for new accounts, accounts that are deactivated may be optionally deleted by authorities to reclaim storage (see discussion in Section 4).

In addition to the public balance $\mathcal{B}^{id}(\alpha)$, the owner of an account id may own some anonymous coins $A = \mathcal{C}^{id}(\alpha, cm)$.

Sharding and cross-shard queries. In order to scale the processing of client requests, each Zef authority $\alpha$ may be physically divided in an arbitrary number of shards. Every request $R$ sent to an account id in $\alpha$ is assigned a fixed shard as a public function of id and $\alpha$. If a request requires a modification of another target account id', the shard processing the confirmation of $R$ in $\alpha$ must issue an internal cross-shard query to the shard of id'. Cross-shard queries in Zef are asynchronous messages within each authority. They are assumed to be perfectly reliable in the sense that they are never dropped, duplicated, or tampered with.

Transfer of anonymous coins. In Zef, anonymous coins are both (i) unlinkable and (ii) opaque in the sense that during an anonymous payment: (i) authorities cannot see or tracks users across coins being created; (ii) authorities cannot see or tracks users across coins.

Specifically, as illustrated in Figure 2, the owner of an account id may spend all the anonymous coins $A^{in}_i = \mathcal{C}^{id}(\alpha, cm^{in}_i)$ linked to id altogether and create new anonymous coins $A^{out}_j$ using two communication round-trips as follows:

- Provided the recipient accounts $id^{in}_j$ and desired coin values $v^{out}_j$ (1), compute fresh random commitments $cm^{out}_j$ for $v^{out}_j$ and fresh blinded messages $B_j = \text{blind}(id^{out}_j, cm^{out}_j; v^{out}_j)$.
- Using the knowledge of the seed and coin value behind each random commitment $cm^{in}_j$, construct an NIZK proof $\pi$ that the $B_j$ are well-formed—in particular, that the values $v^{out}_j$ are non-negative and have the expected sum.
- Broadcast a locking request $R$ on the account id, containing the hash of the proof $\pi$ and its public inputs $A^{in}_i$ and $B_j$ (2).
- Aggregate the responses from a quorum of authorities into a locking certificate $L = \text{cert}[R]$.
- Broadcast a suitable request $R^*$ containing the proof $\pi$ together with $L$, the coins $A^{in}_i$, and the blinded messages $B_j$ (3).
- Obtain signature shares from a quorum of authorities for each $B_j$ (4), then unblind and aggregate the signatures shares to form new coins $A^{out}_j = \mathcal{C}^{id}(id^{out}_j, cm^{out}_j)$ (5).
- Communicate each new coin $A^{out}_j$, as well as its commitment seed and value, privately to the owner of id^{out}_j (6).

Section 5 further elaborates on the creation of coins from public balances balance^{id}(\alpha) and supporting multiple source accounts.
for account operations—here used to prove finality of account creation, initialized with an authentication key chosen by the client. In practical deployments, we expect authorities to charge a fee for account creation and brokers to forward this cost to their users plus a small margin. Discussing the appropriate pricing and means of payment is out of scope of this paper.

Finally, a Zef system must be set up with a number of root accounts (i.e., account without a parent). In the rest of the paper, we assume that the initial configuration of a Zef system always includes one root account $id_\alpha$ per authority $\alpha$.

**Transfers of account ownership.** An interesting benefit of using unique identifiers as account addresses is that the authentication key $pk^{id}(\alpha)$ can be changed. Importantly, the change of key can be certified to a new owner of the account. This unlocks a number of applications:

- **Anonymous coins.** Anonymous coins (see Section 5) are defined as certificates of the form $A = \text{cert}\{(id, cm)\}$ for some commitment value $cm$. Spending $A$ to create new coins is an unlinkable operation but it reveals the existence of coins controlled by the account id. Account transfers provide an alternative way to transfer anonymous coins that is linkable (and cannot divide coins) but delays revealing the existence of coins altogether.
- **Lower account-generation latency.** While transferring ownership of an account id requires the same number of messages as creating a new account, we will see in Section 4 that it only involves executing an operation within the shard of id itself (i.e., no cross-shard requests are used). Hence, brokers who wish to provide new accounts with the lowest latency may create a pool of accounts in advance then re-assign UIDs to clients as needed.

## 4 ACCOUNT MANAGEMENT PROTOCOL

We now describe the details of the Zef protocol when it comes to account operations. An upshot of our formalism is that it also naturally generalizes the FastPay transfer protocol [5]. Notably, in Zef, the one-time effect of a transaction consists in one of several possible operations, instead of transparent payments only. Additionally, in order to support deletion of accounts, Zef must handle the fact that a recipient account might be deleted concurrently with a transfer.

### 4.1 Protocol Messages and Operations

**Unique identifiers.** A unique identifier (UID) is a non-empty sequence of numbers written as $id = [n_1, \ldots, n_k]$ for some $1 \leq k \leq k_{\text{max}}$. We use $:\$ to denote the concatenation of one number at the end of a sequence: $[n_1, \ldots, n_{k+1}] = [n_1, \ldots, n_k] : n_{k+1}$ ($k < k_{\text{MAX}}$). In this example, we say that $id = [n_1, \ldots, n_k]$ is the parent of $id : n_{k+1}$. We assume that every authority $\alpha$ possesses at least one root identifier of length one: $id_\alpha = [n_\alpha]$ such that the corresponding account is controlled by $\alpha$ at the initialization of the system (i.e., for every honest $\alpha'$, $pk^{id}(\alpha') = \alpha$).

**Protocol messages.** A message $(\text{Tag}, \text{arg}_1, \ldots, \text{arg}_n)$ is a sequence of values starting with a distinct marker $\text{Tag}$ and meant to be sent over the network. In the remainder of the paper, we use capitalized names to distinguish message markers from mathematical functions (e.g. hash) or data fields (e.g. $pk^{id}(\alpha)$), and simply write $\text{Tag}(\text{arg}_1, \ldots, \text{arg}_n)$ for a message.

**Account operations.** A regular operation is a message $O$ meant to be executed once on a main account id, with possible effects on an optional recipient account id’. The regular operations supported by Zef include the following messages:

- $\text{OpenAccount}(id', pk')$ to activate a new account with a fresh identifier $id'$ and authentication key $pk'$—possibly on behalf of another user who owns $pk$;
- $\text{Transfer}(id', \text{value})$ to transfer value coins in a transparent way to an existing account id;
- $\text{ChangeKey}(pk')$ to transfer the ownership of an account;
- $\text{CloseAccount}$ to remove the account id.

In Section 5, we introduce additional regular operations as well as a non-regular (i.e., locking) operation Spend that is not meant to be executed but instead locks an account until it is eventually deactivated. We introduce the operation $\text{CloseAccount}$ now to mimic locking operations introduced later on.

**Account states.** The state of every authority $\alpha$ includes a map accounts$(\alpha)$ that contains the states of the accounts present in $\alpha$, indexed by their UID. The state of such an account id includes the following data:

- An optional public key $pk^{id}(\alpha)$ registered to control id, as seen before.
- A transparent (i.e., public) amount of coins, noted balance$(\alpha)$ (initially equal to balance$(\alpha)$, where balance$(\alpha)$ is 0 except for some special accounts created at the beginning).
- An integer value, written next_sequence$(\alpha)$, tracking the expected sequence number for the next operation on id. (This value starts at 0.)
- pending$(\alpha)$, an optional request indicating that an operation on id is pending confirmation (the initial value being $\bot$).
- A list of certificates, written confirmed$(\alpha)$, tracking all the certificates $C_n$ that have been confirmed by $\alpha$ for requests issued from the account id. One such certificate is available for each sequence number $n$ ($0 \leq n < \text{next_sequence}^{id}(\alpha)$).
- A second list of certificates, written received$(\alpha)$, tracking all the certificates that have been confirmed by $\alpha$ and involving id as a recipient account.

### 4.2 Protocol Description

**Operation safety and execution.** Importantly, account operations may require some validation before being accepted. We say that an operation $O$ is safe for the account id in $\alpha$ if one of the following conditions holds:

- $O = \text{OpenAccount}(id', pk')$ and $id' = \text{next_sequence}^{id}(\alpha)$;
- $O = \text{Transfer}(id', \text{value})$ and $0 \leq \text{value} \leq \text{balance}^{id}(\alpha)$;
- $O = \text{ChangeKey}(pk')$ or $O = \text{CloseAccount}$ (no additional verification).
Algorithm 1 Account operations (internal functions)

1: function InitAccount(id, pk)
2: \text{pk}^{id} \leftarrow pk
3: next_sequence^{id} \leftarrow 0
4: balance^{id} \leftarrow balance^{id}(\text{init}) \triangleright Set to 0 except for special accounts
5: confirmed^{id} \leftarrow [ ]
6: received^{id} \leftarrow [ ]

7: function ValidateOperation(id, n, O)
8: switch O do
9: case OpenAccount(id', pk'):
10: \quad ensure id' = id \triangleright next_sequence^{id}
11: \quad \text{pk}^{id'} \leftarrow Received(id', pk') \triangleright Create new account
12: case Transfer(id', value):
13: \quad ensure 0 < value \leq balance^{id}
14: case ChangeKey(pk') | CloseAccount:
15: \quad balance^{id} \leftarrow balance^{id} - value \triangleright Update sender's balance
16: case Spend(value, h):
17: \quad Lock(id, n, O) \triangleright O is valid and locking
18: \quad \text{ReceiveAndTransfer(id', value, a_1, \ldots, a_r, v_1, \ldots, v_r, r_1, \ldots, r_l):}
19: \quad ensure 0 \leq value \leq balance^{id}
20: \quad for i = 1, \ldots, l do
21: \quad \quad let cm_i = \text{com}_i(v)
22: \quad \quad ensure cm_i \neq \text{com}_i(k, c)
23: \quad \quad ensure cm_i is a valid coin signature for (id, cm_i)
24: \quad return Execute(id, n, O) \triangleright If we reach O, is valid and regular.

24: function ExecuteOperation(id, n, C)
25: switch O do
26: case OpenAccount(id', pk'):
27: \quad do asynchronously \triangleright Cross-shard request to id'
28: \quad \text{receive}^{id'} \leftarrow \text{receive}^{id'} \triangleright Update receiver's log
29: case Transfer(id', value):
30: \quad balance^{id} \leftarrow balance^{id} - value \triangleright Update receiver's balance
31: \quad do asynchronously \triangleright Cross-shard request to id'
32: \quad if id' \neq \text{accounts} then
33: \quad \quad \text{run Init}(id', pk') \triangleright Create new account
34: \quad \quad \text{receive}^{id'} \leftarrow \text{receive}^{id'} \triangleright Receiver's balance
35: \quad \quad \text{balance}^{id'} \leftarrow balance^{id'} - value \triangleright \text{Receive}^{'s} \text{balance}
36: \quad \quad \text{case ChangeKey(pk'):
37: \quad \quad \quad \text{pk}^{id'} \leftarrow pk' \triangleright Update authentication key
38: \quad \quad \text{case CloseAccount:}
39: \quad \quad \quad \text{pk}^{id'} \leftarrow \bot \triangleright Make account inactive
40: \quad \quad \text{case SpendAndTransfer(id', value, a_1, \ldots, a_r, v_1, \ldots, v_r, r_1, \ldots, r_l):
41: \quad \quad \quad \text{pk}^{id'} \leftarrow \bot \triangleright Deactivate sender's account
42: \quad \quad \quad \text{do asynchronously \triangleright Cross-shard request to id'}
43: \quad \quad \quad if id' \neq \text{accounts} then
44: \quad \quad \quad \quad \text{run Init}(id', \bot) \triangleright Make account inactive
45: \quad \quad \quad \text{balance}^{id'} \leftarrow balance^{id'} + \sum_i v_i
46: \quad \quad \quad \text{receive}^{id'} \leftarrow \text{receive}^{id'} \triangleright \text{Receive}^{'s} \text{balance}

When a regular operation O for an account id is confirmed (i.e. a suitable certificate C is received), we expect every authority \(\alpha\) to execute the operation O in the following way:

- if \(O = \text{OpenAccount}(id', pk')\), then the authority \(\alpha\) uses a cross-shard request to set \(\text{pk}^{id'}(\alpha) = pk'\); if necessary, a new account id' is created first;
- if \(O = \text{Transfer}(id', value)\), the authority subtracts value from \(\text{balance}^{id}(\alpha)\) and uses a cross-shard request to add value to \(\text{balance}^{id}(\alpha)\); if necessary, the account id' is created first using an empty public key \(\text{pk}^{id'}(\alpha) = \bot\);
- if \(O = \text{CloseAccount}\), then the authority sets \(\text{pk}^{id'}(\alpha) = \bot\);
- if \(O = \text{CloseAccount}\), then the authority remove the account id.

These definitions translate to the pseudo-code in Algorithm 1. The pseudo-code also includes the logging of certificates with \(\text{confirmed}^{id}(\alpha)\) and \(\text{received}^{id}(\alpha)\) as well as additional operations Spend and SpendAndTransfer that will be described in Section 5.

Account management protocol. We can now describe the protocol steps for executing a regular operation O on an account id:

1. A client knowing the signing key of id and the next sequence number n signs a request \(R = \text{Execute}(id, n, O)\) and broadcasts it to every authority in parallel, waiting for a quorum of responses.
2. Upon receiving an authenticated request \(R = \text{Execute}(id, n, O)\) an authority \(\alpha\) must verify that \(R\) is authenticated for the current account key \(\text{pk}^{id}(\alpha)\), that \(\text{next_sequence}^{id}(\alpha) = n\), that the operation \(O\) is safe (see above), and that \(\text{pending}^{id}(\alpha) = \bot\). Then, it sets \(\text{pending}^{id}(\alpha) = R\) and returns a signature on \(R\) to the client.
3. The client aggregates signatures into a confirmation certificate \(C = \text{cert}[R]\).
4. The client (or another stakeholder) broadcasts \(\text{Confirm}(C)\).
5. Upon receiving \(\text{Confirm}(C)\) for a valid certificate \(C\) of value \(R = \text{Execute}(id, n, O)\) when \(O\) is a regular operation, each authority \(\alpha\) verifies that \(\text{pk}^{id}(\alpha) \neq \bot, \text{next_sequence}^{id}(\alpha) = n\), then increments \(\text{next_sequence}^{id}(\alpha)\), sets \(\text{pending}^{id}(\alpha) = \bot\), adds C to \(\text{confirmed}^{id}(\alpha)\), and finally executes the operation \(O\) once (see above).

The corresponding pseudo-code for the service provided by each authority \(\alpha\) is summarized in Algorithm 2. Importantly, inactive accounts, i.e., those accounts id satisfying \(\text{pk}^{id}(\alpha) = \bot\), cannot accept any request (step (2)) or execute any confirmed operation (step (5)). The protocol to submit locking operations (such as Spend

Algorithm 2 Account service (message handlers)

1: function HandleRequest(auth[R])
2: \quad let Execute(id, n, O) | Lock(id, n, O) = R \triangleright Allow regular and locking operations
3: \quad ensure \text{pk}^{id} \neq \bot \triangleright The account must be active
4: \quad verify that auth[R] is valid for \text{pk}^{id} \triangleright Check authentication
5: \quad if \text{pending}^{id} \neq R then
6: \quad \quad ensure \text{pending}^{id} = \bot
7: \quad \quad ensure \text{next_sequence}^{id} = n
8: \quad \quad ensure \text{ValidateOperation}(id, n, O) = R
9: \quad \quad \text{pending}^{id} \leftarrow R \triangleright Lock the account on R
10: \quad return Vote(R) \triangleright Success: return a signature of the request

11: function HandleConfirmation(C)
12: \quad verify that \(C = \text{cert}[R]\) is valid
13: \quad match Execute(id, n, O) = R \triangleright Allow regular operations only
14: \quad ensure \text{pk}^{id} \neq \bot \triangleright Make sure the account is active
15: \quad if \text{next_sequence}^{id} = n then
16: \quad \quad \text{run ExecuteOperation}(id, n, C)
17: \quad \quad \text{next_sequence}^{id} \leftarrow n + 1 \triangleright Update sequence number
18: \quad \quad \text{pending}^{id} \leftarrow \bot \triangleright Make the account available again
19: \quad \quad \text{confirmed}^{id} \leftarrow \text{confirmed}^{id} \triangleright C \triangleright Log certificate
in Section 5) is similar except that there is no final execution step (5), and by convention, the request is written \( R = \text{Lock}(id, n, O) \) and its certificate \( L = \text{cert}(R) \). Note that step (1) above implicitly assumes that all authorities are up-to-date with all past certificates.

In practice, a client may need to provide each authority with missing confirmation certificates for past sequence numbers. (See also “Liveness considerations” below.)

### 4.3 Security Properties

**Agreement on account operations.** When it comes to the operations executed from one account id, the Zef protocol guarantees that authorities execute the same sequence of operations in the same order. Indeed, the quorum intersection property entails that two certificates \( C \) and \( C' \) must contain a vote by a same honest authority \( \alpha \). If they concern the same account id and sequence number \( n \), the verification by \( \alpha \) in step (2) above and the increment of \( \text{next\_sequence}^id(\alpha) \) in step (5) implies that \( C \) and \( C' \) certifies the same (safe) request \( R \).

It is easy to see by induction on the length of id = \( [n_1, \ldots, n_k] \) that each authority can only execute certified operations for a given id by following the natural sequence of sequence numbers (i.e., \( \text{next\_sequence}^id(\alpha) = 0, 1, \ldots \)). Indeed, by the induction hypothesis (resp. by construction for the base case), at most one operation of the form \( \Omega = \text{OpenAccount}(id, \ldots) \) can ever be executed by \( \alpha \) on the parent account of id (resp. as part of the initial setup if id has no parent). We also note that due to the checks in step (5), no operation can be executed from id while the account id is locally absent or if \( \text{pk}^id(\alpha) = \perp \). Account creation executed by the parent account of id is the only way for \( \text{pk}^id(\alpha) \) to be updated from an empty value \( \perp \). Therefore, if an account id is deleted by \( \alpha \) due to an operation \( \text{CloseAccount} \), it is necessarily so after \( \text{OpenAccount}(id, \ldots) \) was already executed once. The account id may be created again by some operation \( \text{Transfer}(id, \text{value}) \) after deletion, but since \( \text{OpenAccount}(id, \ldots) \) is no longer possible, \( \text{pk}^id(\alpha) \) will remain empty, thus no more operations will be executed from id at this point. Therefore, due to the checks in step (5), the operations executed on id while \( \text{pk}^id(\alpha) \neq \perp \) follows the natural sequence of sequence numbers.

**Agreement on account states.** Let \( \alpha \) be authority and id be an account such that pending(\( \alpha \)) = \( \perp \) and \( \alpha \) has not executed an operation \( \text{CloseAccount} \) on id yet. We observe that the state of id seen by \( \alpha \) is a deterministic function of the following elements:

- the sequence of operations previously executed by \( \alpha \) on id, that is, the content of \( \text{confirmed}^id(\alpha) \), and
- the (unordered) set of operations previously executed by \( \alpha \) that caused a cross-shard request to id as recipient, that is, the content of \( \text{received}^id(\alpha) \).

Indeed, operations issued by id are of the form \( \text{ChangeKey}(\text{pk}), \text{Transfer}(\ldots, \text{value}^{\text{out}}) \), and \( \text{OpenAccount}(\ldots) \). Similarly, possible operations received by id are of the form \( \text{OpenAccount}(id, \text{pk}) \) and \( \text{Transfer}(id, \text{value}^{\text{out}}) \). We can determine the different components of the account id as seen by \( \alpha \) as follows:

- \( \text{next\_sequence}^id(\alpha) \) will be the size of \( \text{confirmed}^id(\alpha) \);
- \( \text{pk}^id(\alpha) \) will be the last key set by \( \text{OpenAccount}(id, \text{pk}) \) (or an equivalent initial setup for special accounts) then subsequent \( \text{ChangeKey}(\text{pk}) \) operations, and otherwise \( \text{pk}^id(\alpha) = \perp \);
- \( \text{balance}^id(\alpha) = \sum_j \text{value}^{\text{out}}_j - \sum_j \text{value}^{\text{out}}_j + \text{balance}^id(\text{init}) \), where \( \text{balance}^id(\text{init}) \) denotes a possibly non-zero initial balance for some special accounts. (In the presentation of FastPay [5], additionally terms account for external transfers with the primary blockchain in replacement of \( \text{balance}^id(\text{init}) \).

The agreement property on account operations (see above) entails that whenever two honest authorities have executed the same operations, they must also agree on the current set of active accounts and their corresponding states. In other words, if for all id, \( \text{confirmed}^id(\alpha) = \text{confirmed}^id(\alpha') \), then for all id such that \( \text{pk}^id(\alpha) \neq \perp \) or \( \text{pk}^id(\alpha') \neq \perp \), we have \( \text{next\_sequence}^id(\alpha) = \text{next\_sequence}^id(\alpha') \), \( \text{pk}^id(\alpha) = \text{pk}^id(\alpha') \), and \( \text{balance}^id(\alpha) = \text{balance}^id(\alpha') \).

In particular, similar to the proof of FastPay [5], \( \text{balance}^id(\alpha) \geq 0 \) holds for every id once every certified operations has been executed. Indeed, consider an honest authority which accepted to vote at step (2) for the last transfer \( \text{Transfer}(\ldots, \text{value}^{\text{out}}) \) from id.

**Liveness considerations.** Zef guarantees that conforming clients may always (i) initiate new valid operations on their active accounts and (ii) confirm a valid certificate of interest as a sender or as a recipient. We note that question (i) is merely about ensuring that the sequence number of an active sender account can advance after a certificate is formed at step (3). This reduces to the question (ii) of successfully executing step (5) for any honest authority, given a valid certificate \( C \).

If the client, an honest authority \( \alpha \), or the network was recently faulty, it is possible that (a) the sender account id may not be active yet at \( \alpha \), or (b) the sequence number of id may be lagging behind compared to the expected sequence number in \( C \). In the latter case (b), similarly to Fastpay, the client should replay the previously confirmed certificates \( C_i \) of the same account—defined as \( C_i \in \text{confirmed}^id(\alpha') \) for some honest \( \alpha' \)—in order to bring an authority \( \alpha \) to the latest sequence number and confirm \( C \). In the case (a) where id is not active yet at \( \alpha \), the client must confirm the creation certificate \( C' \) of id issued by the parent account id’ = parent(id). This may recursively require confirming the history of \( C' \). Note however that this history is still sequential (i.e. there is at most one parent per account) and the number of parent creation certificates is limited by \( k_{\text{MAX}} \).

Importantly, a certificate needs only be confirmed once per honest authority on behalf of all clients. Conforming clients who initiate transactions are expected to persist past certificates locally and pro-actively share them with all responsive authorities.

In practice, the procedure to bring authorities up-to-date can be implemented in a way that malicious authorities that would always request the entire history do not slow down the protocol. (See the discussion in FastPay [5], Section 5.)

### 4.4 Accounts Deletion and Delegation

**Deletion of deactivated accounts.** We have seen that once deactivated, an account id plays no role in the protocol and that id will
never be active again. Therefore, it is always safe for an authority $\alpha$ to delete a once-deactivated account.

A simple strategy for an authority $\alpha$ to take advantage of this fact and reclaim some local storage consists in deleting the account id whenever $pk_{id}(\alpha)$ changes its value to $\bot$. We note however that this strategy is only a best effort. Effectively reclaiming the maximum amount of storage available in the system requires addressing two questions:

1. If an honest authority $\alpha$ deletes id, how to guarantee that the account is not recreated later by $\alpha$.
2. If an honest authority $\alpha$ deletes id, how to guarantee that every other honest authority $\alpha' \neq \alpha$ eventually deletes id;

Regarding (1), when a cross-shard request is received for an operation $\text{Transfer}(id, \text{value})$, the current version of the protocol may indeed require re-creating an empty account id. This storage cost can be addressed by modifying Zef so that an authority $\alpha$ does not re-create id (or quickly deletes it again) if it determines that no operation $O = \text{OpenAccount}(id, ...)$ can occur any more. This fact can be tested in background using $|id| \leq \kappa_{\text{max}}$ cross-shard queries. Indeed, consider the opposite fact: an inactive account id $id_0 \vdash n$ can become active in $\alpha$ iff it holds that (i) $\text{next\_sequence} \leq n$ and (ii) the parent account id is either active or can become active.

Regarding (2), we note that sending and receiving clients in payment operations have an incentive to fully disseminate the confirmation certificates to all authorities—rather than just a quorum of them—whenever possible. (The incentives are respectively to fully unlock the sender’s account and to fully increase the receiver’s balance in the eventuality of future unresponsive authorities.) However, such an incentive does not exist in the case of the CloseAccount operation (resp. the message CreateAnonymousCoins of Section 5). Therefore, in practical deployments of Zef, we expect authorities to either communicate with each other a minima in background, or to incentivize clients to continuously disseminate missing certificates (resp. missing free queries $R'$ of Section 5) between authorities.

Safety of delegated account generation. In the eventuality of malicious brokers, a client must always verify the following properties before using a new account id:

- The certificate $C$ returned by the broker is a valid certificate $C = \text{cert}(R)$ such that $R = \text{Execute}(id, n, O)$ and $O = \text{OpenAccount}(id', pk)$ for the expected public key $pk$. (Under BFT assumption, this implies $id' = id \vdash n$.)
- If the client did not pick a fresh key $pk$, it is important to also verify that $C$ is not being replayed.

To avoid revealing which accounts they own, clients should use a fresh authentication key $pk$ every time and consider communicating with brokers privately (e.g. over Tor). How a client may anonymously purchase their first UID from a broker raises the interesting question of how to effectively bootstrap a fully anonymous payment system. (For instance, a certain number of fresh key-less accounts could be given away regularly for anyone to acquire and reconfigure them over Tor before receiving their very first anonymous payment.) Yet, we should point out that revealing the owner of an account does not contradict the confidentiality and the unlinkability properties of the anonymous coins described in Section 5.

5 ANONYMOUS PAYMENTS

We now describe the Zef protocol for anonymous payments using generic building blocks. In particular, we use a blind signature scheme, random commitments, and Zero-Knowledge (ZK) proofs in a black-box way. A more integrated realization of the protocol suitable for an efficient implementation is proposed in Appendix B.

5.1 Protocol Description

Anonymous coins. An anonymous coin is a triplet $A = (id, cm, \sigma)$ where id is the unique identifier (UID) of an active account, cm is a random commitment on a value $v \in [0, \kappa_{\text{max}}]$ using some randomness $r$, denoted $cm = \text{com}_r(e)$, and $\sigma$ is a threshold signature from a quorum of authorities on the pair $\langle id, cm \rangle$. Following the notations of Section 3, an anonymous coin $A$ can also be seen as a certificate $A = \text{cert}(id, cm, \sigma)$. To spend a coin, a client must know the value $v$, the randomness $r$, and the authentication key controlling id. Importantly, authorities do not need to store commitments cm or signatures $\sigma$ but only manage the active accounts id. Looking ahead, spending the same coin twice will be prevented by making sure that the id is only spent once, or in other words, by removing id from the list of active accounts.

New account operation. We extend the account operations of Section 4 with a locking operation $O = \text{Spend}(value, \text{hash}(P))$ meant to be included in a request Lock(id, n, O) in order to prepare some payment $P$, withdraw value coins publicly, and eventually deactivate the corresponding account. (See details below and algorithm 1.)

Creating anonymous coins. Suppose that a user owns $\ell$ coins $A_i^{in} = (id_i^{in}, cm_i^{in}, \sigma_i^{in})$ ($1 \leq i \leq \ell$) such that all id$_i^{in}$ are registered with the authorities as active, the cm$_i^{in}$ are $\ell$ mutually distinct random commitments, and $\sigma_i^{in}$ is a blind rand randomizable signature on $\langle id_i^{in}, cm_i^{in} \rangle$ supporting threshold issuance [28]. Let $\ell_i^{in}$ be the value of the coin $A_i^{in}$. Let value $\geq 0$ be a value that the user wishes to withdraw publicly from the account id$_i^{in}$.

Importantly, we require commitments cm$_j^{in}$ to be distinct but not the identifiers id$_j^{in}$. This allows several coins to be linked to the same account — assuming that their owner agrees to spend them simultaneously. In practice, we expect $\sum_j value_j$ to be the entire balance of the set of accounts $\{id_j^{in}\}$ about to be closed, to the user’s knowledge.

We define the total input value of the transfer as $v = \sum_j (v_j^{in} + value_j)$. To spend the coins into d new coins with values $v_j^{out}$ ($1 \leq j \leq d$) such that $\sum_j v_j^{out} = v$, the sender requests an UID $id_j^{out}$ from each recipient, then proceeds as follows:

1. First, the sender constructs a payment description $P$ as follows:
   (a) For $1 \leq j \leq d$, sample randomness $r_j^{out}$ and set $cm_j^{out} = \text{com}_{r_j^{out}}(v_j^{out})$.
   (b) For $1 \leq j \leq d$, sample random blinding factor $u_j$ and let $B_j = \text{blind}((id_j^{out}, cm_j^{out}); u_j)$. 

(c) Construct a zero-knowledge proof \( \pi \) for the following statement: I know \( a_i^n, r_i^n \) for each \( 1 \leq i \leq \ell \) and \( e_j^n, o_j^n, u_j, id_j^n \) for each \( 1 \leq j \leq d \) such that
- \( cm_i^n = cm_{i^n}^{\pi_i}(a_i^n) \) and \( cm_{o_j^n}^{\pi_i}(e_j^n) \)
- \( B_j = \text{blind}(e_j^n, cm_{o_j^n}^{\pi_i}(e_j^n); u_j) \)
- \( \sum_j id_j^n + \sum_j value_j = \sum_j e_j^n \)
- Each value \( e_j^n \) and \( o_j^n \) is in \( [0, \sigma_{\text{max}}] \)

(d) Let \( P = (\pi, A_1^n, ..., A_{\ell}^n, value_1, ..., value_\ell, B_1, ..., B_d) \).

(2) For every distinct \( id \in \{id_{\ell}^n\} \), the sender broadcasts an authenticated request \( R_i = \text{Lock}(id, n, O) \) where \( O = \text{Spend}(value, hash(P)) \), \( n \) is the next available sequence number for the account \( id \), and \( value = \sum id_{id=\ell} \).

(3) Upon receiving an authenticated request \( R = \text{Lock}(id, n, \text{Spend}(value, h)) \) from the owner of id, an authority \( \alpha \) verifies that next_sequence\( \&(\alpha) = n \), pending\( id_{\ell}^{\alpha}(\alpha) \), and \( 0 \leq value \leq \text{balance}^{\alpha}_{\ell}(\alpha) \). Then, \( \alpha \) sets pending\( id_{\ell}^{\alpha}(\alpha) = R \) and responds with a signature on \( R \).

(4) The sender collects a quorum of signatures for each \( R_i \) sent above, thus forming a certificate \( L_i = \text{cert}[R_i] \) for every \( i \). It now sends a free request \( R^\prime = \text{CreateAnonymousCoins}(P, L_1, ..., L_\ell) \) to all authorities and waits for a quorum of responses.

(5) Upon receiving a free request of the form \( R^\prime = \text{CreateAnonymousCoins}(P, L_1, ..., L_\ell) \) where
\[
P = (\pi, A_1^n, ..., A_{\ell}^n, value_1, ..., value_\ell, B_1, ..., B_d)
\]
and \( A_1^n = (id_{\ell}^{\pi_1}, cm_{\ell}^{\pi_1}, value_1, ..., value_\ell, B_1, ..., B_d) \)
and the following:
- The values \( cm_1 \) are mutually distinct.
- For every \( i, \sigma_{\ell}^{\pi_i} \) is a valid signature on \( (id_{\ell}^{\pi_i}, cm_{\ell}^{\pi_i}) \).
- Every \( L_i \) is a valid certificate for a request of the form \( R_i = \text{Lock}(id, n, O) \) such that we have \( id = id_{\ell}^{\pi_i}, O = \text{Spend}(value, hash(P)), \) and \( value = \sum id_{id=\ell} \).
- The proof \( \pi \) is valid.

The authority then deactivates each account \( id_{\ell}^{\pi_i} \) (if needed), and responds with \( d \) signature shares, one for each \( B_j = \text{blind}(e_j^n, cm_{o_j^n}^{\pi_i}(e_j^n); u_j) \).

(6) For every \( j \), the sender finally combines the signature shares received by a quorum of authorities, then unblinds to obtain a signature \( e_j^{\pi_i} \) on \( (id_{\ell}^{\pi_i}, cm_{o_j^n}^{\pi_i}(e_j^n)) \).

(7) The \( j \)th recipient receives \( (id_{\ell}^{\pi_i}, cm_{o_j^n}^{\pi_i}(e_j^n), e_j^{\pi_i}, o_j^{\pi_i}) \). She verifies that the values and UIDs are as expected, that the commitments \( cm_{o_j^n}^{\pi_i} \) are mutually distinct, that the signatures \( e_j^{\pi_i} \) are valid.

We note that finality is achieved as soon as the request \( R^\prime \) is formed by the sender. Importantly, the operation Spend is a locking operation (Section 4), meaning that a certificate \( L_i = \text{cert}[R_i] \) alone is not sufficient to be executed and deactivate the account \( id_{\ell}^{\pi_i} \).

Appendix B provides a concrete instantiation of this scheme.

The corresponding pseudo-code for coin creation is presented in Algorithm 3.

### Algorithm 3 Coin creation service

1. function \( \text{HandleCoinCreationRequest}(R^\prime) \)
2. let \( \text{CreateAnonymousCoins}(P, L_1, ..., L_\ell) = R^\prime \)
3. let \( (\pi, A_1^n, ..., A_{\ell}^n, value_1, ..., value_\ell, B_1, ..., B_d) = P \)
4. let \( (id_i, cm_{\pi_i}, \sigma_i) = A_j \) for each \( i = 1, ..., \ell \)

5. for \( i = 1, ..., \ell \) do
6. ensure \( cm_i \not\in \{cm_k\}_{k<i} \)
7. ensure \( \sigma_i = \text{cert}(id_i, cm_{\pi_i}) \) is a valid certificate
8. ensure \( L_i = \text{cert}[R_i] \) is a valid certificate
9. match \( \text{Lock}(id, n, \text{Spend}(value, h)) = R_i \)
10. ensure \( h = \text{hash}(P) \)
11. ensure \( id = id_i \)
12. ensure \( value = \sum id_{id=\ell} \)

13. let \( s_j = \text{SignShare}(B_j) \) for each \( j = 1, ..., d \)
14. verify the ZK-proof \( \pi \) on inputs \( (cm_1, ..., cm_\ell, s, B_1, ..., B_d) \)
15. for \( i = 1, ..., \ell \) do
16. \( \text{pk}^{\pi_i} \leftarrow \bot \) \( \text{// Deactivate sender accounts} \)
17. let \( s_j = \text{SignShare}(B_j) \) for each \( j = 1, ..., d \)
18. return \( (s_1, ..., s_d) \) \( \text{// Return a blinded signature for each output} \)

We define a new (regular) account operation
\[
O = \text{SpendAndTransfer}(id', value, \sigma_1, ..., \sigma_\ell, u_1, ..., u_\ell, r_1, ..., r_\ell)
\]
meant to be included in a request \( R = \text{Execute}(id, n, O) \). Following the framework of Section 4:
- \( O \) is safe \( id \in \text{accounts}(\alpha), 0 \leq value \leq \text{balance}^{\alpha}_{\ell}(\alpha), \) and every signature \( \sigma_i \) is a valid signature of a distinct pair \( (id_i, cm_{\pi_i}) \) with \( cm_{\pi_i} = \text{cert}(u_i) \).
- Upon receiving a valid confirmation certificate \( C = \text{cert}[R], \) the execution of \( O \) consists in removing the account id and sending a cross-shard request to add the value \( o = value + \sum_i u_i \) to balance\(^{\alpha'}_{\ell}(\alpha) \) (possibly after creating an empty account id').

The pseudo-code for redeeming operations is presented in Algorithm 1.

### 5.2 Security Properties

**Safety of the protocol.** We say that an account id is locked-or-deleted \( id \) if there exists a valid certificate of the form
- \( L = \text{cert}[R] \) where \( R = \text{Lock}(id, n, O) \) for some locking operation \( O \), or
- \( C = \text{cert}[R] \) where \( R = \text{Execute}(id, n, O) \) such that \( O \) is an operation \( \text{SpendAndTransfer} \) or \( \text{CloseAccount} \).

If \( O \) is a transfer operation we write \( value(O) \) for the value of the transfer, \( source(O) \) for the main account, \( recipient(O) \) for the recipient account. By extension, we write \( value(C) \) for a valid confirmation certificate containing such operation \( O \). Summations over certificates range over all valid certificates for distinct requests or coins.

We define the \( \text{spendable value} \) of an account id as spendable\( id = 0 \) if id is locked-or-deleted, and otherwise:
\[
\text{spendable}^{id} = \text{balance}^{id}(\text{init}) + \sum_{\text{recipient}(C)=id} value(C) - \sum_{\text{source}(C)=id} value(C) + \sum_{id(A)=id} value(A)
\]
We note that if an authority \( a \) is perfectly up to date with the certificates related to id and the account id is not locked-or-deleted:

\[
\text{spendable}^{id} = \text{balance}^{id}(a) + \sum_{id(A) = id} \text{value}(A)
\]

The protocol for account operations entails that a locked-or-deleted account id can never produce new certificates \( C \) (in particular with recipient \( (C) = id^r \neq id \)). Indeed, the case of account deletion was analyzed in Section 4. Similarly, in the case of a locking request \( R = \text{Lock}(id, n, O) \), at least a quorum of authorities \( a \) have processed \( R \). From this point on, the account id held by such authority \( a \) can only (i) process the same locking request \( R \) and return the same vote, or (ii) become deleted or inactive. By quorum intersection, no new certificate can be produced.

By inspection of the protocol, we deduce that the total spendable value over all accounts \( S = \sum_{id} \text{spendable}^{id} \) never increases during regular account operations, coin creation, and redeeming of anonymous coins:

- Regular account operations have been studied in Section 4.
- Redeeming coins with SpendAndTransfer increases the balance of a recipient but changes the account to be locked-or-deleted, effectively “burning” at least an equivalent amount. (To this effect, note that the definition of spendable counts distinct coins and so does the protocol.)
- Creating coins with a free request \( R^* \) = CreateAnonymousCoins\( (P, L_1, \ldots, L_t) \) requires changing all the source accounts in \( L_1, \ldots, L_t \) to be locked-or-deleted. Importantly, \( L_t \) contains a commit of \( P \) and cannot re-used for another payment \( P' \neq P \). We also note that replaying \( R^* \) produces the same coins \( A_j \) and does not increase \( S \).

Liveness considerations. For coin creation, we used hash\( (P) \) instead of \( P \) in each \( R_i \) both to minimize communication and for liveness. Indeed, it is important for the initiator to keep \( P \) secret before collecting all the certificates \( L_i \). We note that otherwise an attacker knowing \( P \) may intercept the requests \( R_i \), use them to obtain the certificates \( L_i \), then send \( R_i \) to kill the input accounts \( id^{in}_{j} \) before the sender has a chance to replay the requests \( R_i \). Depending on the archiving policy for \( L_i \), this may leave the sender unable to replay \( R^* \) to obtain the signature shares of step (5).

Privacy properties. The protocol to create anonymous coins guarantees the following privacy properties:

- Opacity: Except for the ZK proofs \( \pi \), the coin values under the commitments \( cm^{in}_{j} \) and \( cm^{out}_{j} \) are never communicated publicly.
- Unlinkability: Assuming that the sender during coin creation is honest, authorities cannot trace back to the origin of an anonymous coin when it is spent.

Regarding unlinkability, we note indeed that the receiver information \( id^{out}_{j} \) and \( cm^{out}_{j} \) are only communicated to authorities in blinded form. Besides, after unblinding, the threshold signature \( \sigma_j \) does not depend on values controlled by authorities, therefore is not susceptible to tainting.

To prevent double spending, the protocol must reveal the identifiers \( id^{in}_{j} \) of the coins being spent. This means that the sender who initially created the coins linked to \( id^{in}_{j} \) must be trusted for unlinkability to hold. To mitigate this concern, it is recommended that receivers of anonymous coins re-send their coins anonymously to themselves sometime before spending their coins.

In general, the account identifiers \( id^{out}_{j} \) needed for anonymous transfers should be obtained ahead of time and using anonymity solution such as Tor. For simplicity, we have only described account authentication based on a transparent public key \( pk^{id}(a) \). In practice, using a random commitment of a public key and a proof of knowledge of the corresponding secret would allow using the same authentication key for several accounts without degrading privacy.

6 IMPLEMENTATION

We implement a multi-core, multi-shard Zef authority in Rust, based on the existing FastPay codebase\(^4\) which implements the Byzantine reliable broadcast needed. In particular, we were able to re-use modules based on Tokio\(^5\) for asynchronous networking and cryptographic modules based on ed25519-dalek\(^6\) for elliptic-curve-based signatures. For simplicity, data-structures in our Zef prototype are held in memory rather than persistent storage. The core of Zef is idempotent to tolerate retries in case of packet loss. Each authority shard is a separate native process with its own networking and Tokio reactor core. We are open-sourcing Zef\(^7\) along with any measurements data to enable reproducible results\(^8\).

We have chosen Coconut credentials\(^28\) to implement the blind randomized threshold-issuance signatures \( \sigma^{in}_{j} \) and \( \sigma^{out}_{j} \) of Section 5. Zero-Knowledge proofs are constructed using standard sigma protocols, made non-interactive through the Fiat-Shamir heuristic\(^16\). As a result, our implementation of Zef assumes the hardness of LRSW\(^20\) and XDH\(^8\) (required by Coconut), and the existence of random oracles\(^16\). Appendix B presents this protocol in details. Our implementation of Coconut is inspired from Nym\(^9\) and uses the curve BLS12-381\(^33\) as arithmetic backend.

We have implemented all range proofs using Bulletproofs\(^9\) as they only rely on the discrete logarithm assumption (which is implied by XDH) and do not require a trusted setup. Unfortunately, we couldn’t directly use Dalek’s implementation of Bulletproofs\(^10\) as it uses Ristretto\(^14\) as arithmetic backend. Ristretto is incompatible with Coconut (which requires a pairing-friendly curve). Therefore, we have modified Dalek’s implementation to use curve BLS12-381. This required significant effort as the curve operations are deeply baked into the library. Our resulting library is significantly slower than Dalek’s for two reasons: operations over BLS12-381 are slower than over Ristretto, and we couldn’t take advantage of the parallel formulas in the AVX2 backend present in the original library. We are open-sourcing our Bulletproof implementation over BLS12-381\(^11\).

7 EVALUATION

We now present our evaluation of the performance of our Zef prototype based on experiments on Amazon Web Services (AWS).

\(^4\)https://github.com/novifinancial/fastpay  
\(^5\)https://tokio.rs  
\(^6\)https://github.com/dalek-cryptography/ed25519-dalek  
\(^8\)https://github.com/novifinancial/fastpay/tree/extensions/bulletproofs  
\(^11\)https://github.com/novifinancial/fastpay/tree/extensions/bulletproofs
We measured it by tracking sample requests throughout the system. We benchmarked the performance of Zef when making a regular Xeon Platinum 8175, 128GB memory, and ran Linux Ubuntu server (collocated on the same machine) submitting transactions at a fixed Tokyo (ap-northeast-1). Authorities were distributed across those regions as equally as possible. Each machine provided 10Gbps of bandwidth, 32 virtual CPUs (16 physical core) on a 2.5GHz, Intel Xeon Platinum 8175, 128GB memory, and ran Linux Ubuntu server 20.04. We selected these machines because they provide decent performance and are in the price range of “commodity servers”.

In the following sections, each measurement in the graphs is the average of 2 independent runs, and the error bars represent one standard deviation. We set one benchmark client per shard (collocated on the same machine) submitting transactions at a fixed rate for a duration of 5 minutes.

7.1 Regular Transfers

We benchmarked the performance of Zef when making a regular transfer as described in Section 4. When referring to latency in this section, we mean the time elapsed from when the client submits the request (Step 1 in Figure 1) to when at least one honest authority processes the resulting confirmation certificate (Step 5 in Figure 1). We measured it by tracking sample requests throughout the system.

Benchmark in the common case. Figure 4 illustrates the latency and throughput of Zef for varying numbers of authorities. Every authority ran 10 collocated shards (each authority ran thus a single machine). The maximum throughput we observe is 20,000 tx/s for a committee of 10 nodes, and lower (up to 6,000 tx/s) for a larger committee of 50. This highlights the importance of sharding to achieve high-throughput. This reduction is due to the need to transfer and check transfer certificates signed by 2\(f\) + 1 authorities; increasing the committee size increases the number of signatures to verify since we do not use threshold signatures for regular transfers.

Scalability. Figure 5 shows the maximum throughput that can be achieved while keeping the latency under 250ms and 300ms.

Our focus was to verify that (i) Zef achieves high throughput even for large committees, (ii) Zef has low latency even under high load and within a WAN, (iii) Zef scales linearly when adding more shards, and (iv) Zef is robust when some parts of the system inevitably crash-fail. Note that evaluating BFT protocols in the presence of Byzantine faults is still an open research question [4].

We deployed a testbed on AWS, using m5.8xlarge instances across 5 different AWS regions: N. Virginia (us-east-1), N. California (us-west-1), Sydney (ap-southeast-2), Stockholm (eu-north-1), and Tokyo (ap-northeast-1). Authorities were distributed across those regions as equally as possible. Each machine provided 10Gbps of bandwidth, 32 virtual CPUs (16 physical core) on a 2.5GHz, Intel Xeon Platinum 8175, 128GB memory, and ran Linux Ubuntu server 20.04. We selected these machines because they provide decent performance and are in the price range of “commodity servers”.

In the following sections, each measurement in the graphs is the average of 2 independent runs, and the error bars represent one standard deviation. We set one benchmark client per shard (collocated on the same machine) submitting transactions at a fixed rate for a duration of 5 minutes.

7.1 Regular Transfers

We benchmarked the performance of Zef when making a regular transfer as described in Section 4. When referring to latency in this section, we mean the time elapsed from when the client submits the request (Step 1 in Figure 1) to when at least one honest authority processes the resulting confirmation certificate (Step 5 in Figure 1). We measured it by tracking sample requests throughout the system.

Benchmark in the common case. Figure 4 illustrates the latency and throughput of Zef for varying numbers of authorities. Every authority ran 10 collocated shards (each authority ran thus a single machine). The maximum throughput we observe is 20,000 tx/s for a committee of 10 nodes, and lower (up to 6,000 tx/s) for a larger committee of 50. This highlights the importance of sharding to achieve high-throughput. This reduction is due to the need to transfer and check transfer certificates signed by 2\(f\) + 1 authorities; increasing the committee size increases the number of signatures to verify since we do not use threshold signatures for regular transfers.

Scalability. Figure 5 shows the maximum throughput that can be achieved while keeping the latency under 250ms and 300ms.

Our focus was to verify that (i) Zef achieves high throughput even for large committees, (ii) Zef has low latency even under high load and within a WAN, (iii) Zef scales linearly when adding more shards, and (iv) Zef is robust when some parts of the system inevitably crash-fail. Note that evaluating BFT protocols in the presence of Byzantine faults is still an open research question [4].

We deployed a testbed on AWS, using m5.8xlarge instances across 5 different AWS regions: N. Virginia (us-east-1), N. California (us-west-1), Sydney (ap-southeast-2), Stockholm (eu-north-1), and Tokyo (ap-northeast-1). Authorities were distributed across those regions as equally as possible. Each machine provided 10Gbps of bandwidth, 32 virtual CPUs (16 physical core) on a 2.5GHz, Intel Xeon Platinum 8175, 128GB memory, and ran Linux Ubuntu server 20.04. We selected these machines because they provide decent performance and are in the price range of “commodity servers”.

In the following sections, each measurement in the graphs is the average of 2 independent runs, and the error bars represent one standard deviation. We set one benchmark client per shard (collocated on the same machine) submitting transactions at a fixed rate for a duration of 5 minutes.

7.1 Regular Transfers

We benchmarked the performance of Zef when making a regular transfer as described in Section 4. When referring to latency in this section, we mean the time elapsed from when the client submits the request (Step 1 in Figure 1) to when at least one honest authority processes the resulting confirmation certificate (Step 5 in Figure 1). We measured it by tracking sample requests throughout the system.

Benchmark in the common case. Figure 4 illustrates the latency and throughput of Zef for varying numbers of authorities. Every authority ran 10 collocated shards (each authority ran thus a single machine). The maximum throughput we observe is 20,000 tx/s for a committee of 10 nodes, and lower (up to 6,000 tx/s) for a larger committee of 50. This highlights the importance of sharding to achieve high-throughput. This reduction is due to the need to transfer and check transfer certificates signed by 2\(f\) + 1 authorities; increasing the committee size increases the number of signatures to verify since we do not use threshold signatures for regular transfers.

Scalability. Figure 5 shows the maximum throughput that can be achieved while keeping the latency under 250ms and 300ms.

Our focus was to verify that (i) Zef achieves high throughput even for large committees, (ii) Zef has low latency even under high load and within a WAN, (iii) Zef scales linearly when adding more shards, and (iv) Zef is robust when some parts of the system inevitably crash-fail. Note that evaluating BFT protocols in the presence of Byzantine faults is still an open research question [4].

We deployed a testbed on AWS, using m5.8xlarge instances across 5 different AWS regions: N. Virginia (us-east-1), N. California (us-west-1), Sydney (ap-southeast-2), Stockholm (eu-north-1), and Tokyo (ap-northeast-1). Authorities were distributed across those regions as equally as possible. Each machine provided 10Gbps of bandwidth, 32 virtual CPUs (16 physical core) on a 2.5GHz, Intel Xeon Platinum 8175, 128GB memory, and ran Linux Ubuntu server 20.04. We selected these machines because they provide decent performance and are in the price range of “commodity servers”.

In the following sections, each measurement in the graphs is the average of 2 independent runs, and the error bars represent one standard deviation. We set one benchmark client per shard (collocated on the same machine) submitting transactions at a fixed rate for a duration of 5 minutes.

7.1 Regular Transfers

We benchmarked the performance of Zef when making a regular transfer as described in Section 4. When referring to latency in this section, we mean the time elapsed from when the client submits the request (Step 1 in Figure 1) to when at least one honest authority processes the resulting confirmation certificate (Step 5 in Figure 1). We measured it by tracking sample requests throughout the system.

Benchmark in the common case. Figure 4 illustrates the latency and throughput of Zef for varying numbers of authorities. Every authority ran 10 collocated shards (each authority ran thus a single machine). The maximum throughput we observe is 20,000 tx/s for a committee of 10 nodes, and lower (up to 6,000 tx/s) for a larger committee of 50. This highlights the importance of sharding to achieve high-throughput. This reduction is due to the need to transfer and check transfer certificates signed by 2\(f\) + 1 authorities; increasing the committee size increases the number of signatures to verify since we do not use threshold signatures for regular transfers.

Scalability. Figure 5 shows the maximum throughput that can be achieved while keeping the latency under 250ms and 300ms.
We measured it by in Figure 2) to when it assembles the new coins (Step 3 in Figure 2). We measured it by tracking sample requests throughout the system.

### 7.2 Anonymous Payments

We benchmarked the performance of Zef when spending two opaque coins into two new ones, as described in Section 5. When referring to latency in this section, we mean the time elapsed from when the client submits the request (Step 2 in Figure 2) to when it assembles the new coins (Step 3 in Figure 2). We measured it by tracking sample requests throughout the system.

**Microbenchmarks.** We report on microbenchmarks of the single-CPU core time required execute the cryptographic operations. Table 1 displays the cost of each operation in milliseconds (ms); each measurement is the result of 100 runs on a AWS m5.8xlarge instance. The first 3 rows respectively indicate the time to (i) produce a coin creation request meant to spend two opaque coins into two new ones, (ii) verify that request, and (iii) issue a blinded coin share. The last 3 rows indicate the time to unblind a coin share, verify it, and aggregate 3 coin shares into an output coin. The dominant CPU cost is on the user when creating a coin request (438.35ms), which involves proving knowledge of each input coins (1 Bulletproof per coin). However, verifying coin requests (142.31ms) is also expensive: it involves verifying the input coins (1 pairing check per input coin) and the output coins request (1 Bulletproof per coin). Issuing a blinded coin share (1 Coconut signature per output coin) is relatively faster (4.90ms). Unblinding (3.37ms), verifying (9.62ms) and aggregating (1.70ms) coin shares take only a few milliseconds. These results indicate that a single core shard implementation may only settle just over 7 transactions per second—highlighting the importance of sharding to achieve high-throughput.

**Benchmark in the common case.** Figure 7 illustrates the latency and throughput of Zef for varying numbers of authorities. Every authority runs 10 collocated shards. The performance depicted in Figure 7 (anonymous payments) are 3 order of magnitude lower than those depicted in Figure 4 (regular transfers); this is due to the expensive cryptographic operations reported in Table 1. We observe virtually no difference between runs with 10, 20, 30, or even 50 authorities: Zef can process about 50 tx/s while keeping latency under 1s in all configurations. This highlights that anonymous payments operations are extremely CPU intensive and that bandwidth is far from being the bottleneck.

**Scalability.** Figure 8 shows the maximum throughput that can be achieved while keeping the latency under 500ms and 1s. The committee was composed by 4 authorities each running a data-center; each shard runs on a separate machine. Figure 5 demonstrates our scalability claim: throughput increases linearly with the number of shards, ranging from 5 tx/s with 1 shard per authority to 55 tx/s with 10 shards per authority (with a latency cap of 1s).

**Benchmark under crash-faults.** Figure 9 depicts the performance of Zef when a committee of 10 authorities suffers 1 to 3 crash-faults. Every authority ran 35 collocated shards (each authority ran thus a single machine). There is no noticeable throughput drop under crash-faults, and Zef can process up to 100 tx/s within a second with 0, 1, or 3 faults. The performance of Zef shines compared to Zcash [7] which is known to process about 27 tx/s with a 1 hour latency [2]. Similarly, Monero [22] processes about 4 tx/s with a 30 minute latency [2].

### 8 CONCLUSION

Zef is the first linearly-scalable BFT protocol for anonymous payments with sub-second latency. Zef defines authorities as sharded services and by managing singly-owned objects using reliable broadcast rather than consensus. To support anonymous coins without sacrificing storage costs, Zef introduces a new notion of uniquely-identified, spendable account. Users can bind new anonymous coins to their accounts and spend coins in a privacy-preserving way thanks to state-of-the-art techniques such as the Coconut scheme [28]. Despite the CPU-intensive cryptographic operations required to preserve opacity and unlinkability of digital coins, our experiments confirm that anonymous payments in Zef provides unprecedentedly quick confirmation time (sub-second instead of tens of minutes) while supporting arbitrary throughput thanks to the linearly-scalable architecture.
REFERENCES


[15] Amirali Abdolfattahi, Hamidreza Ghorbani, and Iraj Fazlalizadeh. 2019. Transparent coins. A certificate T = cert[S] on a triplet S = (id, v, r) where id is the UID of an active account, v ∈ [0, vmax], and r is some random seed value.

[16] Seed values r are used to distinguish coins of the same value attached to the same id. In what follows, we identify certificates with the same content, that is: cert[S] = cert[S′] iff S = S′.

[17] To spend a transparent coin C, a client must possess the authentication key controlling id. Importantly, authorities do not need to store C themselves—although they will observe such certificates occasionally in clear.

[18] New account operation. Similar to Section 5, we assume a locking account operation $O = Spend\text{valu}e, hash(P))$ meant to prepare some payment P (see below), withdraw value coins publicly, and eventually destroy the corresponding account.

[19] Transparent coin payment protocol. Suppose that a user owns f mutually distinct transparent coins $T^i = cert[S^i]$ where $S^i = (id^i, v^i, r^i)$ (1 ≤ i ≤ f). Let $value_i ≥ 0$ be a value that the user wishes to withdraw publicly from the account id^i.

[20] Similar to Section 5, we require certificates $T^i$ to be distinct but not the UIDS id^i. In practice, we expect $\Sigma_i value_i$ to be the entire balance of the set of accounts (id^i).

[21] We define the total input value of the transfer as $\Sigma_i (v^i + value_i)$. To spend the coins into d new coins with values $v^\text{out}_j (1 ≤ j ≤ d)$.
For every \( j \leq d \) such that \( \sum_j q^\text{out}_j = v \), the sender requests an UID \( id^\text{out}_j \) from each recipient, then proceeds as follows:

1. First, the sender constructs a payment description \( P \) as follows:
   a. For every \( 1 \leq j \leq d \), sample randomness \( r^\text{out}_j \)
   b. Let \( P = (T^\text{in}_1, \ldots, T^\text{in}_n, \text{value}_1, \ldots, \text{value}_n, S^\text{out}_1, \ldots, S^\text{out}_n) \)

2. For every distinct \( id^\text{in}_i \), the sender broadcasts an authenticated request \( R_i = \text{Lock}(id^\text{in}_i, n_i, O) \) where \( O = \text{Spend(value, hash}(P)) \), \( n_i \) is the next available sequence number for the account \( id^\text{in}_i \), and value = \( \sum_{id^\text{in}_i} \text{value}_i \).

3. Upon receiving an authenticated request \( R = \text{Lock}(id, n, \text{Spend(value, h)}) \) from the owner of an account \( \alpha \), \( \alpha \) verifies that next_sequence\( \alpha(n) = n \), pending\( \alpha(n) = 1 \), and \( 0 \leq \text{value} \leq \text{balance}\( \alpha(n) \). Then, \( \alpha \) sets pending\( \alpha(n) = R \) and responds with a signature on \( R \).

4. The sender collects a quorum of signatures for each \( R_i \) sent above, thus forming a locking certificate \( L_i = \text{cert}[R_i] \) for every \( i \). It now sends a request \( R^* = \text{CreateTransparentCoins}(P, L_1, \ldots, L_d) \) to all authorities and waits for a quorum of responses.

5. Upon receiving a free request of the form \( R^* = \text{CreateTransparentCoins}(P, L_1, \ldots, L_d) \) such that

\[
P = (T^\text{in}_1, \ldots, T^\text{in}_n, \text{value}_1, \ldots, \text{value}_n, S^\text{out}_1, \ldots, S^\text{out}_n)
\]

where \( T^\text{in}_j = \text{cert}(id^\text{in}_j, r^\text{in}_j) \) and \( S^\text{out}_j = (id^\text{out}_j, v^\text{out}_j, \ell^\text{out}_j) \), each authority \( \alpha \) verifies the following:

- The certificates \( T^\text{in}_i \) are valid and mutually distinct.
- Every \( L_i \) is a valid certificate for some request \( R_j = \text{Lock}(id, n, O) \) where \( id = id^\text{in}_i \), \( O = \text{Spend(value, hash}(P)) \), and value = \( \sum_{id^\text{in}_i} \text{value}_i \).

The authority then destroys each account \( id^\text{in}_i \) (if needed) and responds with \( d \) signatures, one for each \( S^\text{out}_j \).

6. For every \( j \), the sender finally combines a quorum of signatures on \( S^\text{out}_j \) into a new coin \( T^\text{out}_j \).

7. The \( j \)th recipient receives \( T^\text{out}_j = \text{cert}(id^\text{out}_j, v^\text{out}_j, \ell^\text{out}_j) \).

The verifies that the values and UIDDs are as expected, that the random seeds \( r^\text{out}_j \) are mutually distinct, and that the certificates \( T^\text{out}_j \) are valid.

### Redeeming transparent coins
Suppose that a user owns \( \ell \) transparent coins \( T_i \) \( (1 \leq i \leq \ell) \) linked to the same active account id. We define a new account operation

\[
O = \text{SpendAndTransfer}(id', value, T_1, \ldots, T_\ell)
\]

meant to be included in a request \( R = \text{Execute}(id, n, O) \) and following the framework of Section 4:

- \( O \) is safe iff id \in accounts(\alpha), 0 \leq \text{value} \leq \text{balance}\( \alpha(n) \), and every \( T_j \) is a valid certificate of some distinct triplet \( S_j = (id, q_j, r_j) \).
- Upon receiving a valid certificate \( C = \text{cert}[R_j] \), the execution of \( O \) consists in removing the account id and sending a cross-shard request to add the value \( \text{value} = \text{value} + \sum_j q_j \) to balance\( id'(\alpha) \) (possibly after creating an empty account id').

### B NIZK Protocol

In this section, we show one possible efficient instantiation of the anonymous payment protocol from Section 5 by opening up the cryptographic primitives used. Our protocol here makes use of the Coconut threshold credential scheme [28], which is based on the work of Pointcheval and Sanders [24]. Informally, Coconut allows users to obtain credentials on messages with private attributes in a distributed setting using a threshold \( t \) out of \( n \) authorities.

#### B.1 Coconut++

We start by giving an overview of a suitable variant of the Coconut scheme, nicknamed Coconut++. This variant of Coconut is formally proven secure by Rial and Piotrowska [26]. At a high level, Coconut allows a user to obtain, from a threshold number of authorities, an anonymous credential on a private attribute \( m \) showing that it satisfies some application-specific predicate \( \phi(m) = 1 \). Later, the user can anonymously prove the validity of this credential to any entity in possession of the verification key. While the standard Coconut scheme works for a single attribute, [28] also includes an extension that allows for credentials on a list of \( q \) integer-valued attributes \( \bar{m} = (m_1, \ldots, m_q) \).

Below, we use the notation \( \bar{X} = (X_1, \ldots, X_q) \) for any list of \( q \) variables \( X_i \) \( (1 \leq i \leq q) \). The scheme Coconut++ consists of the following algorithms:

| Setup(1^\ell) \rightarrow (pp) | Choose groups \((G_1, G_2, G_T)\) of order \( p \) (a \( \ell \)-bit prime) with a bilinear map \( e : G_1 \times G_2 \rightarrow G_T \). Let \( H : G_1 \rightarrow G_1 \) be a secure hash function. Let \( q_1, q_2, \ldots, q_q \) be generators of \( G_1 \) and let \( g_2 \) be a generator of \( G_2 \). The system parameters are given as \( pp = (G_1, G_2, G_T, p, e, H, g_1, g_2, h) \). Parameters are implicit in the remaining descriptions.
| KeyGen(t, n) \rightarrow (sk, vk) | Pick \( q + 1 \) polynomials \( u, v_1, \ldots, v_q \) each of degree \( t \) - 1 with coefficients in \( F_p \) and set \( sk = (x, y) = (u(0), v_1(0), \ldots, v_q(0)) \). Publish the verification key \( vk_1 = (y, x, \beta) = (y, x, \beta) \)\). Also issue to each authority \( j \in \{1, \ldots, n\} \), the secret key \( sk_j = (x_j, y_j) = (u(j), w(j), \ldots, v_q(j)) \). Publish the corresponding verification key \( vk_j = (y_j, x_j, \beta) = (y_j, x_j, \beta) \) for every \( j \). PrepareBlindSign(\( \bar{m}, \phi \)) \rightarrow (r, A) | Pick a random \( o \in F_p \). Compute the commitment \( c_o \) and group element \( h \) as

\[
c_o = g_1^o \prod_{i=1}^{q} h_i^{x_i} \quad \text{and} \quad h = H(c_o)
\]

For all \( i = 1 \ldots q \), pick a random \( r_i \in F_p \) and compute the blinded value \( c_i \) as follows:

\[
c_i = h^{x_i} g_1^{r_i}
\]

Output \((r, A)\) where \( A = (c_o, c, \pi_o) \) where \( \pi_o \) is defined as:

\[
\pi_o = \text{NIZK}(\bar{m}, \bar{r}, \bar{o}) : \forall i, c_i = h^{x_i} g_1^{r_i} \land c_o = g_1^o \prod_{i=1}^{q} h_i^{x_i} \land \phi(c_o) = 1
\]
We now instantiate the anonymous transfer protocol from Section 5 using the Coconut scheme with three attributes \( m = (k, q, v) \) consisting of a key \( k \), a random seed \( q \), and a private coin value \( v \). From the point of view of its owner, an opaque coin is defined as \( A = (\text{id}, x, q, v, \sigma) \) where \( \text{id} \) is the linked account, \( x \) is an unique index within the same account \( \text{id} \), \( q \) is a secret random seed, \( v \) is the value of the coin, and \( \sigma \) denotes the Coconut credential for \( k = \text{hash}(\text{id} :: [x], q, v) \). When a new opaque coin is created, the three attributes are hidden to authorities. The account \( \text{id} \text{id} \) and the index \( x \) of a coin are revealed when it is spent to verify coin ownership and prevent double-spending of coins within the same account. We use the third attribute \( q \) to guarantee the privacy of the value \( v \) even after \( k \) is revealed\(^\text{13}\).

Suppose that a sender owns \( t \) input coins \( A_i^\text{in} = (\text{id}_i^\text{in}, x_i^\text{in}, q_i^\text{in}, v_i^\text{in}, \sigma_i^\text{in}) \) (\( 1 \leq i \leq t \)) and wishes to create \( d \) output coins of the form \( (\text{id}_j^\text{out}, x_j^\text{out}, q_j^\text{out}, v_j^\text{out}, \sigma_j^\text{out}) \) (\( 1 \leq j \leq d \)). Let \( v_i^\text{out} \) denote the public value associated with the Zef account \( \text{id}_i^\text{in} \) (possibly 0) as in Section 5. The sender must ensure that \( \sum_i v_i^\text{in} = \sum_j v_j^\text{out} \) and that the coin indices \((\text{id}_j^\text{out}, x_j^\text{out})\) are mutually distinct.

Using Coconut for opaque coin transfers. We present an overview of the changes to the anonymous transfer protocol from Section 5 to implement opaque coins. We present an intuition on how these changes use the Coconut primitives described in Appendix B1); the next paragraphs provide detailed explanations of the opaque coin transfer protocol.

Recall that the sender first constructs a payment description \( P \) and uses it to lock the UIDs of the input coins. For this, the sender proceeds as follows. For every \( 1 \leq i \leq t \), it reveals \( k_i^\text{in} \). Then, for every \( 1 \leq i \leq t \) and \( 1 \leq j \leq d \), it calls

\[
\Theta_i \leftarrow \text{ProveCred}(\text{vk}, (q_i^\text{in}, v_i^\text{in}), \sigma_i^\text{in}, \phi')
\]

and

\[
((rk_j, rq_j, rv_j, \Lambda_j) \leftarrow \text{PrepareBlindSign}(k_j^\text{out}, q_j^\text{out}, v_j^\text{out}, \phi')
\]

where \( \phi' \) is a predicate satisfied by the input and output coin values and defined as follows: \( \phi'(q_i^\text{in}, v_i^\text{out}) = \text{true} \)

\[
\sum_i q_i^\text{in} + \sum_i v_i^\text{out} = \sum_j v_j^\text{out} \quad \land \quad v_i^\text{out} \in [0, v_{\text{max}}]
\]

Effectively, the predicate \( \phi' \) binds the NIZKs associated with all ProveCred proofs for the input coins and all PrepareBlindSign proofs for the output coins. It also shows that the value on both sides of the transfer is consistent. The payment description \( P \) reveals \( \tilde{k}^\text{in} \) and \( \tilde{x}^\text{in} \) (and thus \( k^\text{in} \)), and is now constructed as

\[
P = (\tilde{k}^\text{in}, \tilde{x}^\text{in}, \Theta, \Lambda, \phi', A_1^\text{in}, \ldots, A_n^\text{in}, v_1^\text{out}, \ldots, v_l^\text{out})
\]

Recall now that the sender uses this \( P \) to lock the input UIDs, and after retrieving a locking certificate for each UID from the authorities, it submits the request \( R^\text{in} = \text{CreateAnonymousCoins}(P, L_1, \ldots, L_i) \) where \( l_i \) denote locking certificates. On receiving \( R^\text{in} \) from the sender, an authority \( \chi \) now verifies the proofs \( \Theta \) and \( \Lambda \) and the predicate \( \phi' \) by running

\[
\text{VerifyCred}(\text{vk}, \Theta_i, \phi') \quad \text{for each \( i \) and } \sigma_i^\text{out} = \text{BlindSign}(sk_X, \Lambda_i, \phi')
\]

for each \( i \). If the proofs are valid, it returns \( \sigma^\text{out} \) to the sender.

After collecting \( t \) such responses, the sender can now run Unblind and AggCred to obtain a valid credential on each created output coin. Finally, to complete the transfer, it can send the coin \((\text{id}_j^\text{out}, x_j^\text{out}, q_j^\text{out}, v_j^\text{out}, \sigma_j^\text{out})\) to the \( j^{\text{th}} \) recipient.

\(^\text{13}\)As noted in the original Coconut paper [28], if a credential contains a single attribute \( m \) of low entropy (such as a coin value), the verifier can run multiple times the verification algorithm making educated guesses on the value of \( m \) and effectively recover its value through brute-force.
**Opaque coin construction.** We present the cryptographic primitives used by the opaque coins transfer protocol. The Setup and KeyGen algorithms are exactly the same as Coconut.

- **CoinRequest**(vk, σ^[in], q^[in], k^[out], q^[out], value^[in], value^[out], ..., value^[out]) → (rk, q, r, θ): Parse vk = (y₀, y₁, y₂, α, β₀, β₁, β₂). For every input coin σ^[in] = (hᵢ, sᵢ), pick at random rᵢ, rₛ ∈ ℤ_p, and compute
  \[ hᵢ' = hᵢ^rᵢ \quad \text{and} \quad sᵢ = sᵢ^rᵢ (hᵢ')^{sᵢ} \]
  Then set σᵢ^out = (hᵢ', sᵢ') and build:
  \[ kᵢ = α gᵢ^rᵢ βᵢ^σᵢ^in βᵢ^σᵢ^out \]
  For every output coin j (1 ≤ j ≤ d), pick a random α ∈ ℤ_p, and compute the commitments cm and the group elements hᵢ as
  \[ cm_j = gᵢ^c qᵢ^j hᵢ'^j hᵢ^j \quad \text{and} \quad h_j = H(cm_j) \]
  For all 1 ≤ j ≤ d, pick a random (rk_j, q_j, r_j) ∈ ℤ_p and compute the commitments (ck_j, cq_j, cv_j) as follows:
  \[ ck_j = h_j^{q_j} g_j^{r_j} \quad \text{and} \quad cq_j = h_j^{q_j} g_j^{r_j} \quad \text{and} \quad cv_j = h_j^{q_j} g_j^{r_j} \]
  Output ((rk, q, r, θ), Γ) where Γ = (σ^[in], k, cm, ck, cq, cv, πᵣ) and
  \[ πᵣ = \text{NIZK}(\{σ^[in], k, cm, ck, cq, cv, πᵣ\} : \forall i, kᵢ = α gᵢ^rᵢ βᵢ^σᵢ^in βᵢ^σᵢ^out \]
  \[ \land \forall j, cm_j = gᵢ^c qᵢ^j hᵢ'^j hᵢ^j \]
  \[ \land \forall j, cq_j = h_j^{q_j} g_j^{r_j} \]
  \[ \land \forall j, cv_j = h_j^{q_j} g_j^{r_j} \]
  \[ \land \sum_i τ_i^in + \sum_j τ_j^out = \sum_j τ_j^out \]
  \[ \land e_{τ_i}^{out} ∈ [0, \sigma_{max}] \]

- **IssueBlindCoin**(sk, Γ, k^[in], value^[in], ..., value^[out], value^[out]) → (θ): The authority θ parses sk = (x, y₀, y₁, y₂), vk = (y₀, y₁, y₂, α, β₀, β₁, β₂), and Γ = (σ^[in], k, cm, ck, cq, cv, πᵣ). Recompute h_j = H(cm_j) for each 1 ≤ j ≤ d.
  Verify the proof πᵣ using Γ, hᵢ, vk, value^[in], ..., value^[out], and value^[out]. For each 1 ≤ i ≤ ℓ, parse σ^[in] = (hᵢ, sᵢ'), verify hᵢ' ≠ 1, and that the following bilinear evaluation holds:
  \[ e(θ_i κ_i + β_i^σ_i^in, e) = e(s_i, g_2) \]
  If one of these checks fail, stop the protocol and output ⊥. Otherwise, compute:
  \[ s_j = h_j^ι \cdot \text{ck}_j \cdot \text{cq}_j \cdot \text{cv}_j \]