Zether: Towards Privacy in a Smart Contract World

Benedikt Bünz[1], Shashank Agrawal[2], Mahdi Zamani[3], and Dan Boneh[4]

[1]Stanford University, `benedikt@cs.stanford.edu`
[2]Visa Research, `shaagraw@visa.com`
[3]Visa Research, `mzamani@visa.com`
[4]Stanford University, `dabo@cs.stanford.edu`

Abstract

Blockchain-based smart contract platforms like Ethereum have become quite popular as a way to remove trust and add transparency to distributed applications. While different types of important applications can be easily built on such platforms, there does not seem to be an easy way to add a meaningful level of privacy to them.

In this paper, we propose *Zether*, a fully-decentralized, confidential payment mechanism that is compatible with Ethereum and other smart contract platforms. We take an account-based approach similar to Ethereum for efficiency and usability. We design a new smart contract that keeps the account balances encrypted and exposes methods to deposit, transfer and withdraw funds to/from accounts through cryptographic proofs.

We describe techniques to protect Zether against replay attacks and front-running situations. We also develop a mechanism to enable interoperability with arbitrary smart contracts. This helps to make several popular applications like auctions, payment channels, voting, etc. confidential.

As a part of our protocol, we propose Σ-Bullets, an improvement of the existing zero-knowledge proof system, Bulletproofs. Σ-Bullets make Bulletproofs more inter-operable with Sigma protocols, which is of general interest.

We implement Zether as an Ethereum smart contract and show the practicality of our design by measuring the amount of *gas* used by the Zether contract. A Zether confidential transaction costs about 0.014 ETH or approximately $1.51 (as of early Feb, 2019). We discuss how small changes to Ethereum, which are already being discussed independently of Zether, would drastically reduce this cost.

1 Introduction

Blockchain-based smart contract platforms have great promise to remove trust and add transparency to distributed applications. Ethereum is a prominent example of such a platform [etha]. It provides high-level powerful programming languages like Solidity [Sola] to build decentralized applications (DApps) with ease. Unfortunately, there is no easy way to *add* some meaningful level of privacy to these applications. Take the case of auction contracts for instance, which can be built on Ethereum without much trouble [solb]—but, could we build a *sealed-bid* auction mechanism just as easily?

Sealed-bid auctions work roughly as follows: In a bidding phase, bidders submit *sealed* bids to an auctioneer so that no bidder knows how much others have bid. Afterwards, the bids are unsealed and a winner is chosen by comparing the bid values. If we try to build such

an auction contract on Ethereum, how do bidders deposit their bids with the contract given that all transaction amounts in Ethereum are publicly visible?

There are several ways people deal with this problem in practice. Ethereum Name Service suggests that users submit just a hash of their bids to register a name with the registrar, and deposit more ether (Ethereum's native currency) than the true bid value [ENSa, ENSb]. The official Solidity documentation has an example for blind auctions too, where users submit multiple bids which include some fake ones [solb]. These mechanisms, however, do not hide the bid values completely and put additional burden on the users. Some powerful general-purpose cryptographic solutions have also been proposed to run arbitrary smart contracts in a privacy-preserving way [KMS+16, CZK+18], but they are not fully decentralized and/or too expensive for simple contracts.

Indeed, the quest for confidentiality is not limited to auctions. Payment channels are widely seen as a central technology to increase the throughput of crypto-currencies. On a powerful platform like Ethereum, payment channels can be easily set up too [Fer17, BKM17]—but, could we make such channels *confidential* just as easily?

Confidential transfers. If there was a way to send ether confidentially on Ethereum, perhaps we could leverage it to *add* confidentiality to important applications like auctions and payment channels. Unfortunately, almost all known ways to transfer confidentially [Max15, Noe15, MGGR13, DFKP13, BCG+14] are in the unspent-transaction-output (UTXO) model (popularized by Bitcoin), where the inputs to a new transaction are the unspent outputs of previous transactions. UTXOs are not well-suited for applications that need to maintain some state [But16], so smart-contract platforms like Ethereum operate in the account-based model.

Another drawback of UTXO-based mechanisms is that though they have been proposed to fix privacy issues with Bitcoin, they actually require major changes to Bitcoin's design and have spun off into separate crypto-currencies. An important benefit of powerful platforms like Ethereum is that the platform's core capability itself can be enhanced by deploying new applications. Payment channels, for instance, can be deployed to improve throughput. So perhaps we can deploy a new payment application to improve confidentiality of not just payments but potentially other applications too.

It is still conceivable that one of the UTXO-based mechanisms could be implemented over a contract. However, this approach suffers from multiple issues including storage cost, lower confidentiality, interoperability with other contracts, and adoption. We discuss the issues in depth in Appendix A.

1.1 Zether

In this paper, we propose an efficient, fully-decentralized confidential payment mechanism in the account-based model called *Zether*, which does not require any changes to the design of the underlying smart contract platform like Ethereum. We describe Zether as a smart contract that can be executed either individually or by other smart contracts to exchange confidential amounts of a token, denoted by ZTH. The techniques used in Zether can apply to other account-based crypto-currencies, completely independent of their consensus mechanisms.

Our contributions can be summarized as follows:

- *Confidentiality.* Transactions on Zether are confidential by design. Account balances are kept encrypted at all times and users provide cryptographic proofs to spend ZTH.

- *Zero-knowledge proofs.* Zether uses zero-knowledge (ZK) proofs as an important building block. To efficiently instantiate Zether, we propose a new ZK-proof mechanism, called Σ-**Bullets**, which enhances the interoperability of Σ-protocols [Dåm] and Bulletproofs [BBB+18]. This allows us to efficiently combine Bulletproofs-based range proofs with ElGamal encryptions. (Σ-Bullets could be useful in other settings too.)

- *Implementation.* We implement Zether as an Ethereum smart contract and measure the gas amount required for executing it. We show that Zether is practical today and with already-planned enhancements to Ethereum will become even more efficient. As part of our implementation, we provide an efficient implementation of Bulletproofs [BBB+18] on Ethereum which is of independent interest.

- *Interoperability.* Zether provides a way to lock funds in an account to a smart contract, making it easy to *add* confidentiality to several important applications. We show how Zether can be used in a natural way to build four applications: sealed-bid auction, confidential payment channel, confidential stake-voting, and private proof-of-stake.

- *Anonymity.* We describe an extension to Zether that can also hide the sender and receiver involved in a transaction among a group of users chosen by the sender. Though the overhead associated with anonymity scales linearly with the size of the group, no trusted set-up is needed and no changes to the underlying smart contract platform are required. Thus, Zether anonymity guarantee is more similar to Monero [NMT16] than Zcash [zcaa], but in the account model.

Organization. The rest of the paper is organized as follows. We provide some background on Ethereum in Section 2, with a focus on smart contract execution. Section 3 provides an overview of the Zether payment mechanism, its use in other applications, and the new ZK-proof system. Section 4 defines the cryptographic tools we need for Zether. It then formally defines the notion of a payment mechanism in a smart-contract world, and the security properties it should satisfy. Section 6 provides a detailed description of Zether. Section 7 describes our implementation in Solidity, its evaluation, various optimizations, etc. Section 8 shows how Zether can be used with smart contracts to get more privacy. Section 9 discusses the work related to Zether.

We describe an anonymous version of Zether in detail in Appendix D. Appendix F has some discussion on important matters related to the use of Zether. Finally, Appendix G has a thorough discussion of Σ-Bullets.

2 Background on Ethereum

Accounts are Ethereum's basic units. There are (a) *externally-owned accounts (EOAs)*, controlled by private keys and (b) *contract accounts*, controlled by their code. Both types of accounts have an ether balance, denominated in units of *wei*: 1 ether is 1e18 wei. The Ethereum blockchain tracks the state of every account [etha, Woo]. State changes are initiated through *transactions* coming from EOAs. A transaction consists of the destination account address, a signature σ, the transferred amount in wei, an optional data field representing inputs to a contract, a GASLIMIT value, and a GASPRICE value. Every EOA is associated with a nonce, a counter that increments with every transaction. The signature σ signs the transaction and the sender's nonce. During transaction processing, σ is verified against the nonce value. As a result, transactions cannot be "replayed" on the Ethereum network [etha].

A transaction can transfer wei between accounts or trigger the execution of smart contract code. Contracts can send messages to other contracts, mimicking function calls. Every transaction and code execution is replicated on all nodes in the network. Every executed operation has a specified cost expressed in terms of *gas* units. For example, storing 256 bits of data costs 20,000 units of gas while changing it costs 5,000 and reading it costs 200 [Woo]. The sender pays for all contract operations that the transaction calls.

The sender sets GASLIMIT field to the total amount of gas she is willing to spend for a transaction, and the GASPRICE field to the amount of wei she is willing to pay per unit of gas. A miner, that is happy with the gas price, can include the transaction in a block and collect the fee. If the gas limit falls short of the gas needed to process the transaction, the miner will collect the fee but not change the blockchain's state. Excess fees are refunded to the account that issued the transaction [Woo].

The total gas consumed by all transactions in a block is limited. This ensures that the time needed for processing and propagating a block remains sufficiently small, allowing for an adequately-decentralized network. Currently that limit is around 8 million gas units. Simple arithmetic operations cost 3 gas units and the average block time is 15s. The total Ethereum network can, therefore, perform less than 180k arithmetic operations per second. Some complex operations, e.g., the Keccak 256-bit hash function, however, do not need to be arithmetized but are provide as a standalone functionality at a reduced cost (36 gas for a 32 byte hash) [Woo].

Contracts are written in specific programming languages such as Solidity [Sola]. Once compiled to bytecode, the contract can be read and executed by the *Ethereum virtual machine (EVM)*, a sandboxed and isolated runtime environment. The EVM has access to a global persistent storage system and each contract account has separate storage available to it.

In Ethereum, transactions are processed individually in an arbitrary order. Therefore, it is important to ensure that contract codes are written properly so that unexpected outcomes are avoided when a common part of the EVM state is changed by two or more transactions [LCO+16]. The low computational power, along with the asynchronous transactional nature of the Ethereum network make programming complicated smart contracts a delicate endeavor.

3 Overview of Zether

In this section, we provide an overview of the Zether payment mechanism, its use in other applications, and the new ZK-proof system.

Commitment vs encryption. Several proposals for making transactions confidential use homomorphic commitments, such as Pedersen commitments [Ped92]. Though they are simple and efficient, the opening of these commitments must be transferred to the receiver, say Bob, so that he can spend the money later. This randomness could be stored on-chain in some encrypted manner or sent directly to Bob through a separate channel. In the UTXO model, if Bob is unable to recover the randomness (an incorrect value was encrypted/sent, nothing sent at all, etc.), then it cannot spend the UTXO later. However, other UTXOs controlled by Bob are not affected at all and could still be spent. On the other hand, with an account-based model, since all the incoming transfers go into the same account, failure to recover the randomness for even a single transfer could render the whole account unusable.

One could require senders to encrypt the randomness under receivers' public key, and prove that the commitment indeed uses the randomness encrypted. We take a more direct

and simpler approach here using ElGamal encryption with messages in the exponent [CGS97]. The encryption scheme has linear encoding properties, i.e., it is homomorphic, which we utilize to create efficient ZK-proofs of correct encryption. We describe the encryption scheme in Section 4.

3.1 Building Zether

Zether strives not just to make transfers confidential but also to prevent accidental loss of funds. We first discuss a simplistic version of Zether with the core functionality. We then describe some shortcomings and how to overcome them.

A simplistic Zether. The Zether smart contract (ZSC) works with Zether tokens (ZTH). Zether accounts are identified with ElGamal public keys, which are stored in ZSC's internal state. To fund an account with public key y with b ZTH, one can send b ETH to the smart contract. ZSC generates an ElGamal encryption of b with randomness 0 (since b is anyway part of the transaction) and *adds* it to the encrypted balance associated with y.[1] One can convert ZTH back to ETH by revealing the current balance $b^\star$ and providing a ZK-proof that y's ciphertext (i.e., the ciphertext associated with y on the smart contract) indeed encrypts $b^\star$.

In order to transfer some b amount of ZTH to a public key y' without revealing b itself, one can encrypt b under *both* y and y'. A ZK-proof is provided to show that the two ciphertexts are well-formed, they encrypt the same positive value, and the remaining balance associated with y is positive. In our implementation, we use a new ZK-proof system, called Σ-Bullets to efficiently prove the statements over the encrypted transfer balance and the new sender balance.

Front-running. The very first problem with the simplistic version of Zether is that the ZK-proofs are generated w.r.t. a certain state of the contract. For example, the ZK-proof in a transfer transaction needs to show that the remaining balance is positive. A user Alice generates this proof w.r.t. to her current account balance, stored in an encrypted form on the contract. However, if another user Bob transfers some ZTH to Alice, and Bob's transaction gets processed first, then Alice's transaction will be rejected because the proof will not be valid anymore. Note that Bob may be a totally benign user yet Alice loses the fees she paid to process her transaction. We refer to this situation as the *front-running* problem. Burn transactions have a similar problem too: a proof that a ciphertext encrypts a certain value becomes invalid if the ciphertext changes.

To solve this problem, one could introduce a new type of transaction that just locks an account to keep away incoming transfers. Alice could wait until this transaction gets into the blockchain before initiating an outgoing transfer (or doing a burn). While this seems to fix the problem (at the cost of making transfer, the primary transaction, a two-step process), it creates new problems for users like Bob who want to send ZTH to Alice. Alice's account may not be locked when Bob publishes a transfer transaction tx, but it could get locked before tx gets in, resulting in tx being rejected.

Any kind of locking approach becomes more untenable when we bring in anonymity. (We will discuss anonymity in more detail at the end of this section.) If Alice wants to hide herself among other users and make sure that her transaction gets through, she will have to lock *all*

---

[1]If y has no record on ZSC yet, then a new record is created and initialized with the aforementioned ciphertext.

the accounts in the anonymity set. Clearly, this cannot be allowed: Alice must not be able to lock accounts of other users. Alternatively, Alice could only put locked accounts in her anonymity set. However, if someone unlocks their account before Alice's transaction gets in, Alice's degree of anonymity is reduced.

Pending transfers. To address the front-running problem, we keep all the incoming transfers in a *pending* state. These transfers are rolled over into the accounts from time to time so that the incoming funds could be spent. This rollover cannot happen at arbitrary times, otherwise the proofs would get invalidated again.

To handle this, we divide time into *epochs* where an epoch consists of k consecutive blocks. The choice of k depends on two factors: a) the gap between the latest state of blockchain and any user's view, and b) the time it takes to get a transaction into the blockchain. At the end of every epoch, pending transfers are rolled over into the corresponding accounts. Users are expected to publish their transfer or burn transaction at the beginning of an epoch so that even if they do not see the latest state of the blockchain and it takes some time for their transaction to be included, they do not step into the next epoch. As long as k is chosen wisely, transactions will be processed before the account changes state.

Rolling over on a smart contract. Unfortunately, rolling over accounts is not as straightforward as it may appear because a smart contract does not do anything unless a transaction is sent to it. One cannot expect every user to send a rollover message for every epoch. Moreover, there is no way they will be able to get such a message in at the right time.

A first idea is to rollover the pending transfers for *all* accounts on the receipt of the first message in an epoch. This, however, places an unreasonably large burden on the sender of that message: it will have to pay for the cost of rolling over the accounts that it does *not* own, which could be too many. Furthermore, users would have no way to know if their transaction would be the first in an epoch, so they cannot estimate the right amount of gas to supply.

We rollover an account in an epoch when the first message from *this* account is received; so, one message rolls over only one account. To achieve this, we define a separate (internal) method for rolling over, and the first thing every other method does is to call this method. There could be accounts that do not get rolled over for several consecutive epochs because no transaction is initiated from them. This is not a problem because the account holder, say Alice, is not trying to use her money anyway. At some later point in time, when Alice wants to operate on her account, she will publish a transaction. All the money transferred into her account since the last rollover will be rolled over immediately and become available to be spent. Indeed, when Alice creates a ZK-proof, she will assume the state of her account to be what it would be when all the pending transfers are rolled over into it.

Replay protection. Like any other payment mechanism, Zether needs to handle replay attacks. Ethereum provides replay protection of its own by associating nonces with every account, which need to be signed into every transaction. Unfortunately, this level of protection is not enough for Zether due to two reasons: (1) Zether accounts have their own public keys; they are not associated with Ethereum addresses. (2) Zether transactions contain *non-interactive* ZK-proofs. A malicious actor can steal these proofs and put them inside new transactions. If the state of the account has not changed, then the new transactions will also be processed successfully, leading to loss of funds. Later in this section, we will discuss another important feature of Zether: locking accounts to other smart contracts. Even if the request to lock a Zether account shows knowledge of the secret key, and the account is unlocked later, an adversarial entity could lock the account again by just replaying the request.

To protect against such issues, we associate a nonce with every Zether account. The nonces are incremented as transactions are processed. A new transaction from an account must sign the latest value of the nonce associated with the account along with the transaction data, which includes any ZK-proof. This approach binds all components of a transaction together and ensures freshness. ZK-proofs cannot be imported into malicious transactions and valid transactions cannot be replayed.

One way wonder if there is a way to use Ethereum addresses themselves as the identities of Zether accounts. The accounts would then be operated with the secret keys corresponding to the addresses, and we would get replay protection and signature verification for free. However, this would force users to operate a Zether account from a fixed Ethereum address. They would not be able to delegate the account to a different address, like when locking the account to a smart contract (which will be discussed in more detail later). Furthermore, Ethereum addresses are only a hash of public keys, not the full form. Proving statements about hashes in zero-knowledge is quite expensive. Lastly, having separate public keys for Zether accounts also helps make the design more modular and platform-independent.

Anonymity. Zether can be extended to transfer anonymously. An anonymous version of Zether needs a more complex ZK-proof, a new replay and double-spend protection mechanism, and a different mechanism to lock accounts to smart contracts. We defer the discussion to Appendix D.1.

3.2   Interoperability with Smart Contracts

A main design goal for Zether is to be interoperable with arbitrary smart contracts, which may contain bugs or even be maliciously designed. An important distinction between regular users and smart contracts is that contracts cannot generate ZK-proofs because they do not have any secret state. As a result, they cannot initiate a ZTH transfer.

We make Zether interoperable with other smart contracts by exposing a lock/unlock functionality. To illustrate, suppose Alice owns an account acc. She can *lock* acc to any arbitrary smart contract, say SC. In effect, this transfers the ownership of acc to SC. Now, Zether will process only those transactions on acc that come from SC. Any transactions sent by Alice, other users or other contracts will simply be declined. ZK-proofs, however, would still be generated by Alice if needed, and transferred to the Zether smart contract via SC. SC can finally *unlock* acc to return its control to Alice.

Even this simple locking mechanism can help us realize several important applications in a confidential away. We provide a brief discussion here and defer the details to Section 8.

Sealed-bid auctions. Auctions are used to sell a wide variety of resources on Ethereum [Tok]. A primary example is the Ethereum Name Service (ENS) [ENSa]. In the ENS bidding phase, a bidder submits a hash of her bid along with an amount of ether. ENS suggests that the amount should be higher than the bid value to disguise the true value of the bid. There are several drawbacks to this approach including that it reveals a good upper-bound to bid value. Using Zether, bidders can simply lock their accounts (or transfer the bid value to a new account and lock that) to the auction contract, thus getting full bid confidentiality. No other collateral needs to be put in place. After the bidding phase, bidders can open their bids by providing a ZK-proof on the encrypted bid value (a *burn* proof essentially). The auction smart contract can then simply unlock the accounts of the bidders who lost.

Confidential payment channels. Payment channels are widely considered to be one of the most important solutions to the scalability problem of crypto-currencies. On Ethereum, they can be set up very easily through smart contracts. A certain amount of ether is locked into the contract, transfers are conducted off-the-chain between the parties, and then a final settlement is made on chain. This clearly reveals a lot of information, but Zether can be used to prevent it. A Zether account could be locked to the channel contract and ZK-proofs could be exchanged offline to show that the channel has enough liquidity. Thus, we have a simple way to make channels confidential.

Stake voting. Several blockchain-based voting protocols have been proposed to deal with the transparency issues of traditional voting systems. An important example is the Open Vote Network of McCorry et al. [MSH17]. Here, the vote values are binary: participants publish a special encryption of their votes and prove that they are 0 or 1. With Zether, we can allow the votes to carry weights, proportional to the assets a participant owns. Once again, this can be achieved by just locking account to the vote contract and proving in zero-knowledge that the vote value is equal to the amount locked.

Proof-of-stake. Proof-of-stake is a popular alternative to the wasteful proof-of-work consensus mechanism. Users *stake* a number of coins and then a random beacon is used to select one of them as leader. This reveals the stake of users, making them susceptible to targeted attacks. Zether could be used to make proof-of-stake confidential. At a high level, users could encrypt an initial lottery ticket t under their public key and stake an encrypted Zether balance b under the same key. Then the random beacon value is used to derive a lottery drawing v. If v falls between t and $t + b$ then the user wins the lottery, which it can prove without revealing t or b. See Appendix 8.4 for details.

3.3 Σ-Bullets

Zether ensures that encrypted transactions are correct by using ZK-proofs that certify correctness without revealing any additional information. We design a custom proof system called Σ-Bullets that is well-suited for Zether. Σ-Bullets integrate Bulletproofs [BBB$^+$18] with Σ-protocols to enable efficient proofs on algebraically-encoded values such as $\exists x : g^x = y \wedge h^x = u \in \mathbb{G}$. Bulletproofs on the other hand is a circuit proof system that is well suited for range proofs and other more complicated arithmetic statements. Bulletproofs does enable proofs on Pedersen committed values if all values use the same commitment key. With Σ-Bullets we can prove complex statements on algebraically encoded data. For example, we can efficiently prove that a set of ElGamal encrypted values are in some range. Further, we combine one-out-of-many proofs[GK15], also known as ring signatures, with range proofs to allow anonymous transfers. The one-out-of-many proof is a Σ-protocol that hides which account is being used. Bulletproof is then used to show that the account has sufficient funds for the transfer. Σ-Bullets inherit from Bulletproofs the trapdoor-free setup and the short, logarithmic sized, proof lengths. The ability to prove statements on encrypted values further significantly reduces the prover and verifier time compared to a naive implementation using Bulletproofs. We describe Σ-Bullets in detail in Appendix G.

4 Notation and Tools

We use λ to denote the security parameter. Let GroupGen be a polynomial-time algorithm that on input 1^λ outputs $(p, g, \mathbb{G})$ where $p = \Theta(\lambda)$, p is prime, $\mathbb{G}$ is a group of order p, g is a generator of $\mathbb{G}$, and the decisional Diffie-Hellman (DDH) assumption holds in $\mathbb{G}$. The DDH assumption states that a tuple $(g, g^a, g^b, g^{a \cdot b})$ is computationally indistinguishable from (g, g^a, g^b, g^c) for random a, b, c. It implies the discrete logarithm assumption.

Let $\mathbb{Z}_p$ denote the integers modulo p. $\mathbb{Z}_p^\star$ is the set of inverses in $\mathbb{Z}_p$. We use $[a, b]$ for $a, b \in \mathbb{Z}$ to denote the set of integers $\{a, a + 1, \ldots, b - 1, b\}$.

We use $x \xleftarrow{\$} S$ to denote that x is sampled uniformly at random from a set S. We use PPT as a shorthand for probabilistic polynomial time and $\mathsf{negl}(\lambda)$ to denote negligible functions.

ElGamal encryption. ElGamal encryption is a public key encryption scheme secure under the DDH assumption. A random number from $\mathbb{Z}_p^\star$, say x, acts as a private key, and $y = g^x$ is the public key corresponding to that. To encrypt an integer b, it is first mapped to one or more group elements. If $b \in \mathbb{Z}_p$, then a simple mapping would be to just raise g to b. Now, a ciphertext for b is given by $(g^b y^r, g^r)$ where $r \xleftarrow{\$} \mathbb{Z}_p^\star$. With knowledge of x, one can divide $g^b y^r$ by $(g^r)^x$ to recover g^b. However, g^b needs to be brute-forced to compute b.

We argue that this is not an issue. First, as we will see, the Zether smart contract does not need to do this, only the users would do it. Second, users will have a good estimate of ZTH in their accounts because, typically, the transfer amount is known to the receiver. Thus, brute-force computation would occur only rarely. Third, one could represent a large range of values in terms of smaller ranges. For instance, if we want to allow amounts up to 64 bits, we could instead have 2 amounts of 32 bits each, and encrypt each one of them separately. In this paper, for simplicity, we will work with a single range, 1 to MAX, and set MAX to be 2^{32} in the implementation.

The primary benefit of putting balances in exponent is that it makes ElGamal encryption additively homomorphic. If b and b' are encrypted under the same public key y to get ciphertexts $(C_L = g^b y^r, C_R = g^r)$ and $(C'_L = g^{b'} y^{r'}, C'_R = g^{r'})$ respectively, then $(C_L C'_L = g^{b+b'} y^{r+r'}, C_R C'_R = g^{r+r'})$ is an encryption of $b + b'$ under y.

Zero-knowledge proofs. A zero-knowledge (ZK) proof of a statement does not reveal any information beyond the validity of the statement. For example, one could prove that two ciphertexts encrypt the same message without revealing the message itself. Though any NP statement can be proved in zero-knowledge, the concrete costs depend on a number of factors.

Σ protocols are honest-verifier public-coin zero-knowledge interactive proofs of a special form. Very efficient Σ protocols exist for proving a wide variety of algebraic statements like knowledge of b and r s.t. an ElGamal ciphertext encrypts b with randomness r. The Fiat-Shamir transform is a way of transforming any public-coin honest-verifier ZK-proof (like Σ protocols) into a *non-interactive* zero-knowledge *proof of knowledge* in the random oracle model.

A ZK-proof for the statement

$$\mathsf{st} : \{(a, b, c, \ldots; x, y, z, \ldots) : f(a, b, c, \ldots, x, y, z, \ldots)\}$$

means that the prover shows knowledge of $x, y, z, \ldots$ such that $f(a, b, c, \ldots, x, y, z, \ldots)$ is true, where $a, b, c, \ldots$ are public variables. We use $\mathsf{st}[a, b, c, \ldots]$ to denote an instance of st where the variables $a, b, c, \ldots$ have some fixed values.

We represent a non-interactive ZK (NIZK) proof system with algorithms $(\mathsf{Setup_{nizk}}, \mathsf{Prove}, \mathsf{Verify_{nizk}})$, where $\mathsf{Setup_{nizk}}$ outputs some public parameters, Prove generates a proof for a statement given a witness, and $\mathsf{Verify_{nizk}}$ checks if the proof is valid w.r.t the statement. Zether uses NIZKs that are a) correct, an honest prover can produce a valid proof b) zero-knowledge, a verifier learns nothing from the proof but the validity of the statement, and c) sound, a computationally bounded prover cannot convince a verifier of a false statement. Σ protocols, with the Fiat-Shamir transform applied, have all these properties.

Digital signatures. Signature schemes are used to authorize messages by *signing* them. A verifier can check a signature but will be unable to forge a signature on a previously unsigned message. Signatures can be built from Fiat-Shamir transformed NIZK proofs [AABN02].

We represent a signature scheme with algorithms $(\mathsf{Setup_{nizk}}, \mathsf{Sign}, \mathsf{Verify_{nizk}})$, where $\mathsf{Setup_{nizk}}$ outputs some public parameters, Sign generates a signature on an input message, and $\mathsf{Verify_{nizk}}$ checks if the signature is valid w.r.t. the message. Zether requires a signature scheme that is a) correct, it is possible to create valid signatures on arbitrary messages and b) existentially unforgeable, a computationally bounded adversary can't create a valid signature on a *new* message, even after seeing signatures on other messages.

We omit formal definitions for brevity and refer to [BS18] for a thorough treatment of the properties.

5 Payment Mechanism

A payment mechanism for Ethereum consists of a setup routine, user algorithms, and a smart contract. The contract maintains a state st which changes over time. The state at block height h is denoted by st_h. Users rely on the state of the smart contract to create transactions. A user account is identified by a public key pk. Let MAX be the maximum amount of money that the mechanism can handle. Any amount below must be an integer between 0 and MAX.[2]

The payment mechanism also provides a way to lock funds of an account to an Ethereum address addr so that the address can control the movement of funds through the account, until the lock is released. In Section 8, we will use the locking/unlocking feature to bring privacy to several commonly used smart contracts.

The term *transaction* is used in Ethereum to refer to a signed data package that stores a message to be sent from an externally owned account to another account on the blockchain. It can include binary data (its payload) and Ether. If the target account contains code, that code is executed and the payload is provided as input data. For a transaction tx, we use $\mathsf{tx.ETH}$ to denote the amount of ether being sent through tx.

Contracts can call other contracts or send Ether to non-contract accounts by the means of *message calls*. The message call most relevant to us is $\mathsf{msg.sender.transfer}$ (in the syntax of Solidity) which transfers a certain amount of Ether from a contract to the sender who called it. For a transaction tx that calls a function f on a contract, we use $f(\mathsf{tx}).\mathsf{ETH}$ to denote the amount of Ether successfully sent back to the caller when f is executed with tx. (In Figure 5 and Figure 2, where we describe the details of our Zether instantiation, we use a programming oriented, Solidity inspired, syntax as defined in Table 1.)

We are now ready to describe the various components of a payment mechanism.

---

[2]MAX should be treated as a constant with respect to the security parameter.

Setup. In the setup phase, some public parameters are generated. They could be distributed off-chain or put into the smart contract (described below). The smart contract is also deployed.

User algorithms. A user can run one of the following algorithms to interact with the smart contract. The output of these algorithms are *raw* transactions. We leave it implicit that they will be signed (using the public key of the Ethereum account from which they are sent) and destined to the Zether smart contract. Nonetheless, we use tx.addr to denote the Ethereum address addr from which tx was sent. All the algorithms get the security parameter as input but we show it explicitly only for the first one.

1. CreateAddress(1^λ) → (sk, pk). CreateAddress provides a way for a user to uniquely identify itself to the smart contract. It takes (a unary representation of) the security parameter as input and outputs a secret key sk and a public key pk. We assume that pk is derived in a deterministic way from sk, and use pkOf(sk) to denote the public key that corresponds to sk.

2. CreateFundTx(pk, amt) → tx_{fund}. CreateFundTx is used to add funds to an account. It takes a public key pk and an amount amt as inputs. It outputs $tx_{fund} = (pk, \ldots)$.

3. CreateTransferTx($sk_{from}, pk_{to}, amt, st_h$) → tx_{trans}. CreateTransferTx is used to transfer money from one account to another. It takes a secret key sk_{from}, a destination public key pk_{to}, an amount amt, and the state of the smart contract st_h at a certain block height h as inputs. It outputs tx_{trans}. (For anonymous transfers, this algorithm would also take a set AnonSet as input, which would contain both pkOf(sk_{from}) and pk_{to}. AnonSet would be a part of the output too.)

4. CreateBurnTx(sk, st_h) → tx_{burn}. CreateBurnTx is used to withdraw the entire balance from an account. It takes a secret key sk and a state st_h as inputs. It outputs $tx_{burn} = (pkOf(sk), amt, \ldots)$.

5. CreateLockTx(sk, addr, st_h) → tx_{lock}. CreateLockTx is used to lock an account to an Ethereum address. It takes a secret key sk and an address addr as inputs. It outputs $tx_{lock} = (pkOf(sk), addr, \ldots)$.

6. CreateUnlockTx(pk) → tx_{unlock}. CreateUnlockTx is used to unlock an account. It takes a public key pk as input. It outputs $tx_{unlock} = (pk, \ldots)$.

7. ReadBalance(sk, st_h) → b. ReadBalance is used to find the balance of an account. It takes a secret key sk and state st_h as inputs, and outputs an integer b.

Smart contract. The smart contract has five functions Fund, Transfer, Burn, Lock and Unlock. They take tx_{fund}, tx_{trans}, tx_{burn}, tx_{lock} and tx_{unlock}, respectively. These functions output 1 or 0, denoting success and failure respectively. If any of the inputs are not of the correct type the function automatically fails. Moreover the functions check certain properties of the input, such as verifying a proof or checking a nonce. If any of these checks fail, the function outputs 0. The five functions modify the state st as needed. We use SC as a shorthand for the smart contract.

SC has access to the current block height and the sender of every transaction. (In Solidity, the syntax for these are block.number and msg.sender, respectively.) It makes use of two constants: maximum amount value MAX and epoch length E, where E ≥ 1. The epoch number of a block at height h is defined to be $\lfloor h/E \rfloor$. Thus, for example, the blocks at heights $0, 1, \ldots, E - 1$ are in the first epoch, the ones at heights $E, E + 1, \ldots, 2E - 1$ are in the second epoch, and so on.

11

We now discuss informally the correctness and security requirements of a payment mechanism. See Appendix B and C for formal definitions. The definitions are for the more general case of anonymity, where not only the transfer amount but the sender/receiver are also hidden (among a chosen set of public keys).

Correctness. Correctness captures the basic functionality a payment mechanism should provide if transactions are generated honestly but they could be sent from arbitrary Ethereum addresses and processed in an arbitrary order. We will assume, however, that if a transaction is generated in a certain epoch, then it gets processed in the same epoch. To illustrate, suppose Alice has X ZTH in her account. In an epoch e_1, she publishes a transfer transaction to send $Y \leq X$ ZTH to someone else. There could be other users in the network who transfer to Alice at about the same time. Even if some of these transfers are processed before Alice's, we don't want her transfer to fail. Further, suppose Alice receives Z ZTH from others in e_1. Then, in any epoch after e_1, if she publishes a burn transaction with amount $X - Y + Z$, then we would like her to get back that amount of ETH.

To specify correctness formally, we define the notion of an *ideal state* and describe how it evolves over time as honestly generated transactions are processed. The ideal state tracks the balance of every account and the Ethereum address (if any) to which it is locked. When a transaction is processed, the ideal state is updated depending on the type of transaction and the current state. Informally, we say that a payment mechanism is correct if whenever a burn transaction is processed for a certain account, the amount of Ether returned to the user is equal to the amount of Zether held in the *ideal state account*.

Security requirements. We define two security requirements for a payment mechanism Π, overdraft-safety and privacy. Overdraft-safety ensures that users cannot misuse the smart contract to withdraw more money from their accounts that they rightfully own. Privacy of a payment-mechanism ensures that no additional information about the payments of honest parties beyond the intended is leaked to an adversary. In other words, only the sender and receiver of a payment should know the amount transferred in the payment. The formulation of overdraft-safety and privacy is inspired by Zerocash [BCG+14].

We define a game between a challenger Chal and an adversary Adv to capture the requirements, where Chal represents the honest users in the network. Both Chal and Adv have access to an oracle $\mathcal{O}_{SC}$ who maintains the smart contract SC. Adv has full view of the oracle: it can see all the transactions sent by Chal to SC, how the state of SC changes, etc. We provide Adv substantial control over SC's state. It can instruct any honest party at any time (via the challenger) to publish a transaction. It can create its own malformed transactions based on the transactions of honest parties, and then push the former into the blockchain ahead of the latter. In particular, it can arbitrarily delay the transactions of honest parties.

For overdraft-safety, we associate some quantities with the game with respect to Adv: EtherDeposited, ZetherReceived and EtherBurnt, which have self-explanatory names. Informally, a payment mechanism is safe against overdrafts if

$$\text{EtherDeposited} + \text{ZetherReceived} \geq \text{EtherBurnt}.$$

There are two important things to note here. First, it is not enough to just require that the *total* ether burnt (honest parties and adversary combined) should be no more than the *total* ether deposited because it could still be possible that the adversary is able to burn more than its fair share. Second, we cannot take the more direct approach of computing the amount

<div style="border:1px solid black; padding:10px;">

<u>Setup</u>

INPUT: Security parameter λ (in unary)

1. $(p, g, \mathbb{G}) \leftarrow \mathsf{GroupGen}(1^\lambda)$
2. $\mathrm{pp}_{\mathsf{nizk}} \leftarrow \mathsf{Setup}_{\mathsf{nizk}}(1^\lambda)$
3. $\mathrm{pp}_{\mathsf{sig}} \leftarrow \mathsf{Setup}_{\mathsf{nizk}}(1^\lambda)$
4. Initialize
   - empty account table, $\mathsf{acc} : \mathbb{G} \to \mathbb{G}^2$
   - empty pending transfers table, $\mathsf{pTransfers} : \mathbb{G} \to \mathbb{G}^2$
   - an empty last roll over epoch table, $\mathsf{lastRollOver} : \mathbb{G} \to \mathbb{Z}$,
   - an empty lock table, $\mathsf{lock} : \mathbb{G} \to \{0,1\}^*$,
   - an empty counter table, $\mathsf{ctr} : \mathbb{G} \to \mathbb{Z}$,
   - total balance $b_{\mathsf{total}} \in \mathbb{Z}$ to 0,
5. Deploy smart contract ZSC (Figure 2) with parameters $(p, g, \mathbb{G}), \mathrm{pp}_{\mathsf{nizk}}, \mathrm{pp}_{\mathsf{sig}}, \mathsf{acc}, \mathsf{pTransfers},$ $\mathsf{lastRollOver}, \mathsf{lock}, b_{\mathsf{total}}, \mathsf{MAX}, \mathsf{E}$.
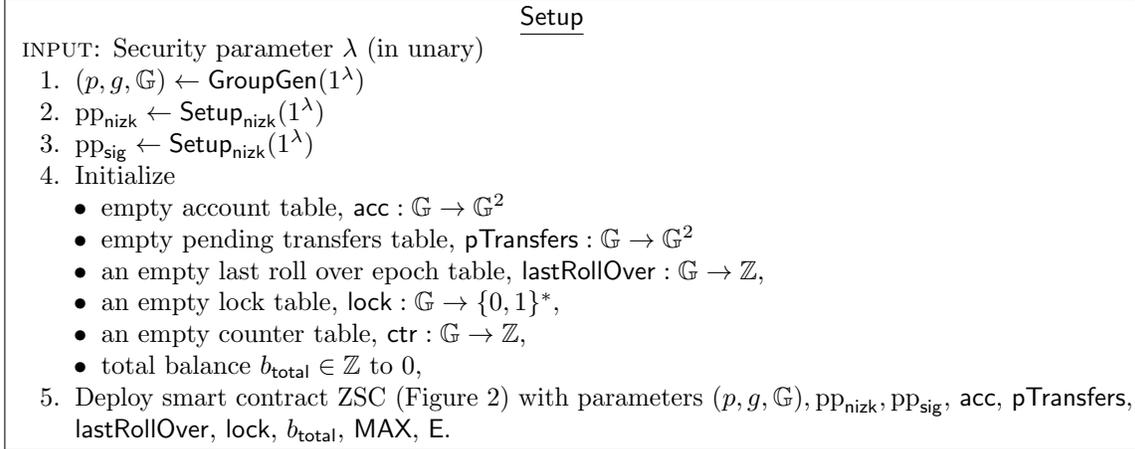
</div>

Figure 1: Zether setup

adversary can withdraw by just reading the balance of the accounts controlled by it from the smart contract because its secret keys are not available.

We slightly modify the game discussed above to capture the privacy requirement. Instead of sending just one instruction to Chal every time (asking an honest party to create a transaction), Adv sends two *consistent* instructions at some point. Chal executes the $(b+1)$-th instruction based on a bit b hidden from Adv, which is chosen randomly in advance. Adv is supposed to guess b at the end of the game. (This is the typical left-or-right setting used for indistinguishability-based definitions.) Consistency is defined carefully to rule out trivial wins for the adversary.

6 Zether Payment Mechanism

We now present a secure payment mechanism called Zether. It consists of three components: a global setup algorithm that is run once to generate the global parameters for the protocol as well as to deploy the Zether smart contract. The second component is the Zether smart contract (ZSC) that handles transactions between users, interoperability with external smart contracts, and keeps the state of the system. The final component of the mechanism are the user algorithms which describe how users can interact with the smart contract and create valid transactions. A user is of course not bound to the behavior described in the user algorithms. Our security proof in Appendix E shows that even if an adversarial user does not comply with these algorithms, he can't break Zether's correctness, privacy and over-draft protections.

Setup. The setup algorithm calls $\mathsf{Setup}_{\mathsf{nizk}}$ and $\mathsf{Setup}_{\mathsf{nizk}}$ as subroutines, which are the setup algorithms for the proof system and the signature scheme, respectively. The former setup could depend on the relations for which proofs are constructed. If these subroutines are trustless, then the whole setup is trustless, meaning that its correctness can be verified publicly. In the implementation (Section 7), we use Bulletproofs [BBB+18] and Schnorr signatures [Sch90], both of which have a trustless setup. Zether significantly differs from Zcash [zcaa] in this respect because Zcash has a trusted setup and its security is broken if the setup is subverted.

Setup algorithm is formally described in Figure 1. Apart from setting up the proof system and signature scheme, it initializes account tables acc and pending transfers table $\mathsf{pTransfers}$

(recall that incoming transfers are put into a pending state first), a last roll over epoch table lastRollOver to keep track of the last epochs accounts were updated, a lock table lock to keep track of the addresses to which accounts are locked, a counter table ctr to prevent replay attacks, and a variable b_{total} that tracks the total amount of ZTH held by the contract. The setup also specifies an epoch length E and a maximum amount value MAX.

Zero-knowledge relations. Each transfer and burn transaction in Zether contains a ZK-proof which ensures that the transfer is valid without revealing the reasons why it is valid.

Burn transaction. Let us first consider a burn transaction where a user needs to verifiably decrypt his Zether balance. It can certainly do this by revealing its secret key to the smart contract. However, an adversary can use the secret key to decrypt all previous balances and transactions of the user, thus completely breaking its privacy. So, instead of decrypting in the clear, the user creates a ZK-proof for the following statement:

$$\mathsf{st}_{\mathsf{burn}} : \left\{ (y, C_L, C_R, u, b, g, g_{\mathsf{epoch}}; \mathsf{sk}) : y = g^{\mathsf{sk}} \wedge C_L = g^b C_R^{\mathsf{sk}} \right\} \tag{1}$$

The statement shows that the user knows an sk such that y is indeed the public key corresponding to sk and (C_L, C_R) is a valid encryption of b under y. A simple Σ protocol can be used to prove the statement.

Transfer transaction. Let us now consider a transfer transaction. Suppose a user wants to transfer an amount $b^\star$ from a public key y to a public key $\overline{y}$. Let (C_L, C_R) be the encryption of balance associated with y. The smart contract needs to deduct $b^\star$ from y's balance and add the same amount to $\overline{y}$'s balance, which will be put into a pending state. Since we need to hide $b^\star$ in this process, user will encrypt $b^\star$ under both y and $\overline{y}$ to get (C, D) and $(\overline{C}, \overline{D})$, respectively. Now, it must provide a proof to show that:

1. both ciphertexts are well formed and encrypt the same value $b^\star$;

2. $b^\star$ is a positive value; and,

3. the remaining balance of y, say b', is positive too.

More formally, a user proves the following statement:

$$\mathsf{st}_{\mathsf{ConfTransfer}} : \big\{ (y, \overline{y}, C_L, C_R, C, D, \overline{C}, g; \mathsf{sk}, b^\star, b', r) :$$
$$C = g^{b^\star} y^r \wedge \overline{C} = g^{b^\star} \overline{y}^r \wedge D = g^r \wedge$$
$$C_L/C = g^{b'} (C_R/D)^{\mathsf{sk}} \wedge y = g^{\mathsf{sk}} \wedge$$
$$b^\star \in [0, \mathsf{MAX}] \wedge b' \in [0, \mathsf{MAX}] \big\} \tag{2}$$

Kurosawa [Kur02] first showed that in the ElGamal encryption scheme, randomness can be reused to encrypt to multiple recipients. We use the same idea here to make the zero-knowledge component more efficient: the same random number r is used to encrypt $b^\star$ under both y and $\overline{y}$.

Zether contract. The Zether contract (ZSC) is defined in Figure 5. It consists of five public methods Fund, Burn, Transfer, Lock, Unlock and two additional internal helper methods RollOver, CheckLock. The helper methods are used to modularize the contract's logic. We use Solidity syntax at some places in the description of ZSC, instead of introducing new notation; see Table 1 for the syntax we use and what it means. We now discuss ZSC's methods in detail.

block.number	current block number
msg.sender	sender of the message (current call)
msg.value	number of Wei sent with the message
address.transfer	send given amount of Wei to address
require	check conditions; current call reverts if condition fails

<div align="center">Table 1: Solidity syntax</div>

Rolling over. Pending transfers for an account must be rolled over into the account every epoch, or at least in the epochs the account is used. However, no instruction on a smart contract can execute unless triggered by a transaction. As a result, all public methods of ZSC first call RollOver on the input public key(s).

Given a public key y, RollOver checks if the last roll over was in an older epoch. If yes, then it rolls over the pending transfers pTransfers[y] into acc[y] and resets pending transfers as well as the last roll over epoch.

Check lock. Every transaction to operate on an account is associated with an Ethereum address (returned by msg.sender). If the account is unlocked, then it can be operated from any address. However, if it is locked to a certain address, then it can only be operated from that address. CheckLock is an internal methods to check these two conditions. All the methods call CheckLock before operating on an account.

Locking. Given a public key y, an address addr and a signature σ_{lock}, Lock checks if it is appropriate to operate on the account by calling CheckLock, which will be discussed in more detail shortly, and verifies that σ_{lock} is a valid signature on addr and the current value of counter ctr[y]. It sets lock[y] to be addr and increments the counter, which ensures that this lock transaction cannot be replayed. Unlock method also calls CheckLock first, then sets the pending lock to be $\perp$.

Funding. Anybody can fund an account, even an account that he/she does not own, by simply specifying the public key y and transferring some ETH. The only exception is for locked accounts; they can only be operated from the locking address. (One could have a different rule for funding locked accounts.) Fund converts ETH into ZTH. The ETH gets stored in the smart contract and the ZTH are homomorphically added to y's (pending) balance. If the account does not exist yet, a new one is created. Fund also ensures that the deposit does not exceed the total amount of funds, MAX, that Zether can handle.

Burn. Burn converts ZTH back to ETH. It verifies the proof π_{burn} against st_{burn} (see (1)) to ensure that the sender knows the right private key and is claiming the right amount. It also checks a signature on the transaction data and the current value of counter, which prevents replay attacks. Note that a burn operation does not close an account.

Transfer. Transfer transfers some ZTH from an account to another. The proof π_{transfer} makes

Fund
- INPUTS: public key y
1. $\mathsf{RollOver}(y)$
2. Let $b = \mathsf{msg.value}$
3. require:
   - $b + b_{\mathsf{total}} \leq \mathsf{MAX}$
   - $\mathsf{CheckLock}(y, \mathsf{msg.sender}) = 1$
4. If $\mathsf{acc}[y] = \bot$:
   - Let $H = \mathsf{block.number}$, $e = \lfloor H/\mathsf{E} \rfloor$
   - Set $\mathsf{acc}[y] = (1,1)$
   - Set $\mathsf{pTransfers}[y] = (g^b, 1)$
   - Set $\mathsf{lock}[y] = \bot$
   - Set $\mathsf{lastRollOver}[y] = e$
   - Set $\mathsf{ctr}[y] = 0$

   Else:
   - Set $\mathsf{pTransfers}[y] = \mathsf{pTransfers}[y] \circ (g^b, 1)$
5. Set $b_{\mathsf{total}} = b_{\mathsf{total}} + b$

Transfer
- INPUTS: sender public key y, recipient public key $\overline{y}$, ciphertexts (C, D), $(\overline{C}, D)$ proof π_{Transfer}, signature $\sigma_{\mathsf{transfer}}$
1. $\mathsf{RollOver}(y)$
2. $\mathsf{RollOver}(\overline{y})$
3. Let $(C_L, C_R) = \mathsf{acc}[y]$
4. require:
   - $\mathsf{CheckLock}(y, \mathsf{msg.sender}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(\mathsf{st}_{\mathsf{ConfTransfer}}[y, \overline{y}, C_L, C_R, C, \overline{C}, D], \pi_{\mathsf{transfer}}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(y, (\overline{y}, C, \overline{C}, D, \pi_{\mathsf{transfer}}, \mathsf{ctr}[y]), \sigma_{\mathsf{transfer}}) = 1$
5. Set $\mathsf{acc}[y] = \mathsf{acc}[y] \circ (C^{-1}, D^{-1})$
6. Set $\mathsf{pTransfers}[\overline{y}] = \mathsf{pTransfers}[\overline{y}] \circ (\overline{C}, D)$
7. Set $\mathsf{ctr}[y] = \mathsf{ctr}[y] + 1$

Lock
- INPUTS: public key y, Ethereum address addr, signature σ_{lock}
1. $\mathsf{RollOver}(y)$
2. require:
   - $\mathsf{CheckLock}(y, \mathsf{msg.sender}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(y, (\mathsf{addr}, \mathsf{ctr}[y]), \sigma_{\mathsf{lock}}) = 1$
3. Set $\mathsf{lock}[y] = \mathsf{addr}$
4. Set $\mathsf{ctr}[y] = \mathsf{ctr}[y] + 1$

Burn
- INPUTS: public key y, balance b, proof π_{burn}, signature σ_{burn}
1. $\mathsf{RollOver}(y)$
2. Let $(C_L, C_R) = \mathsf{acc}[y]$
3. require:
   - $\mathsf{CheckLock}(y, \mathsf{msg.sender}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(\mathsf{st}_{\mathsf{burn}}[y, C_L, C_R, b, g], \pi_{\mathsf{burn}}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(y, (b, \pi_{\mathsf{burn}}, \mathsf{ctr}[y]), \sigma_{\mathsf{burn}}) = 1$
4. Set $\mathsf{acc}[y] = \mathsf{acc}[y] \circ (C_L^{-1}, C_R^{-1})$
5. Set $\mathsf{ctr}[y] = \mathsf{ctr}[y] + 1$
6. Set $b_{\mathsf{total}} = b_{\mathsf{total}} - b$
7. Do $\mathsf{msg.sender.transfer}(b)$

Unlock
- INPUTS: public key y
1. $\mathsf{RollOver}(y)$
2. require:
   - $\mathsf{CheckLock}(y, \mathsf{msg.sender}) = 1$
3. Set $\mathsf{lock}[y] = \bot$

Internal Helper Methods

RollOver
- INPUTS: public key y
1. Let $H = \mathsf{block.number}$, $e = \lfloor H/\mathsf{E} \rfloor$
2. If $\mathsf{lastRollOver}[y] < e$:
   - Set $\mathsf{acc}[y] = \mathsf{acc}[y] \circ \mathsf{pTransfers}[y]$
   - Set $\mathsf{pTransfers}[y] = (1, 1)$
   - Set $\mathsf{lastRollOver}[y] = e$

CheckLock
- INPUTS: public key y, Ethereum address addr
- OUTPUT: 1 if account y can be operated by addr; 0 otherwise
1. If $\mathsf{lock}[y] = \bot$ or $\mathsf{lock}[y] = \mathsf{addr}$:
   - Output 1

   Else:
   - Output 0

Figure 2: ZSC: Zether smart contract

sure that the ciphertext has the right form and the sender has enough money (see (2)). Similar to Burn, there is a signature here to prevent replay attacks.

Note that the transferred amount is added to pTransfers of the recipient, not acc. (It will be rolled over into acc in a later epoch.) Thus, outgoing transfers of the recipient in this epoch will not be invalidated.

CreateAddress
- INPUTS: 1^λ
- OUTPUT: $x \in \mathbb{Z}_p, y \in \mathbb{G}$
1. $x \xleftarrow{\$} \mathbb{Z}_p$
2. $y = g^x$

CreateTransferTx
- INPUTS: sender public key y, receiver public key $\overline{y}$, sender private key x, sender balance b_{from}, transfer amount $b^\star$, state st_h of ZSC
- OUTPUT: $\text{tx}_{\text{trans}} = (y, \overline{y}, C, \overline{C}, D, \pi_{\text{transfer}}, \sigma_{\text{transfer}})$
1. Roll over $y, \overline{y}$ in st_h
2. Let $(C_L, C_R) = \text{acc}[y]$
3. $r \xleftarrow{\$} \mathbb{Z}_p$
4. Set $C = g^{b^\star} y^r$
5. Set $\overline{C} = g^{b^\star} \overline{y}^r$
6. Set $D = g^r$
7. Set $w = (x, b^\star, b_{\text{from}}, r)$
8. $\pi_{\text{transfer}} = \text{Prove}(\text{st}_{\text{ConfTransfer}}[y, \overline{y}, C_L, C_R, C, \overline{C}, D, g], w)$
9. $\sigma_{\text{transfer}} = \text{Sign}(x, (\overline{y}, C, \overline{C}, D, \pi_{\text{transfer}}, \text{ctr}[y]))$

CreateBurnTx
- INPUTS: private key x, state st_h of ZSC
- OUTPUT: $\text{tx}_{\text{burn}} = (y, b, \pi_{\text{burn}}, \sigma_{\text{burn}})$
1. Let $b = \text{ReadBalance}(x, \text{st}_h)$
2. $w = (x)$
3. Set $y = g^x$
4. Let $(C_L, C_R) = \text{acc}[y]$
5. $\pi_{\text{burn}} = \text{Prove}(\text{st}'_{\text{burn}}[y, C_L, C_R, b, g], w)$
6. $\sigma_{\text{burn}} = \text{Sign}(x, (b, \pi_{\text{burn}}, \text{ctr}[y]))$

CreateLockTx
- INPUTS: private key x, locking Ethereum address addr, state st_h of ZSC
- OUTPUT: $\text{tx}_{\text{lock}} = (y, \text{addr}, \sigma_{\text{lock}})$
1. Compute $\sigma_{\text{lock}} = \text{Sign}(x, (\text{addr}, \text{ctr}[y]))$
2. Set $y = g^x$

ReadBalance
- INPUTS: private key y, state st_h of ZSC
- OUTPUT: balance b
1. Set $y = g^x$
2. Roll over y in st_h
3. $(C_L, C_R) = \text{acc}[y]$
4. Find b s.t. $C_L / C_R^x = g^b$

Figure 3: User algorithms of Zether. CreateFundTx and CreateUnlockTx are straightforward, so not specified here.

User algorithms. User algorithms specify how users can interact with ZSC. CreateTransferTx and CreateBurnTx first do a roll over of the input public keys to ensure that any pending transfers are rolled over. CreateBurnTx uses ReadBalance to recover the amount of ZTH in the account. Using the private key, ReadBalance finds the right b s.t. $C_L / C_R^x = g^b$. In typical cases, a user would *not* have to try all positive integers one by one to recover b. She will already have a good estimate of b.

Anonymity. Zether can be extended to transfer anonymously. We describe the extension in detail in Appendix D.2. We also discuss some important matters related to the use of Zether in Appendix F.

Proof of security. We prove that Zether satisfies our security requirements in Section E. The proof is actually for the more general, anonymous version of Zether.

7 Implementation & Evaluation

In order to properly evaluate the Zether protocol and show its feasibility we implemented basic Zether as an Ethereum smart contract. The implementation shows that Zether is feasible today and can be run on top of the Ethereum virtual machine. We also discuss several optimizations that we made in order to improve the performance of the contract. Further, we will analyze what small improvements to the EVM would significantly benefit Zether. Some of these improvements have been discussed independently and are already part of the *Ethereum improvement proposal (EIP)* track.

7.1 Solidity Implementation & Optimizations

We describe our Ethereum implementation of the basic Zether contract. The implementation was written in Solidity and makes use of several observations. Ethereum recently introduced precompiled contracts for elliptic-curve operations on the curve BN-128 [bn1a]. These precompiled contracts reduce the cost of executing these operations compared to direct implementations. The reason is that miners can use specialized software, i.e., special cryptography libraries, to run these functions more efficiently. The operations were originally introduced to support pairing-based ZK-SNARKs. Σ-Bullets do not require pairings and the curve BN-128 is not an optimal choice in terms of efficiency or security for Bulletproofs/Σ-Bullets. Nevertheless, we chose to implement Zether using this curve because it is natively supported (precompiled contracts are far cheaper than a Solidity implementation of another curve such as secp256k1 [sec].) As we explain in Section 7.3, this means that we have to rely on the DDH assumption in the $\mathbb{G}_1$ group of BN-128. This assumption is called the external DDH or XDH assumption and is less general than the DDH assumption.

Despite the precompiled contract, a majority of the gas cost lies in the cryptographic operations used, especially curve multiplication. We therefore aimed to reduce the number of exponentiations to an absolute minimum. We did this by implementing the optimizations presented in Section 6.2 of [BBB$^+$18].

We did not implement multi-exponentiation as this would not be beneficial. Multi-exponentiations reduce the number of curve operations but do this by splitting up the exponentiation. Multi-exponentiation algorithms assume that a k-bit exponentiation use k curve operations. This is not the case for Solidity however. The gas cost for an exponentiation is independent of the exponents length and curve additions are relatively overpriced to curve multiplications. A curve multiplication is only 80 times more expensive than a curve addition even if the exponent has 256 bits. Therefore, multi-exponentiation would not lower but increase the gas cost.

In a further optimization, we rolled out the inner product argument and combined all possible exponentiations into a single large statement. Furthermore, we slightly modified the recursive inner product argument such that it terminates at $n = 4$ instead of $n = 1$. This means that instead of sending scalars a and b, the prover sends the two 4 scalar vectors $[a_1, a_2, a_3, a_4]$ and $[b_1, b_2, b_3, b_4]$. By doing this, the prover has to send 6 more elements in $\mathbb{Z}_p$ but on the other hand saves sending 4 Pedersen hashes which are elements in $\mathbb{G}$. Since Solidity does not support point compression, i.e., points in $\mathbb{G}$ are encoded using 64 bytes and scalars using 32 bytes, this small modification therefore saves 64 bytes in space and also reduces the number of curve exponentiations that need to be done. In total for the ConfTransfer transaction the elliptic curve operations for the account state manipulations, the Σ-protocol and the 2 32-bit range proofs use 156 curve additions and 154 curve multiplications.

18

A further optimization concerns the common reference string (CRS). Bulletproofs unlike SNARKs do not use a structured reference string which would require a trusted setup. Nevertheless, Bulletproofs still requires a long linear-sized reference string that the verifier needs to access. While the CRS could be generated on the fly, this would add over 3.9 million gas to the cost of the transaction. Storing the CRS in the blockchain storage also creates high additional cost as loading a 32-byte word costs 200 gas. On the other hand, loading a 32-byte code instruction costs only 3 gas which is why we choose to hard-code the generators into the smart contract. While this makes the contract-generation process more expensive, it is a one-time cost which is amortized over the lifetime of a contract.

7.2   Measurements

We now present several measurements for our implementation of basic Zether. We measure the total gas cost which includes the basic cost for sending a transaction, the storage cost as well as the proof/signature verification. We also present the gas cost in USD using a gas cost price of 2 Gwei per unit of gas [Ethb] and exchange rate of 105 USD per ETH [mar]. At the time of writing, a basic Zether transaction costs about 1.5 USD. We also show that a majority of the cost is produced by elliptic-curve operations by factoring out their gas cost. For a transfer transaction, the elliptic curve operations make up 90% of the total cost. For a fund transaction, the majority of the cost comes from initializing a new account. Adding funds to an existing account is significantly cheaper. Finally, we present the size of the transaction data. Note that this does not include the basic Ethereum transaction data which is roughly 110 bytes.

	Gas Cost	in $	EC Cost	|tx|
Burn	384k	0.080	329k	160 bytes
Fund	260k	0.035	41k	64 bytes
Transfer	7188k	1.51	6455k	1472 bytes
Lock	223k	0.049	83k	128 bytes
Unlock	193k	0.041	83k	96 bytes

Table 2: Gas costs for ZSC methods

7.3   Ethereum Limitations & Future Directions

At the current gas costs, Zether is barely feasible. The cost of a single confidential-only transfer is just below a block's roughly 8 million gas limit [Eth18], i.e., the maximum global gas consumed per block. Ethereum's computation power currently is very limited. A simplified estimate is that at 3 gas units per arithmetic operation, Ethereum currently supports less than 180k operations per second for the whole network. There are several efforts to increase the scalability of Ethereum [BG17, Zam17]. Zether, as a fairly computation-heavy application, would benefit from this increase. There are also multiple more specific and smaller changes that would greatly benefit Zether. The majority of the cost of a transaction comes from the cryptographic operations. Despite heavily optimizing them, they make up for almost 90% of the cost. These operations seem overpriced when compared to operations like hashing. This discrepancy has been noted and discussed independently [bn1b]. There currently exists an EIP to reduce the gas cost of elliptic curve multiplications by a factor of 6.66 and additions by a factor of 3.33 [bn1b]. A further EIP reduces the cost of calling a precompiled contract [pre] which would reduce the cost for each cryptographic operation by another 700 units of

gas. If both of these were implemented, the cost of a Zether transfer would reduce to roughly 1.7 million gas (0.36 USD). At that point, optimizations on the non-cryptographic part of the contract could probably further reduce the cost.

There are further changes that Ethereum could make that would benefit Zether. One of them would be supporting elliptic-curve operations for more efficient curves like secp256k1 [sec] or Curve25519-ristretto [cur]. Another would be supporting multi-exponentiation techniques that can reduce the number of cryptographic operations needed to verify the range proofs [Pip80].

A simple but significant optimization that can be implemented without changing Ethereum applies to the proof verification: Bulletproofs can be batch verified. This means that verifying k proofs is significantly faster than verifying a single proof. If transactions were collected by some service provider, combined to a single transaction and then sent to the Zether contract, it would significantly reduce the verification cost per proof. However, all transactions in a batch must be valid because a single invalid transaction will cause the whole verification to fail. Batch verification requires randomness but this randomness can either be sampled from the block header [BCG15] or generated from a hash of the proofs.

8 Applications using Zether

Zether's capability to lock funds to other smart contracts can make several common applications more private. Before going into them, it is worth noting that the Zether contract will never transfer funds without first checking an appropriate burn or transfer proof, even if the request comes from another smart contract whose rules do not permit illegal transfers. This design decision ensures that the security of Zether only depends on itself and not on any outside smart contract. Even a maliciously written or insecure smart contract cannot cause Zether to misbehave.

8.1 Sealed-bid Auctions

Auctions are used on Ethereum to sell tokens, resources, etc. [Tok]. Ethereum Name Service (ENS) [ENSa], for example, resolves human-readable names into machine-readable identifiers, such as Ethereum addresses and IPFS content hashes, and other identifiers. ENS allocates names through a Vickrey auction, a type of sealed-bid auction where the highest bidder wins but only pays the value of the second highest bid. A total of 782,521 of such auctions have been initiated as of early February 2019 [Ethc].

ENS auctions consist of three stages. First, a user initiates an auction on a name by bidding on the name. Other people then get three days to place their own bids. Second, everyone reveals their bids over a period of two days. If a bid is not revealed, then the entire amount is forfeited. In the third stage, the highest bidder is awarded the name but only pays the value of the second highest bid.

In the bidding phase, a bidder is supposed to make two API calls. The first call creates a *sealed* bid by hashing the bid value with a bidder generated secret. The second call submits the committed bid along with a certain amount of ether. ENS suggests that a bidder should deposit more ether than the bid value to disguise the true value of the latter.

Drawbacks. One can easily see why this mechanism does not provide good bid privacy. First, the ether deposited reveals an upper bound on the bid value. Second, the bidder may not want to deposit a very large amount of ether (assuming she has it) because, in the best

case, the amount remains locked till the end of the bidding phase, and, in the worst case, till the end of the whole bidding process.

Using Zether. Zether provides a simple way to deal with these problems.

- *Bidding phase*: To bid b ETH in the bidding phase, a bidder, say B, can transfer b ZTH from her primary Zether account into a new account, and then lock the latter to the auction contract, call it AUC. Thus, the bid value is completely hidden without B having to deposit any extra money to obfuscate it.

- *Reveal phase*: B reveals her bid by sending b and a burn proof to AUC. AUC can check the proof and verify that b is in fact the right value. ZSC may also export the proof checking functionality as an API call. Now, there are three possibilities:

  1. If a bid is not revealed in this phase or the revealed value is incorrect, then AUC does not do anything. Bidder's account remains locked. Thus, bidders have a strong incentive to reveal their bid regardless of the outcome.
  2. If a new revealed bid is lower, then AUC can simply unlock the bidder's account.
  3. If a new revealed bid is highest so far, then AUC unlocks the previous highest bid and stores only its amount.

- *Final phase*: For the winning bid, AUC must only keep the next highest bid, say $b^\star$, and release the difference back to the bidder. This can be done through a Transfer transaction. However, since all amounts are public anyway, AUC can also simply burn the whole amount and retain one part (the winner's payment) while refunding the rest to the winner. This prevents AUC from having to create an expensive Transfer transaction and it can utilize the burn proof which was submitted with the bid. For simplicity, ZSC can provide a functionality to split up the burn refund directly.

8.2 Payment Channels

Payment channels are a popular way to avoid the fee and delay associated with on-chain transactions. Two or more parties can set-up a payment channel amongst them by committing to some money up front. They can then send messages to each other offline to keep track of the money they owe each other.

The first payment channels were proposed for Bitcoin [Spi13, DW15, PD16]. Simpler constructions have been developed for Ethereum [Rai, BKM17]. We will consider a very simple construction here given by Di Ferrante [Fer17] to illustrate some of the confidentiality issues surrounding payment channels and how Zether can help alleviate them. The ideas described below would extend easily to more complex channels.

Suppose Bob wants to make small payments to Alice every time she *tweets* for him. Bob can open a payment channel with Alice with the help of a smart contract, say PC. Bob deposits a certain amount of ETH with PC and sets an expiration date. Whenever Alice tweets, Bob signs the *total* amount of money he owes to Alice so far, and sends the signature to Alice. At any time, Alice can cash out by sending the latest signature to the contract. PC will pay Alice accordingly and send the remaining balance to Bob. (We have omitted several details here because they are not important for the rest of the discussion; please refer to original write-up [Fer17] for them.)

Drawbacks. The amount of ETH Bob deposits with PC is visible to everyone. Indeed, even Alice does not need to know this amount as long as she is convinced that PC holds enough

money to pay her off. Further, when Alice cashes out, everyone can see how much she charges per tweet (since the number of tweets is also public).

Using Zether. Zether can easily be used to create a confidential payment channel. Instead of depositing ETH directly with PC, Bob will lock his Zether account to PC (or, as in the previous example, transfer some money to a new Zether account and lock that to PC). Whenever Alice tweets, Bob would send a Zether transfer transaction to Alice of the amount that she expects, say b. Alice will check the validity of the transaction and that it indeed transfers b to her.

When Alice wants to cash out, she would send the latest transaction to PC, who will pass it on ZSC. ZSC will process the transfer because it is locked to PC. A transfer also unlocks Bob's account. If Alice never cashes out, PC will just unlock Bob's account after an expiration date. As a result, the payment channel between Alice and Bob remains confidential to others. Furthermore, Alice does not learn the total amount Bob locked into the payment channel.

Using a simple signed counter the proposal can be trivially extended to bi-directional channels which in turn can be used to build payment channel networks [PD16, DEFM17]. With a slightly more involved design we can also enable adding more funds to a channel. Suppose Bob wants to add more ZTH to his account. He prepares a transaction for PC and then lets Alice sign the transaction. He then forwards the transaction and the signature to PC which checks both and, if valid, submits the transaction to ZSC. Note that Alice needs to sign the transaction because it might invalidate a previous payment channel transfer. Alice will require that Bob give him a new valid Zether transaction with respect to Bob's new balance.

Green and Miers [GM17] show how to build anonymous payment channels. Their design is more involved but provides strong privacy against an intermediary payment channel hub. It requires an underlying private currency and as such is compatible with Zether.

8.3 Stake Voting

Any voting process must be as open and transparent as possible. A blockchain based solution can provide such benefits but voter privacy becomes a concern. McCorry et al. [MSH17] proposed a decentralized mechanism for boardroom voting, called the Open Vote Network (OVN), which provides voter privacy. They implement OVN as a Ethereum smart contract.

The Election is carried out in several stages. In the voting stage, a participant publishes a special encryption of their vote v_i and a ZK-proof that v_i is binary. In the tally stage, the votes can be summed up to compute the final tally. The encryption scheme is designed such that that only the final tally can be computed—individual votes remain private.

A natural question is whether votes can carry weights, instead of just being zero or one. For instance, can participants cast votes of size proportional to their assets, without revealing the value of those assets? Zether provides a simple way to achieve this. In the sign-up phase of the election, participants will lock their Zether account to the voting smart contract. Then, during the voting stage, when a participant casts a vote v_i (in an encrypted form), he/she will provide a ZK-proof that v_i is equal to the (encrypted) amount in his/her locked account.

8.4 Privacy-preserving Proof-of-Stake

Proof-of-stake (PoS) is a consensus mechanism for blockchains, where a participant is elected as a leader with a probability that is proportional to the amount of coins that the participant *stakes* in the election. There are several PoS protocols [KRDO17, DGKR18, CGMV18] which all roughly follow the following simplified design: Users *stake* a number of coins and then a

random beacon [Rab83, BCG15, BBBF18] is used to select one or a subset of them as leaders. Ethereum is planning to switch to a PoS-based consensus model in the future [BG17]. All current PoS proposals are for non-confidential currencies and require the user to reveal its stake.

We propose a mechanism to make the PoS election process confidential using Zether, i.e., users do not have to reveal their stake in order to participate in the election. Similar ideas could be used to implement PoS for other confidential currencies such as ZCash [BCG+14] or Monero [vS13]. The general idea is that users encrypt an initial lottery ticket t under their public key and stake an encrypted Zether balance b under the same key. Then the random beacon value is used to derive a lottery drawing v. If v falls between t and $t + b$ then the user wins the lottery, i.e. the PoS election. The user can use a range proof to prove that v is in fact between t and $t + b$ without revealing t or b. This range proof is similar to the one used in basic Zether's Transfer.

It is further possible to adjust the winning probability by scaling the range appropriately. Let p denote the desired probability of winning for a single unit of stake. Let q be the size of the ring in which the ElGamal encrypted values lie. For simplicity assume that $p \cdot q$ is an integer. A users wins if v falls in between t and $t + b \cdot p \cdot q$. This happens with probability $b \cdot p$.

The hidden lottery approach does not guarantee that at least one user wins. In order to guarantee this, we can have a series of lottery drawings by utilizing a hash function $\mathcal{H}$ that is modeled as a random oracle. For beacon v, we define $v_i = \mathcal{H}(v||i)$ as a sequence of lottery drawings. The user who can demonstrate a winning ticket on the lowest drawing wins. We can also ensure that exactly 1 participant wins. First, we ensure that the lottery drawings are uncorrelated by appending the serialized public key pk when computing the lottery drawings, i.e. $v_{i,\mathsf{pk}} = \mathcal{H}(v||i||\mathsf{pk})$. Even a malicious user will not be able to correlate lottery tickets for distinct public keys, if $\mathcal{H}$ is in fact a random function. Then we use run-off lottery elections between the previous winners until a single winner remains.

The proposed scheme has the severe flaw that after multiple drawings an adversary will be estimate a user's stake by simply observing the user's probability of winning. This can be circumvented by having a user *prove* in zero-knowledge that she knows a winning ticket instead of revealing it. We can use a similar ZK-proof as the anonymous Zether transfer. The user proves that she *knows* a private key which won the lottery instead of revealing her stake. We can use a similar nonce protection as for the anonymous transfer to prevent that a user claims the same winning lottery ticket twice.

The proposed scheme requires a formal analysis and further investigation which we leave for future work.

9   Related Work

Confidential transactions for Bitcoin were first proposed by Maxwell [Max15]. He uses Pedersen commitments [Ped92] and OR-proofs to build a payment mechanism where the transaction amounts are hidden, yet it can be verified that the sum of outputs of a transaction is no more than the sum of inputs. Monero goes a step further and uses a special type of signature scheme to hide the origins and destinations of transactions among a set of UTXOs chosen by the sender (anonymity set) [Noe15].   The size of the signature, however, increases linearly with the size of the anonymity set.   Thus, the anonymity properties of the extension to Zether is similar to that Monero. (The two are in different models though.)

ZCash [zcaa], based on Zerocash [BCG+14], provides anonymity at a sublinear cost using a

more sophisticated ZK-proof system called zkSNARKs [GGPR13]. Senders and recipients are hidden among the group of people who use shielded addresses. Both Monero and ZCash utilize a set of nullifiers which grows linear in the number of transactions. The downside of using SNARKs is that a large common reference string (CRS) needs to be generated beforehand in a way that no one knows the trapdoor, which is a challenging task [pow]. Spenders needs to download the CRS and generate proofs for a large circuit, which is very time consuming [BCG+14, zcab].

There are several other approaches to make blockchain transactions anonymous. CoinJoin [Max13] provides a way for a set of users to jointly create a Bitcoin transaction. (MimbleWimble/Grin [Poe16, gri] combines confidential transactions [Max15] and CoinJoin along with techniques to aggregate transactions non-interactively.) CoinShuffle [RMK14] and Mixcoin [BNM+14] are mixing protocols for Bitcoin. TumbleBit [HAB+17] uses an untrusted intermediary, called a tumbler, to make transactions unlinkable. Möbius [MM18] replaces the tumbler with an Ethereum smart contract. Zether's approach to anonymity is different from the above: it does not rely on *active* participation of other users. Zether users can choose their own anonymity set like Monero. On the other hand, if a mixing service is used actively, it may provide better anonymity.[3]

Hawk [KMS+16] is a framework for building arbitrary smart contracts in a privacy-preserving way. In particular, it can completely hide the bid values in an auction. This generality, however, comes at a significant cost. In Hawk, the private portion of a contract is converted into a circuit. A manager, who is entrusted with the private inputs of participants, generates a zkSNARK proof on the circuit [BSCTV14] to show that it has been executed correctly. Apart from the fact that SNARKs rely on trusted setup, the reference string is also circuit-dependent, so a different string needs to be generated for every contract. Moreover, the circuit model puts a bound on the number of users who can participate.

As a result, though Hawk is quite powerful and could provide better privacy, it is not fully decentralized and would be too expensive to use for simple contracts. Another general purpose framework, Ekiden [CZK+18], addresses both the performance and confidentiality problems with smart contract platforms, but relies on trusted execution environments like Intel SGX, so are not fully decentralized either.

RSCoin, Solidus, zkLedger, etc. [DM16, CZJ+17, NVV18] operate in a model that falls somewhere between a fully decentralized setting like that of Bitcoin/Ethereum and a centralized setting like that of modern financial systems. In this model, the banks regulate the monetary supply but use a blockchain to transact. There is some similarity between the techniques used here and zkLedger's, where every bank has an account. A sending bank A in zkLedger creates several commitments to send some money x to a receiving bank B. The commitment corresponding to A is to $-x$, to B is to x, and all other commitments are to zero. Then there are proofs to show that the commitments are well-formed and A has more than x amount of money. While we use similar ideas in our protocol, Zether needs to deal with many more issues like front-running, replay, compatibility, etc. that come with building a smart contract on an open platform.

Concurrent work. Zexe [BCG+18] is a recent proposal for a private scripting language for Zerocash-style currencies [BCG+14]. It provides similar functionality to Bitcoin script while hiding the inputs to the script and the script itself. It, however, does not support stateful computations in the way a smart contract does.

---

[3]One can potentially use Zether in combination with Möbius on Ethereum to get the best of both worlds. We leave this as an interesting open question.

Quisquis [FMMO18] is a new anonymity system designed to address some problems with crypto-currencies like Monero and Zcash (e.g., the set of unspent outputs keep growing). Their model is an interesting hybrid of UTXO and account. While the basic unit is an account (consisting of a public key and a commitment), they are only of one-time use: old accounts are destroyed and new accounts created in a transaction.

Though Quisquis provides a new approach to anonymity, it suffers from front-running attacks (public keys in an anonymity set may get updated just before the transaction is processed) and puts additional burden on clients (they have to go through the list of all updated keys to find out which one belongs to them). More importantly, Quisquis is a standalone crypto-currency while our goal is to build a system that can be deployed on any smart contract platform, and can be used by other smart contracts to achieve more privacy. As a result, Zether faces different technical issues and has a different design.

References

[AABN02]   Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In Lars R. Knudsen, editor, *EURO-CRYPT 2002*, volume 2332 of *LNCS*, pages 418–433. Springer, April / May 2002.

[BBB+18]   Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy*, pages 315–334. IEEE Computer Society Press, May 2018.

[BBBF18]   Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 757–788. Springer, August 2018.

[BCC+15]   Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit. Short accountable ring signatures based on DDH. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *ESORICS 2015, Part I*, volume 9326 of *LNCS*, pages 243–265. Springer, September 2015.

[BCC+16]   Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 327–357. Springer, May 2016.

[BCG+14]   Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. IEEE Computer Society Press, May 2014.

[BCG15]   Joseph Bonneau, Jeremy Clark, and Steven Goldfeder. On bitcoin as a public randomness source. Cryptology ePrint Archive, Report 2015/1015, 2015. `http://eprint.iacr.org/2015/1015`.

[BCG+18]   Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu. Zexe: Enabling decentralized private computation. Cryptology ePrint Archive, Report 2018/962, 2018. `https://eprint.iacr.org/2018/962`.

[BCS16]   Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. Interactive oracle proofs. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 31–60. Springer, October / November 2016.

[BG17]   Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. *CoRR*, abs/1710.09437, 2017.

[BKM17]   Iddo Bentov, Ranjit Kumaresan, and Andrew Miller. Instantaneous decentralized poker. Cryptology ePrint Archive, Report 2017/875, 2017. `http://eprint.iacr.org/2017/875`.

[bn1a]   Precompiled contracts for addition and scalar multiplication on the elliptic curve alt bn128. `https://eips.ethereum.org/EIPS/eip-196`.

[bn1b]   Reduce alt bn128 precompile gas costs. `https://eips.ethereum.org/EIPS/eip-1108`.

[BNM+14]   Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. Mixcoin: Anonymity for bitcoin with accountable mixes. In Nicolas Christin and Reihaneh Safavi-Naini, editors, *FC 2014*, volume 8437 of *LNCS*, pages 486–504. Springer, March 2014.

[BS18]   Dan Boneh and Victor Shoup. *A graduate course in applied cryptography*. Cambridge, 2018.

[BSCTV14]   Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a von neumann architecture. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, pages 781–796, Berkeley, CA, USA, 2014. USENIX Association.

[But15]   Vitalik Buterin. On abstraction. `https://blog.ethereum.org/2015/07/05/on-abstraction`, 2015.

[But16]   Vitalik Buterin. Thoughts on UTXOs. `https://medium.com/@ConsenSys/thoughts-on-utxo-by-vitalik-buterin-2bb782c67e53`, 2016.

[CD98]   Ronald Cramer and Ivan Damgård. Zero-knowledge proofs for finite field arithmetic; or: Can zero-knowledge be for free? In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 424–441. Springer, August 1998.

[CGMV18]   Jing Chen, Sergey Gorbunov, Silvio Micali, and Georgios Vlachos. ALGORAND AGREEMENT: Super fast and partition resilient byzantine agreement. Cryptology ePrint Archive, Report 2018/377, 2018. `https://eprint.iacr.org/2018/377`.

[CGS97]   Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 103–118. Springer, May 1997.

[cha]   CHAINALYSIS. https://www.chainalysis.com.

[CL02]   Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and applica-
            tion to efficient revocation of anonymous credentials. In Moti Yung, editor,
            CRYPTO 2002, volume 2442 of *LNCS*, pages 61–76. Springer, August 2002.

[cur]   Curve25519-ristretto. https://ristretto.group/.

[CZJ⁺17]   Ethan Cecchetti, Fan Zhang, Yan Ji, Ahmed E. Kosba, Ari Juels, and Elaine Shi.
            Solidus: Confidential distributed ledger transactions via PVORM. In Bhavani M.
            Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS
            17*, pages 701–717. ACM Press, October / November 2017.

[CZK⁺18]   Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah M.
            Johnson, Ari Juels, Andrew Miller, and Dawn Song. Ekiden: A platform for
            confidentiality-preserving, trustworthy, and performant smart contract execution.
            CoRR, abs/1804.05141, 2018.

[Dåm]   Ivan Dåmgard. On sigma protocols. https://www.cs.au.dk/~ivan/Sigma.pdf.

[DEFM17]   Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. PE-
            RUN: Virtual payment channels over cryptographic currencies. Cryptology ePrint
            Archive, Report 2017/635, 2017. http://eprint.iacr.org/2017/635.

[DFKP13]   George Danezis, Cedric Fournet, Markulf Kohlweiss, and Bryan Parno. Pinocchio
            coin: Building zerocoin from a succinct pairing-based proof system. In *Proceed-
            ings of the First ACM Workshop on Language Support for Privacy-enhancing
            Technologies*, PETShop '13, 2013.

[DGKR18]   Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros
            praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In
            Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*,
            volume 10821 of *LNCS*, pages 66–98. Springer, April / May 2018.

[DM16]   George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies. In
            NDSS 2016. The Internet Society, February 2016.

[DW15]   Christian Decker and Roger Wattenhofer. A fast and scalable payment network
            with bitcoin duplex micropayment channels. In Andrzej Pelc and Alexander A.
            Schwarzmann, editors, *Stabilization, Safety, and Security of Distributed Systems*,
            pages 3–18. Springer International Publishing, 2015.

[ell]   ELLIPTIC. https://www.elliptic.co.

[ENSa]   Ethereum Name Service. https://ens.domains.

[ENSb]   ENS   Docs   –   Register   a   name   with   the   auction   regis-
            trar.   https://docs.ens.domains/en/latest/userguide.html#
            registering-a-name-with-the-auction-registrar.

[EOS]   EOS.io — Blockchain software architecture. https://www.eos.io.

[etha]   Ethereum Project: Blockchain App Platform. https://www.ethereum.org/.

[Ethb]   Ethereum Gasstation. `https://ethgasstation.info/calculatorTxV.php`.

[Ethc]   Etherscan – Ether Name Sservice. `https://etherscan.io/ens`.

[Eth18]   Ethereum network status. `https://ethstats.net/`, 2018.

[Eya15]   Ittay Eyal. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy*, pages 89–103. IEEE Computer Society Press, May 2015.

[Fer17]   Matthew Di Ferrante. Ethereum Payment Channel in 50 Lines of Code, 2017. `https://medium.com/@matthewdif/ethereum-payment-channel-in-50-lines-of-code-a94fad2704bc`.

[FMMO18]   Prastudy Fauzi, Sarah Meiklejohn, Rebekah Mercer, and Claudio Orlandi. Quisquis: A new design for anonymous cryptocurrencies. Cryptology ePrint Archive, Report 2018/990, 2018. `https://eprint.iacr.org/2018/990`.

[FS87]   Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, August 1987.

[GGPR13]   Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645. Springer, May 2013.

[GK15]   Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 253–280. Springer, April 2015.

[GM17]   Matthew Green and Ian Miers. Bolt: Anonymous payment channels for decentralized currencies. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 17*, pages 473–489. ACM Press, October / November 2017.

[gri]   Grin. `https://grin-tech.org/`.

[HAB+17]   Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg. TumbleBit: An untrusted bitcoin-compatible anonymous payment hub. In *NDSS 2017*. The Internet Society, February / March 2017.

[KFTS17]   Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A traceability analysis of monero's blockchain. In Simon N. Foley, Dieter Gollmann, and Einar Snekkenes, editors, *ESORICS 2017, Part II*, volume 10493 of *LNCS*, pages 153–173. Springer, September 2017.

[KMS+16]   Ahmed E. Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy*, pages 839–858. IEEE Computer Society Press, May 2016.

[KRDO17]   Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 357–388. Springer, August 2017.

[Kur02]   Kaoru Kurosawa. Multi-recipient public-key encryption with shortened ciphertext. In David Naccache and Pascal Paillier, editors, *PKC 2002*, volume 2274 of *LNCS*, pages 48–63. Springer, February 2002.

[KYMM18]   George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. An Empirical Analysis of Anonymity in Zcash. In *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018.*, pages 463–477, 2018.

[LCO+16]   Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 254–269, New York, NY, USA, 2016. ACM.

[mar]   Total Market Capitalization. `https://coinmarketcap.com/charts`.

[Max13]   Greg Maxwell. Coinjoin: Bitcoin privacy for the real world, 2013. `https://bitcointalk.org/?topic=279249`.

[Max15]   Greg Maxwell. Confidential transactions, 2015. `https://people.xiph.org/~greg/confidential_values.txt`.

[Maz15]   David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.

[MGGR13]   Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed E-cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy*, pages 397–411. IEEE Computer Society Press, May 2013.

[MM18]   Sarah Meiklejohn and Rebekah Mercer. Möbius: Trustless tumbling for transaction privacy. *PoPETs*, 2018(2):105–121, 2018.

[MPJ+13]   Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA, 2013. ACM.

[MSH17]   Patrick McCorry, Siamak F. Shahandashti, and Feng Hao. A smart contract for boardroom voting with maximum voter privacy. In Aggelos Kiayias, editor, *FC 2017*, volume 10322 of *LNCS*, pages 357–375. Springer, April 2017.

[MSH+18]   Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin. An empirical analysis of traceability in the monero blockchain. *PoPETs*, 2018(3):143–163, 2018.

[NMT16]   Shen Noether, Adam Mackenzie, and Monero Core Team. Ring confidential transactions. https://lab.getmonero.org/pubs/MRL-0005.pdf, 2016.

[Noe15]   Shen Noether. Ring signature confidential transactions for monero. Cryptology ePrint Archive, Report 2015/1098, 2015. http://eprint.iacr.org/2015/1098.

[NVV18]   Neha Narula, Willy Vasquez, and Madars Virza. zkledger: Privacy-preserving auditing for distributed ledgers. In *15th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2018, Renton, WA, USA, April 9-11, 2018*, pages 65–80, 2018.

[PD16]   Joseph Poon and Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 2016. https://lightning.network/lightning-network-paper.pdf.

[Ped92]   Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '91, pages 129–140, London, UK, UK, 1992. Springer-Verlag.

[Pip80]   Nicholas Pippenger. On the evaluation of powers and monomials. *SIAM Journal on Computing*, 9(2):230–250, 1980.

[Poe16]   Andrew Poelstra. Mimblewimble, 2016. https://scalingbitcoin.org/papers/mimblewimble.pdf.

[pow]   Announcing the world's largest multi-party computation ceremony. https://www.zfnd.org/blog/powers-of-tau/.

[pre]   PRECOMPILED CALL opcode (Remove CALL costs for precompiled contracts). https://eips.ethereum.org/EIPS/eip-1109.

[Que17]   Jeffrey Quesnelle. On the linkability of Zcash transactions. *CoRR*, abs/1712.01210, 2017.

[Rab83]   Michael O Rabin. Transaction protection by beacons. *Journal of Computer and System Sciences*, 27(2):256–267, 1983.

[Rai]   The Raiden Network. https://raiden.network.

[Rip]   Ripple - One Frictionless Experience To Send Money Globally. https://www.ripple.com.

[RMK14]   Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. CoinShuffle: Practical decentralized coin mixing for bitcoin. In Miroslaw Kutylowski and Jaideep Vaidya, editors, *ESORICS 2014, Part II*, volume 8713 of *LNCS*, pages 345–364. Springer, September 2014.

[RS13]   Dorit Ron and Adi Shamir. Quantitative analysis of the full Bitcoin transaction graph. In Ahmad-Reza Sadeghi, editor, *FC 2013*, volume 7859 of *LNCS*, pages 6–24. Springer, April 2013.

[Rub18]   Jeremy Rubin. The collapse of ETH is inevitable. https://techcrunch.com/2018/09/02/the-collapse-of-eth-is-inevitable, 2018.

[Sch90]   Claus-Peter Schnorr. Efficient identification and signatures for smart cards (abstract) (rump session). In Jean-Jacques Quisquater and Joos Vandewalle, editors, *EUROCRYPT'89*, volume 434 of *LNCS*, pages 688–689. Springer, April 1990.

[sec]   Secp256k1. `https://en.bitcoin.it/wiki/Secp256k1`.

[Seq]   Sequence. `https://chain.com/sequence`.

[Sola]   Solidity webpage. `https://solidity.readthedocs.io`.

[solb]   Solidity by Example. `https://solidity.readthedocs.io/en/v0.4.24/solidity-by-example.html`.

[Spi13]   Jeremy Spilman. Anti DoS for tx replacement, 2013. `https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002433.html`.

[Tok]   Analyzing Token Sale Models. `https://vitalik.ca/general/2017/06/09/sales.html`.

[Tor]   Tor Project. `https://www.torproject.org`.

[vS13]   Nicolas van Saberhagen. CryptoNote v 2.0, 2013. `https://cryptonote.org/whitepaper.pdf`.

[Woo]   Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger. `https://gavwood.com/paper.pdf`.

[Zam17]   Vlad Zamfir. Casper the friendly ghost: A correct by construction blockchain consensus protocol. `https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf`, 2017.

[zcaa]   Zcash: Privacy-protecting digital currency. `https://z.cash/`.

[zcab]   zcash Documentation. `https://media.readthedocs.org/pdf/zcash/english-docs/zcash.pdf`.

A UTXO on a Contract

One may wonder why one of the existing confidential payment mechanisms developed in the UTXO model cannot be implemented as an Ethereum smart contract. While such a strategy may help us save the effort involved in designing a new mechanism, there are several key advantages in building a confidential payment mechanism in the account-based model rather than the UTXO model:

- *Storage.* Storage on the Ethereum blockchain is quite expensive (for good reasons) and should be minimized as much as possible. For example, storing only 256 bits of information costs roughly 20,000 gas units (see Section 2 for the definition of gas), whereas sending it costs only 2,176 gas units [Woo]. If a UTXO-based model is implemented, then all unspent transactions need to be stored on a smart contract. Moreover, for all UTXO-based currencies that provide cryptographic anonymity [BCG⁺14, Noe15], all *spent* transactions have to be stored as well. This makes the smart contract expensive to use.

- *Confidentiality.* Accounts provide a natural *mixing* property. A new transaction in the account-based model draws from the total available balance, whereas the UTXOs used to create a new transaction in the Bitcoin model could reveal a lot of information about the new transaction, even if all the amounts are cryptographically hidden. For example, if a UTXO (even encrypted) coming from a user's employer is used to create a new transaction, then the user is likely going to spend a significant amount of money. On the other hand, though UTXOs could potentially provide better anonymity, users can often be de-anonymized in practice [MPJ+13, RS13, cha, ell].

- *Interoperability with smart contracts.* An account-based privacy-preserving mechanism can easily inter-operate with smart contracts, which typically maintain accounts for their users and for the contract itself. For example, a private account can be used to fund an account on the smart contract, or be tied to a payment channel smart contract [Rai, BKM17]. Funds can be added to the channel by simply adding funds to the private account.

- *Adoption.* Four out of the six most valuable cryptocurrencies (as of late 2018) use an account-based model (Ethereum, Ripple [Rip], EOS [EOS], Stellar [Maz15]). An account-based privacy mechanism can be used to introduce private payments to these platforms.

- *Simplicity for users.* If we provide privacy in the account-based model, then it encourages users to have a small number of accounts, making account management simpler. This also makes the system more efficient overall.

B   Correctness

To formally state the correctness property, we define what it means for a transaction to be generated honestly and the notion of an ideal state.

Honestly-generated transactions. Let $\mathsf{TX} = (\mathsf{TX}_1, \mathsf{TX}_2, \ldots, \mathsf{TX}_m)$ be a group of transactions such that for every $i \in [m]$, $\mathsf{TX}_i = (\mathsf{tx}_{i,1}, \mathsf{tx}_{i,2}, \ldots)$ is a sequence of transactions which are processed in that order into the block at height h_i ($h_1 < h_2 < \ldots < h_m$). Define the k-th transaction in TX to be the k-th transaction in the sequence $(\mathsf{tx}_{1,1}, \mathsf{tx}_{1,2}, \ldots, \mathsf{tx}_{2,1}, \mathsf{tx}_{2,2}, \ldots, \ldots, \mathsf{tx}_{m,1}, \mathsf{tx}_{m,2}, \ldots)$. We say that these transactions were generated honestly if all of the following are true:

- All secret key, address pairs are generated through the CreateAddress algorithm.

- For all i, j, $\mathsf{tx}_{i,j}$ is generated by running one of the five user algorithms for generating transactions.

- For any $\mathsf{TX}_{i_1}, \mathsf{TX}_{i_2}, \ldots$ s.t. $h_{i_1}, h_{i_2}, \ldots$ are in the same epoch, and any pk, TX_i contains at most one transfer or burn transaction (not one of each) initiated from pk. (This restriction is only for the anonymous version.)

- For any $\mathsf{tx}_{i,j}$, if h_i is in epoch e then a state after the last block of epoch $e - 1$ was used to generate $\mathsf{tx}_{i,j}$ (if a state is needed at all).

The last point above implies that even if there is some delay in processing the transaction, it is no more than the epoch length. In other words, all transactions generated for a certain epoch are assumed to be processed in the same epoch.

For a block height h, let $\mathsf{last}(h)$ denote the height of the last block in the previous epoch, i.e. $\mathsf{last}(h) = \lfloor h/\mathsf{E} \rfloor \cdot \mathsf{E} - 1$, and $\mathsf{next}(h)$ denote the height of the first block in the next epoch, i.e. $\mathsf{next}(h) = \lceil (h+1)/\mathsf{E} \rceil \cdot \mathsf{E}$.

Ideal state. The ideal state IdSt consists of two tables Bal and Lk indexed by addresses. For a public key pk, Bal[pk] gives the balance in pk and Lk[pk] gives the locking Ethereum address (or $\perp$ if pk is not locked). Initially, Bal[pk] and Lk[pk] are set to 0 and $\perp$, respectively, for all pk.[4] These tables are updated as each new transaction is processed. We use Bal_h and Lk_h to denote the state of these tables when all the transactions included in blocks $0, 1, \ldots, h$ have been processed.

Ideal state for a set of transactions TX is defined recursively. Let okToOperate be a function that given a public key pk and an Ethereum address addr, returns 1 iff Lk[pk] is addr or $\perp$. (In either case, addr is allowed to operate on the account.) Let IdSt_k denote the ideal state after the first k transactions have been processed. IdSt_0, ideal state at the beginning, is set to be the initial state of Bal and Lk tables. IdSt_k is defined based on IdSt_{k-1} and the kth transaction as follows. If the kth transaction $\mathsf{tx}_{i,j}$ is:

- $\mathsf{tx}_{\mathsf{fund}} \leftarrow \mathsf{CreateFundTx}(\mathsf{pk}, \mathsf{amt})$: if the sum of all balances and amt is at most MAX, and $\mathsf{okToOperate}(\mathsf{pk}, \mathsf{tx}_{\mathsf{fund}}.\mathsf{addr}) = 1$, then Bal[pk] is incremented by amt.

- $\mathsf{tx}_{\mathsf{trans}} \leftarrow \mathsf{CreateTransferTx}(\mathsf{sk}_{\mathsf{from}}, \mathsf{pk}_{\mathsf{to}}, \mathsf{AnonSet}, \mathsf{amt}, \mathsf{st}_{\mathsf{last}(h_i)})$: if

  - for every $\mathsf{pk} \in \mathsf{AnonSet}$, $\mathsf{okToOperate}(\mathsf{pk}, \mathsf{tx}_{\mathsf{trans}}.\mathsf{addr}) = 1$, and
  - $\mathsf{Bal}_{\mathsf{last}(h_i)}[\mathsf{pkOf}(\mathsf{sk}_{\mathsf{from}})] \geq \mathsf{amt}$,

  then $\mathsf{Bal}[\mathsf{pkOf}(\mathsf{sk}_{\mathsf{from}})]$ is decremented by amt and $\mathsf{Bal}[\mathsf{pk}_{\mathsf{to}}]$ is incremented by amt.

- $\mathsf{tx}_{\mathsf{lock}} \leftarrow \mathsf{CreateLockTx}(\mathsf{sk}, \mathsf{addr})$: if okToOperate $(\mathsf{pk}, \mathsf{tx}_{\mathsf{lock}}.\mathsf{addr}) = 1$ then $\mathsf{Lk}_{\mathsf{next}(h)}[\mathsf{pk}] = \mathsf{addr}$.

- $\mathsf{tx}_{\mathsf{unlock}} \leftarrow \mathsf{CreateUnlockTx}(\mathsf{pk})$: if okToOperate $(\mathsf{pk}, \mathsf{tx}_{\mathsf{unlock}}.\mathsf{addr}) = 1$ then $\mathsf{Lk}_{\mathsf{next}(h)}[\mathsf{pk}] = \perp$.

- $\mathsf{tx}_{\mathsf{burn}} \leftarrow \mathsf{CreateBurnTx}(\mathsf{sk}, \mathsf{amt}, \mathsf{st}_{\mathsf{last}(h_i)})$: if okToOperate $(\mathsf{pk}, \mathsf{tx}_{\mathsf{burn}}.\mathsf{addr}) = 1$ and $\mathsf{Bal}_{\mathsf{last}(h_i)}[\mathsf{pk}] \geq \mathsf{amt}$, then decrement Bal[pk] by amt.

(If in any of the above cases, pk is not defined, then it must be taken to mean $\mathsf{pkOf}(\mathsf{sk})$.)

Correctness. A payment mechanism is **correct** if for every group of transactions TX, whenever $\mathsf{tx}_{i,j}$ is a burn transaction $\mathsf{tx}_{\mathsf{burn}} = (\mathsf{pk}, \mathsf{amt}, \ldots)$, $\mathsf{Burn}(\mathsf{tx}_{\mathsf{burn}}).\mathsf{ETH}$ is same as $\mathsf{Bal}_{\mathsf{last}(h_i)}[\mathsf{pk}]$. (Recall that $\mathsf{Burn}(\mathsf{tx}_{\mathsf{burn}}).\mathsf{ETH}$ is the amount of Ether sent back to the user who called Burn with $\mathsf{tx}_{\mathsf{burn}}$.) Furthermore, for every sk and h, we require that $\mathsf{ReadBalance}(\mathsf{sk}, \mathsf{st}_h)$ returns $\mathsf{Bal}_{\mathsf{last}(h)}[\mathsf{pkOf}(\mathsf{sk})]$.

C   Security Requirements

We define here the common elements of the two security games; we refer to this basic version as just Security-Game. All the entities (Chal, Adv and $\mathcal{O}_{\mathsf{SC}}$) in the game receive the security parameter λ as input. When $\mathcal{O}_{\mathsf{SC}}$ receives a transaction from Chal or Adv, it adds the transaction to the queue of pending transactions. At any time, Chal can get the latest state of SC (or any older state) through $\mathcal{O}_{\mathsf{SC}}$. Adv has full view of the oracle: it can see all the transactions sent by Chal to SC, how the state of SC changes, etc.

Adversary's influence on the contract. We allow Adv to control the state of SC in one of the following ways:

---

[4]A more *natural* way to define ideal state would be to say that addresses are added as they are used in transactions. The formulation here, however, is simpler and does not lose any generality.

1. It can instruct Chal to run one of the user algorithms with certain inputs and send the resulting transaction (if any) to $\mathcal{O}_{SC}$ from an Ethereum address of its choice . Example instructions are (addr, CreateAddress), and (addr, CreateFundTx, pk, amt). Note that:

   - For a CreateAddress instruction, Chal sends the address output by this algorithm—but not the secret key—directly to Adv.
   - For transactions that require a secret key under the possession of Chal as an input, Adv specifies the corresponding public key instead.
   - When Chal receives an instruction, it uses the state of SC in the last block of the previous epoch (if needed) to execute the instruction.
   - If Chal has generated a transfer or a burn transaction in an epoch with a certain public key, then instructions to generate any one of these two transactions again from the same public key in the same epoch will be rejected. Chal will also reject transfer instructions that require it to use accounts locked to different addresses in the anonymity set. (This point and the one before are important because Chal models honest parties in the system.)

2. It can directly send an arbitrary transaction to $\mathcal{O}_{SC}$.

3. It can ask $\mathcal{O}_{SC}$ to process an arbitrary (non-empty) subset of the pending transactions and update the state of SC. This captures the addition of a new block to the blockchain.

The game stops when Adv so desires. Let $h^\star$ be the height of the last block. Let PK denote the set of public keys generated by Chal (at the behest of Adv). Adv does not have the secret keys for them.

C.1   Overdraft-safety

We capture overdraft-safety by means of a game called Overdraft-Safety-Game between a challenger Chal, an adversary Adv and the oracle $\mathcal{O}_{SC}$, who interact in the exact same way as Security-Game. Let us associate some quantities with the game with respect to Adv:

- EtherDeposited. Denotes the sum of all $tx_{fund}.ETH$ for which $tx_{fund} = (pk, \dots)$ is such that $pk \notin PK$.

- ZetherReceived. Let in be the sum of all $tx_{fund}.ETH$ for which $tx_{fund} = (pk, \dots)$ is such that $pk \in PK$. Let $honBal = \sum_{pkOf(sk) \in PK} ReadBalance(sk, st_{h^\star})$ be the total balance of honest parties. (Recall that $h^\star$ is the height of the last added block before the game ends.) Finally, let out be the sum of all $burn(tx_{burn}).ETH$ for which $tx_{burn} = (pk, \dots)$ is such that $pk \in PK$. Then ZetherReceived denotes $in - out - honBal$, which may be negative.

- EtherBurnt. Denotes the sum of all $burn(tx_{burn}).ETH$ for which $tx_{burn} = (pk, \dots)$ is such that $pk \notin PK$.

A payment mechanism is *safe against overdrafts* if for all PPT adversaries Adv, the probability that EtherDeposited + ZetherReceived < EtherBurnt in Overdraft-Safety-Game is $negl(\lambda)$, where the probability is taken over the coin tosses of Adv and the challenger.

C.2   Privacy

In order to capture the privacy requirement formally, we define a game called Privacy-Game between a challenger Chal, an adversary Adv and the oracle $\mathcal{O}_{SC}$, who interact in the same way as Security-Game but with one crucial difference. Instead of sending just one instruction to

Chal every time, Adv sends two *consistent* instructions at some point and only one instruction rest of the time (consistency will be defined below). Chal executes the $(b+1)$-th instruction based on a bit b hidden from Adv, which is chosen randomly in advance. Adv outputs a bit b' at the end of the game as a guess for b. (This is the typical left-or-right setting used for indistinguishability-based definitions.)

Two instructions are *consistent* if they refer to the same user algorithm and need to be sent from the same Ethereum address. Additionally, if the instructions are for

- creating a fund transaction, then they are associated with the same public key and amount.

- creating a transfer transaction, then

  - they are associated with the same anonymity set;
  - the amounts should be at most the value returned by ReadBalance with the respective sender's public key and the state of the last block in the previous epoch;
  - if any of the receivers is a corrupt party, both instructions have the same receiver and the same amount.

- creating a lock transaction, then they are associated with the same public key and Ethereum address.

- creating an unlock transaction, then they are associated with the same public key.

- creating a burn transaction, then they are associated with the same public key, and ReadBalance with that public key and the state of the last block in the previous epoch returns the same value.

- executing ReadBalance, then they must return the same value.

A payment mechanism is *private* if for all PPT adversaries Adv, the probability that $b' = b$ in Privacy-Game is $1/2 + \mathsf{negl}(\lambda)$, where the probability is over the coin tosses of Adv and challenger.

D   Anonymous Zether

In this section, we discuss an anonymous version of Zether in detail. While this version hides both sender and receiver apart from hiding the transfer amount, it also incurs some additional costs. First, the size of ZK-proof for a transfer increases linearly with the size of the anonymity set. Second, as we will see, users would be able to do only one transfer or burn transaction per epoch (not one of each).

D.1   Overview

More complex ZK-proof. An anonymous transfer transaction enables a user Alice with public key y_A interested in sending b ZTH to another user Bob with public key y_B to hide both herself and Bob among a larger group of users $\mathbb{U}$ with public keys $\{y_1, \ldots, y_n\}$, along with hiding b. ($\mathbb{U}$ of course contains Alice and Bob.) As a result, Alice provides a more complex ZK-proof π. Specifically, Alice generates n ciphertexts $C_1, \ldots, C_n$ under keys $y_1, \ldots, y_n$ respectively. π shows that all the ciphertexts are well-formed; only two of the underlying amounts are non-zero and their values only differ in sign; and, the remaining balance of the account with positive amount is non-negative.

We use several optimizations to reduce the size of π and verification cost. The prover sends n ciphertexts, and all of them expect two encrypt 0. We leverage this in our proof construction such that the proof statement only contains two range proofs, as sub-statements. Concretely we use one-out-of-many proofs [GK15]. These proofs can be used to give a secondary encryption to one out of n ciphertexts without revealing which original ciphertext was re-encrypted. One-out-of-many proofs can be used to build ring-signatures. Alice uses this proof to create secondary encryptions of b and $-b$ under y_A and y_B respectively along with a secondary encryption of Alice's balance b^*. Alice then simply shows the relationship between b and $-b$ and that b and $b^* - b$ are non-negative using a range proof.

Replay and double-spend protection. There is a subtle issue with using the same replay protection mechanism we proposed earlier for confidential transfers. An anonymous transaction published by Alice involves multiple accounts only one of which Alice may own. To preserve anonymity, we cannot treat Alice's account in any special way. Indeed, all the accounts involved in the transaction must be treated in the same way. Thus, the nonces associated with *each* one of them should be incremented. Unfortunately, this immediately leads to a serious problem. Other account holders involved in Alice's transaction may have generated a transaction with the previous value of nonce. If their transactions get in later, then they will be rejected. If even one of them gets in before, then Alice's transaction will be rejected.

We take a different approach to replay protection, which has some similarities with that of Monero. Every epoch will be associated with a base g_{epoch} derived from hashing some fixed string like 'Zether' and the current epoch number. To initiate a transfer or burn transaction from an account with public key $y = g^{\mathsf{sk}}$, $g_{\mathsf{epoch}}^{\mathsf{sk}}$ must be included in the transaction. More precisely, the proof π described above for a transfer transaction will also show knowledge of sk such that $\overline{g} = g_{\mathsf{epoch}}^{\mathsf{sk}}$ for $\overline{g}$ included in the transaction. (Burn transactions' proofs will also include this.) Importantly, $\overline{g}$ is computationally unlinkable to y under the DDH assumption. We refer to $\overline{g}$ as a nonce in the sequel.

While in the case of confidential transfers, we subtract the transfer amount from the sender's balance immediately but keep it pending for the receiver, one cannot take the same approach for anonymous transfers. All the transfer amounts, whether positive (for the receiver), negative (for the sender) or zero (for others), have to be kept pending. Thus, an anonymous transfer transaction would not immediately affect the balance of any of the users involved. This opens up the system to double-spending attacks. A user could generate two transfer transactions in an epoch, sending her total balance to two different users. The attached ZK-proofs would both be valid because they will be verified against the same state. Fortunately, the nonce, in addition to preventing replay attacks, also prevents such double-spending attacks.

During every epoch, ZSC will accumulate nonces as they come, rejecting any transaction that reuses a nonce. An important difference from Monero is that the set of nonces does not grow indefinitely; it is reset to null at the beginning of every epoch. Thus, providing anonymity does not lead to a continuous growth in the size of the state of ZSC.

A drawback of this approach to replay protection and double-spending is that even honest users can only initiate at most one transfer or burn transaction in a given epoch.

Global updates. With the new replay protection mechanism in place, a few global updates need to be made in every epoch: set the base for the epoch and empty the nonce set. We will have to make the updates at the receipt of the very first message in an epoch, be it from any account. Thus, users will have to provide a little more gas to cover the possibility that
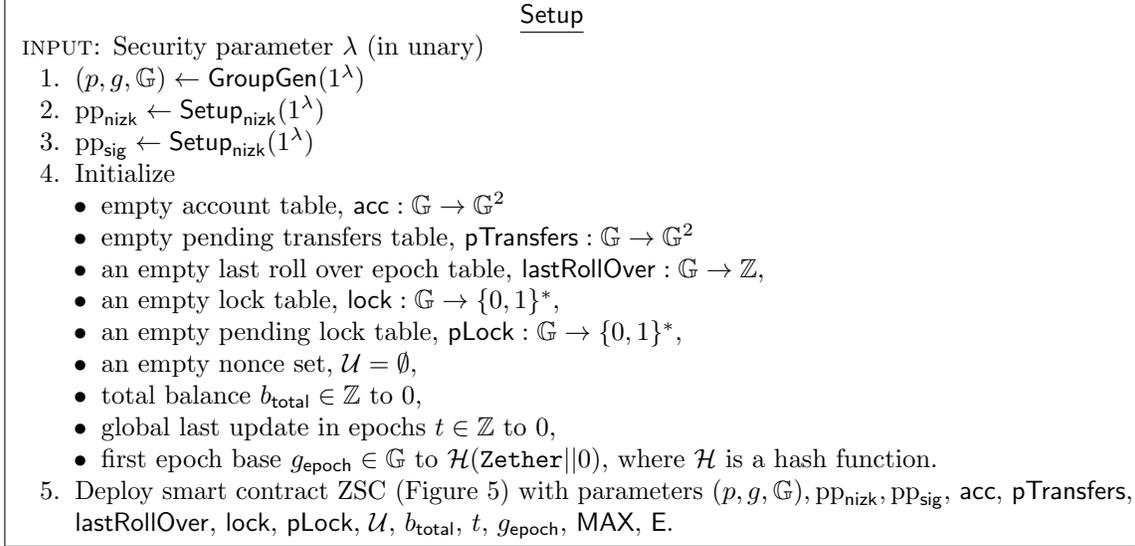
```
                                    Setup
INPUT: Security parameter λ (in unary)
  1. (p, g, 𝔾) ← GroupGen(1^λ)
  2. pp_nizk ← Setup_nizk(1^λ)
  3. pp_sig ← Setup_nizk(1^λ)
  4. Initialize
     • empty account table, acc : 𝔾 → 𝔾²
     • empty pending transfers table, pTransfers : 𝔾 → 𝔾²
     • an empty last roll over epoch table, lastRollOver : 𝔾 → ℤ,
     • an empty lock table, lock : 𝔾 → {0,1}*,
     • an empty pending lock table, pLock : 𝔾 → {0,1}*,
     • an empty nonce set, 𝒰 = ∅,
     • total balance b_total ∈ ℤ to 0,
     • global last update in epochs t ∈ ℤ to 0,
     • first epoch base g_epoch ∈ 𝔾 to ℋ(Zether‖0), where ℋ is a hash function.
  5. Deploy smart contract ZSC (Figure 5) with parameters (p, g, 𝔾), pp_nizk, pp_sig, acc, pTransfers,
     lastRollOver, lock, pLock, 𝒰, b_total, t, g_epoch, MAX, E.
```

Figure 4: Anonymous Zether setup

their message could be the very first one in an epoch. In most cases, this extra gas will be reimbursed.

Locking to smart contracts. It is not hard to see that if some accounts involved in an anonymous transfer are locked to a smart contract then all of the locked accounts must be locked to the same contract. Furthermore, the transfer is processed only if it comes from that contract.

A more difficult thing to observe is that locking must not come into effect immediately. Suppose Alice publishes a transaction in a certain epoch to lock her account to a smart contract. Another user Bob may have published a transfer transaction (at about the same time as Alice) with Alice in his anonymity set while her account was still unlocked. If Alice's transaction gets in first, locking her account, then Bob's transaction will be rejected. The same holds for unlocking as well. Therefore, when ZSC is invoked to lock/unlock an account, it just records the request but does not act on it immediately. When the account is rolled over in some later epoch, the request will be executed. (Recall that every method on ZSC first checks if there is a need for roll over.)

Lock transactions also need replay protection. In fact, using the account secret key, the sender must sign both the nonce and an address (to which the account will be locked) in the case of confidential transfers, and both the epoch base and address in the case of anonymous transfers. As a result, for the latter case, lock transactions must be published at the beginning of an epoch just like transfer and burn transactions.

D.2 Mechanism design

We now formally describe the three components of anonymous Zether (setup, smart contract and user algorithms) with respect to the basic version (see Section 6).

Setup. Four new variables are initialized in setup: a pending lock table pLock to temporarily hold lock requests, a nonce set 𝒰 to prevent replay attacks, a global last update variable t to

record the last epoch in which *any* account was updated, and an epoch base g_{epoch}. Also, the counter table goes away. See Figure 4 for a complete description.

Anonymous transfer ZK-proof. Anonymous transfers not only hide the transfer amount but also the sender and receiver in a transfer. Suppose a user wants to transfer an amount $b^\star$ from a public key y to $\bar{y}$, and it would like to hide the two keys among a larger set of public keys, say $\mathbf{y} = \{y_1, \ldots, y_n\}$. Let $(C_{L,i}, C_{R,i})$ be the encryption of the balance associated with key y_i, for $i \in [n]$. The user now needs to create n ciphertexts $(C_1, D_1), \ldots, (C_n, D_n)$ and prove that:

- they are well-formed;
- one of them (say jth) encrypts $b^\star$, one of them (say ℓth) encrypts $-b^\star$, rest encrypt 0;
- $b^\star$ is positive;
- remaining balance in y_j (say b') is also positive; and,
- the correct nonce is declared.

We can again reuse randomness and set $D_1 = \cdots = D_n = D$.

To handle such a complex statement efficiently without revealing j, ℓ, $b^\star$ and b', we introduce new *binary* variables $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$. Value 1 for an s_i denotes that money is being transferred *from* y_i and value 1 for a t_j denotes that money is being transferred *to* y_j. The user would keep these variables secret and prove various statements using them. Only one of $s_1, \ldots, s_n$ and one of $t_1, \ldots, t_n$ should be 1. This could be shown by proving that each of these variables is either 0 or 1, $\sum_i s_i = 1$ and $\sum_i t_i = 1$.

In addition, the user proves:

$$\prod_{i=1}^{n} C_i^{s_i} = g^{b^\star} \prod_{i=1}^{n} y_i^{r \cdot s_i} \tag{3}$$

$$\prod_{i=1}^{n} C_i^{s_i + t_i} = \prod_{i=1}^{n} y_i^{r \cdot (s_i + t_i)} \tag{4}$$

$$C_i^{(1-s_i) \cdot (1-t_i)} = y_i^{(1-s_i) \cdot (1-t_i) \cdot r} \text{ for } i \in [n] \tag{5}$$

$$\prod_{i=1}^{n} \left(\frac{C_{L,i}}{C_i} \right)^{s_i} = g^{b'} \left(\frac{\prod_{i=1}^{n} C_{R,i}^{s_i}}{D} \right)^{\text{sk}} \tag{6}$$

$$g_{\text{epoch}}^{\text{sk}} = u \tag{7}$$

Given that exactly one of $s_1, \ldots, s_n$ is 1 and rest are 0, Eq (3) shows that the ciphertext for non-zero s_i is a valid encryption of $b^\star$. When Eq (3) is subtracted from Eq (4), we get $\prod_{i=1}^{n} C_i^{t_i} = g^{-b^\star} \prod_{i=1}^{n} y_i^{r \cdot t_i}$, which shows that the ciphertext for non-zero t_i is a valid encryption of $-b^\star$. Thus, Eq (3) and (4) together show that the ciphertexts that encode non-zero quantities are valid.

These statements can be proved more efficiently using techniques from one-out-of-many proofs [GK15] and in particular the extension to ElGamal encryptions [BCC+15]. These proofs are Σ protocols that can be used to show that a decryption of one out of n ciphertexts has certain properties, e.g. they are 0. The proof size is only logarithmic in n. This is achieved by writing i in it's binary representations and constructing n products such that only the ith is 1 and all other are 0.

In Eq (5), the expression $(1 - s_i)(1 - t_i)$ is non-zero only when both s_i and t_i are zero. For such i, C_i should be an encryption of 0, which is what the equation shows. (When s_i or t_i is non-zero, both sides are of the equation are just 0.) Eq (6) shows that b' balance is left in the account for which s_i is 1. Lastly, Eq (7) shows that u is the correct nonce for the current epoch.

Further, the user also needs to show that $g^{\mathsf{sk}} = \Pi y_i^{s_i}$, $b^\star \in [0, \mathsf{MAX}]$ and $b' \in [0, \mathsf{MAX}]$, where the first equation ties the secret key to the spending public key (without revealing the latter), and the rest two show that the amount being transferred and the remaining amount are in the right range. Summing it up, the user proves the following statement:

$\mathsf{st}_{\mathsf{AnonTransfer}}$:

$$\Big\{ ((y_i, C_{L,i}, C_{R,i}, C_i)_{i=1}^n, D, u, g, g_{\mathsf{epoch}}; \mathsf{sk}, b^\star, b', r, (s_i, t_i)_{i=1}^n) :$$

$$\prod_{i=1}^n C_i^{s_i} = g^{b^\star} \prod_{i=1}^n y_i^{r \cdot s_i} \wedge \prod_{i=1}^n C_i^{s_i + t_i} = \prod_{i=1}^n y_i^{r \cdot (s_i + t_i)} \wedge$$

$$D = g^r \wedge (C^{(1 - s_i) \cdot (1 - t_i)} = y_i^{(1 - s_i) \cdot (1 - t_i) \cdot r})_{i=1}^n \wedge$$

$$\prod_{i=1}^n \left(\frac{C_{L,i}}{C_i} \right)^{s_i} = g^{b'} \left(\frac{\prod_{i=1}^n C_{R,i}^{s_i}}{D} \right)^{\mathsf{sk}} \wedge g^{\mathsf{sk}} = \prod_{i=1}^n y_i^{s_i} \wedge$$

$$g_{\mathsf{epoch}}^{\mathsf{sk}} = u \wedge (s_i \in \{0, 1\} \wedge t_i \in \{0, 1\})_{i=1}^n \wedge$$

$$\sum_{i=1}^n s_i = 1 \wedge \sum_{i=1}^n t_i = 1 \wedge b^\star \in [0, \mathsf{MAX}] \wedge b' \in [0, \mathsf{MAX}] \Big\} \quad (8)$$

The statement is complex, but in fact highly structured. The resulting proof size can be logarithmic in the range and in the anonymity set. This is done by combining one-out-of-many proofs for showing that two encryptions are non-zero with Bulletproofs for range proofs and for showing that all other encryptions encrypt 0. The proofs can be efficiently combined using our extension of Bulletproofs called Σ-Bullets (Section G). Even with this efficient proof the transaction size will still be linear in the anonymity set. This is because the sender needs to send an encryption for each account in the anonymity set. This seems inherent as every account needs to be treated equally in an anonymous transfer. This limitation is not present in UTXO-based currencies where constant sized fully anonymous payment systems have been proposed and implemented [MGGR13, BCG+14]. Theoretically, the requirement could be removed using fully homomorphic encryption but it remains an open problem whether a more practical solution is available.

Contract. The contract for anonymous version of Zether is described in Figure 5. We discuss below how it differs from ZSC.

Locking. In the anonymous version, (un)locking must not take effect immediately, i.e. in the same epoch as the transaction is published; it must be deferred to the next epoch (see Appendix D.1). Therefore, both Lock and Unlock change entries in the table pLock rather than changing lock directly. Also, the signature given to Lock is on the epoch base instead of the counter.

Rolling over. RollOver also rolls over any changes to the locking address of the input public key (pLock is assigned to lock) now. Some global changes are also made in an epoch. For this,

Fund
- INPUTS: public key y
1. RollOver(y)
2. Let $b = \mathsf{msg.value}$
3. require:
   - $b + b_{\mathsf{total}} \le \mathsf{MAX}$
   - CheckLock$(y, \mathsf{msg.sender}) = 1$
4. If $\mathsf{acc}[y] = \bot$:
   - Let $H = \mathsf{block.number}$, $e = \lfloor H/\mathsf{E} \rfloor$
   - Set $\mathsf{acc}[y] = (1,1)$
   - Set $\mathsf{pTransfers}[y] = (g^b, 1)$
   - Set $\mathsf{lock}[y] = \mathsf{pLock}[y] = \bot$
   - Set $\mathsf{lastRollOver}[y] = e$
   Else:
   - Set $\mathsf{pTransfers}[y] = \mathsf{pTransfers}[y] \circ (g^b, 1)$
5. Set $b_{\mathsf{total}} = b_{\mathsf{total}} + b$

Transfer
- INPUTS:
  - set of public keys $\mathbf{y} = \{y_1, \ldots, y_n\}$
  - ciphertexts $(C_1, D), (C_2, D), \ldots, (C_n, D)$
  - nonce u
  - proof π_{transfer}
1. For each $i \in [1, n]$:
   a. RollOver(y_i)
   b. Let $(C_{L,i}, C_{R,i}) = \mathsf{acc}[y_i]$
2. Let $\mathbf{C} = \{C_1, \ldots, C_n\}$
3. require:
   - $u \notin \mathcal{U}$
   - CheckLock$(y_i, \mathsf{msg.sender}) = 1$ for $i \in [1, n]$
   - $\mathsf{Verify}_{\mathsf{nizk}}(\mathsf{st}_{\mathsf{AnonTransfer}}[\mathbf{y}, \mathbf{C}, D,$
     $(C_{L,i}, C_{R,i})_{i=1}^n, u, g, g_{\mathsf{epoch}}], \pi_{\mathsf{transfer}}) = 1$
4. Set $\mathcal{U} = \mathcal{U} \cup \{u\}$
5. For each $i \in [1, n]$, set
   $\mathsf{pTransfers}[y_i] = \mathsf{pTransfers}[y_i] \circ (C_i, D)$

Lock
- INPUTS:
  - public key y
  - Ethereum address addr
  - signature σ_{lock}
1. RollOver(y)
2. require:
   - CheckLock$(y, \mathsf{msg.sender}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(y, (\mathsf{addr}, g_{\mathsf{epoch}}), \sigma_{\mathsf{lock}}) = 1$
3. Set $\mathsf{pLock}[y] = \mathsf{addr}$

Burn
- INPUTS:
  - public key y
  - balance b
  - nonce u
  - proof π_{burn}
1. RollOver(y)
2. Let $(C_L, C_R) = \mathsf{acc}[y]$
3. require:
   - $u \notin \mathcal{U}$
   - CheckLock$(y, \mathsf{msg.sender}) = 1$
   - $\mathsf{Verify}_{\mathsf{nizk}}(\mathsf{st}'_{\mathsf{burn}}[y, C_L, C_R, u, b, g, g_{\mathsf{epoch}}],$
     $\pi_{\mathsf{burn}}) = 1$
4. Set $\mathcal{U} = \mathcal{U} \cup \{u\}$
5. Set $\mathsf{acc}[y] = \mathsf{acc}[y] \circ (C_L^{-1}, C_R^{-1})$
6. Set $b_{\mathsf{total}} = b_{\mathsf{total}} - b$
7. Do $\mathsf{msg.sender.transfer}(b)$

Unlock
- INPUTS: public key y
1. RollOver(y)
2. require:
   - CheckLock$(y, \mathsf{msg.sender}) = 1$
3. Set $\mathsf{pLock}[y] = \bot$

Internal Helper Methods

RollOver
- INPUTS: public key y
1. Let $H = \mathsf{block.number}$, $e = \lfloor H/\mathsf{E} \rfloor$
2. If $\mathsf{lastRollOver}[y] < e$:
   - Set $\mathsf{acc}[y] = \mathsf{acc}[y] \circ \mathsf{pTransfers}[y]$
   - Set $\mathsf{pTransfers}[y] = (1,1)$
   - Set $\mathsf{lock}[y] = \mathsf{pLock}[y]$
   - Set $\mathsf{lastRollOver}[y] = e$
3. If $t < e$:
   - Set $g_{\mathsf{epoch}} = \mathcal{H}(\texttt{Zether}||e)$
   - Set $\mathcal{U} = \emptyset$
   - Set $t = e$

Figure 5: Smart contract for anonymous version of Zether. $\texttt{CheckLock}$ is same as in Figure 2.

RollOver checks if the last global update t was in a older epoch. If so, then it sets g_{epoch} for the current epoch, empties the nonce set $\mathcal{U}$ and resets t.

Account counters vs nonce set. Anonymous Zether has a different replay protection mechanism,

so all the logic related to account counters (initializing them in Fund, incrementing them in Transfer, Burn, Lock) goes away. Instead, nonces u that come with Transfer and Burn are added to the set $\mathcal{U}$. This set is reset to null in every epoch.

Burn. A slightly different statement is proved now, denoted by $\mathsf{st}'_{\mathsf{burn}}$. The new statement is same as $\mathsf{st}_{\mathsf{burn}}$ but with one additional condition, $u = g_{\mathsf{epoch}}^{\mathsf{sk}}$. On the positive side, there is no need to verify a signature.

Transfer. As we have seen before, the statement $\mathsf{st}_{\mathsf{AnonTransfer}}$ is a lot more complex than $\mathsf{st}_{\mathsf{ConfTransfer}}$. Transfer takes a set of n public keys and ciphertexts (instead of just two before), rolls over and checks the locks on each one of them, and then verifies a more complex proof π_{transfer}. For all the accounts, the pending transfers table is updated. (Just like Burn, there is no signature verification now.)

CreateTransferTx
- INPUTS:
  - shuffled anonymity set $\mathbf{y} = \{y_1, \ldots, y_n\}$ which includes sender and receiver
  - sender index i_{from}
  - receiver index i_{to}
  - sender private key x
  - sender balance b_{from}
  - transfer amount $b^\star$
  - state st_h of ZSC
- OUTPUT: $\mathsf{tx}_{\mathsf{trans}} = (\mathbf{y}, \mathbf{C}, D, u, \pi_{\mathsf{transfer}})$
1. Roll over all y_i in st_h
2. Let $(C_{L,i}, C_{R,i}) = \mathsf{acc}[y_i]$ for $i \in [n]$
3. $r \xleftarrow{\$} \mathbb{Z}_p$
4. Set $C_{i_{\mathsf{from}}} = g^{b^\star} y_{i_{\mathsf{from}}}^r$
5. Set $C_{i_{\mathsf{to}}} = g^{b^\star} y_{i_{\mathsf{to}}}^r$
6. Set $C_i = y_i^r$ for $i \in [n] \setminus \{i_{\mathsf{from}}, i_{\mathsf{to}}\}$
7. Set $\mathbf{C} = \{C_1, \ldots, C_n\}$ and $D = g^r$
8. Set $s_{i_{\mathsf{from}}} = 1$ and $s_i = 0$ for $i \in [n] \setminus \{i_{\mathsf{from}}\}$
9. Set $t_{i_{\mathsf{to}}} = 1$ and $t_i = 0$ for $i \in [n] \setminus \{i_{\mathsf{to}}\}$
10. Set $u = g_{\mathsf{epoch}}^x$
11. Set $w = (x, b^\star, b_{\mathsf{from}} - b^\star, r, (s_i, t_i)_{i=1}^n)$
12. $\pi_{\mathsf{transfer}} = $ $\mathsf{Prove}(\mathsf{st}_{\mathsf{AnonTransfer}}[\mathbf{y}, \mathbf{C}, D, (C_{L,i}, C_{R,i})_{i=1}^n, u, g, g_{\mathsf{epoch}}], w)$

CreateBurnTx
- INPUTS:
  - private key x
  - state st_h of ZSC
- OUTPUT: $\mathsf{tx}_{\mathsf{burn}} = (y, b, u, \pi_{\mathsf{burn}})$
1. Let $b = \mathsf{ReadBalance}(x, \mathsf{st}_h)$
2. $u = g_{\mathsf{epoch}}^x$
3. $w = (x)$
4. Set $y = g^x$
5. Let $(C_L, C_R) = \mathsf{acc}[y]$
6. $\pi_{\mathsf{burn}} = $ $\mathsf{Prove}(\mathsf{st}'_{\mathsf{burn}}[y, C_L, C_R, u, b, g, g_{\mathsf{epoch}}], w)$

CreateLockTx
- INPUTS:
  - private key x
  - locking Ethereum address addr
  - state st_h of ZSC
- OUTPUT: $\mathsf{tx}_{\mathsf{lock}} = (y, \mathsf{addr}, \sigma_{\mathsf{lock}})$
1. Compute $\sigma_{\mathsf{lock}} = \mathsf{Sign}(x, (\mathsf{addr}, g_{\mathsf{epoch}}))$
2. Set $y = g^x$

Figure 6: User algorithms for anonymous version of Zether. CreateAddress and ReadBalance are same as in Figure 3.

User Algorithms. CreateAddress, CreateFundTx, CreateUnlockTx and ReadBalance do not change. CreateBurnTx and CreateTransferTx produce proofs for different statements now. They roll over the input public key(s) not just to make sure that any pending transfers are rolled over, but also to make sure that any pending lock requests take affect. CreateLockTx signs the epoch base instead of the counter.

E Security Proof

In this section we provide a proof sketch to show that the anonymous version of Zether satisfies the correctness and security requirements from Appendix B and C. (Security proof of basic Zether is roughly a special case of this.)

Correctness. We first prove that Zether satisfies the correctness definition. Consider a slightly modified version of Zether where RollOver is called on all accounts at the end of each epoch. This only differs from Zether from an efficiency viewpoint as Zether implements lazy roll overs (i.e., every ZSC method rolls over all the accounts it touches in the very beginning of the call). Using this we show that every honestly generated transaction will in fact be processed successfully by ZSC.

Algorithms CreateTransferTx and CreateBurnTx roll over all the input public keys based on the state of the smart contract. Thus, any pending transfers associated with these keys are absorbed into the respective accounts and any pending lock requests take effect. Transfer and burn transactions are then generated with respect to this new state of the accounts, which will match with the state ZSC will use to process them (as long as the delay is less than the length of an epoch).

Honest users put only those accounts in their anonymity set that are locked to the same address (if any of them is locked at all). Even if one of the account holders changes the lock on his/her account by calling Lock or Unlock, these methods treat the new locking address (which could be $\perp$) as a pending lock. The lock request will take effect in a subsequent epoch, so transactions generated in this epoch will not be affected.

The rest of the correctness follows from the homomorphic properties of ElGamal encryption as well as the correctness properties of the proof system. Though the encrypted values are in $\mathbb{Z}_p$ and the ideal state handles positive integers, this is not a problem because ZSC takes deposits only up to an amount MAX, a constant much smaller than p. The homomorphic operations, therefore, would not cause an overflow.

Finally, note that a user is able to create a nonce and as such a transaction or burn per epoch unless $g_{\mathsf{epoch}} = g_{\mathsf{epoch}'}$ for $\mathsf{epoch} \neq \mathsf{epoch}'$. This however happens with at most negligible probability if the hash function $\mathcal{H}$ is collision resistant.

Overdraft-safety. We show that ZSC methods move the right amount of funds to/from accounts by proving that they satisfy certain properties. An inductive argument would then show that Zether is safe against overdrafts as per Appendix C.1.

Let us consider the method Fund first. Let (C_L, C_R) be the (rolled over) state of an account y. If, hypothetically, Burn is invoked on this state, suppose it returns b ETH. Now Fund is called with b' ETH. We show that if Burn is invoked again (hypothetically), it will return no more than $b + b'$ ETH. Since Burn returns b on the first invocation, it must be that $C_L = g^b C_R^{\mathsf{sk}}$ due to the soundness property of ZK-proofs. When b' is deposited, pTransfers is set to $(g^{b'}, 1)$. Now when Burn is invoked again, the state of y will either be (C_L, C_R) or $(C_L, C_R) \circ (g^{b'}, 1)$ depending on whether there is a roll over or not. In the first case, only b will satisfy the required relation between C_L and C_R, and, in the second case, only $b + b'$ will. So, again due to the soundness property, at most $b + b'$ can be obtained by burning.

Next we consider the method Transfer. Let $(y_1, \ldots, y_n)$ be the anonymity set, (C_1, D), $\ldots$, (C_n, D) be the ciphertexts, and π_{transfer} be the proof for a transfer transaction tx. Let $(C_{L,i}, C_{R,i})$ be the (rolled over) state of the concerned accounts. If Burn is invoked (hypothetically) on these accounts, suppose it returns $b_1, \ldots, b_n$ ETH, respectively. Now if tx is

processed successfully by Transfer, then it must be that there exists a j, k and $b^\star$ s.t. (C_j, D) encrypts $-b^\star$ under y_j, (C_k, D) encrypts $b^\star$ under y_k, and rest of the ciphertexts encrypt 0 (due to the soundness property). Transfer sets pTransfers$[y_i]$ to be (C_i, D) for all i. Thus, when Burn is invoked again on y_i, its state will either be $(C_{L,i}, C_{R,i})$ or $(C_{L,i}, C_{R,i}) \circ (C_i, D)$ depending on whether there is a roll over or not. For the accounts other than y_j and y_k, the same amount as before will be returned. For y_k, at most $b_k + b^\star$ will be returned. Finally, for y_j, note that no burning can take place in this epoch because transfer has already declared the nonce. When a burn is processed in the next epoch, there will be a roll over changing the account state to $(C_{L,i}, C_{R,i}) \circ (C_i, D)$. So Burn will return $b_j - b^\star$. Therefore, we can see that transfer transactions cannot be used to increase the overall Zether balance of the accounts involved. Further note that the nonce along with the soundness of the proof system, enforce that an adversary will at most be able to do a single transfer per account per epoch.

One can similarly analyze the method Burn. We skip the details.

Now we can use a simple inductive argument to show that an adversary which wins Security-Game will break the soundness of the proof system. This happens with at most negligible probability.

Privacy: Confidentiality & Anonymity. In Privacy-Game, Adv sends one instruction to Chal every time except once, when it sends two consistent instructions. The consistency requirements prevent Adv from trivially winning the game. If the instructions are for funding, locking or unlocking, then it is easy to see that the adversary has no advantage. Two consistent burn instructions will also not reveal any additional information to Adv due to the zero-knowledge property of the proof system.

We are only left with the case of two consistent transfer instructions. A transfer transaction consists of an anonymity set $\mathbf{y}$, a list of commitments $\mathbf{C}$, a blinding value D, a nonce u, and π_{transfer}. Two consistent transactions could have two different senders, so the nonce values could be different. However, g_{epoch}^x (for any x) is indistinguishable from random under the DDH assumption since both y and g_{epoch} are random (when $\mathcal{H}$ is modeled as a random oracle). Further, ciphertexts (C_i, D) for honest i are indistinguishable from the encryption of random messages. Now, let the receivers for the two instructions be j and k. If neither of them are under the control of Adv, then all the ciphertexts Adv can decrypt are just encryptions of 0. Otherwise, both j and k must be corrupt. In this case, Adv can decrypt (C_j, D) and (C_k, D) too, but then they must decrypt to the same amount.

F   Discussion and Extensions

We discuss here certain important things related to the use of Zether.

Paying gas in ZTH through economic abstraction. One of the main limitations of the anonymity of Zether comes from the fact that every transaction needs to pay fees in ETH pegged gas. This is not only cumbersome as a ZTH holder needs to maintain both a Zether and an Ethereum account, it can also have consequences for the anonymity of a transaction. [5] Every transaction is initiated by an EOA (see Section 2) and that EOA pays for the gas. Unfortunately, no matter what privacy guarantees Zether has, transactions that are issued by the same EOA are inevitably linked. Even if a user controls multiple EOAs she has to make

---

[5]Anonymity is a hard to achieve goal in general. There are several ways to attack Monero [KFTS17, MSH$^+$18] and Zcash [Que17, KYMM18] for example.

sure that they remain unlinkable in order to send anonymous transactions on Zether. (The confidentiality of a transaction is not affected by this.)

Ideally, miners could receive transaction fees in ZTH instead of ETH which are by design exchangeable and have as such identical value. In order to do this, a transaction will be sent with a 0 gas price. This means that a newly created unlinked EOA can issue the transaction. Every transaction will specify the fee amount publicly. In the ZK-proof the sender now proves that his new balance is his old balance minus the transacted amount minus the fees. The fees is then sent to a fee pool within the Zether contract that can be spent from without further permission or secrets. A miner can simply insert a raking transaction at the end of the block that pays all of the fees to his account. The fee pool could also be used to fund contract-wide transactions such as RollOver.

The idea of paying fees in a non-native currency is called economic abstraction and has been discussed intensively [But15, Rub18]. The concept is particularly interesting with respect to Zether as it is would make Zether a) more usable and b) more private. The major obstacle to this approach is that miners would need to mine these special 0 gas price transactions and properly rake the fee pool. A similar approach that circumvents the miner adoption problem is to have special delegator nodes that issue the transactions to the network. Users would send their transactions to delegators who will forward them to the miners and will pay the Ethereum gas fees. These delegator nodes could be rewarded in Zether by adding their Zether address to the transaction. The fee amount would not go to the fee pool but to that address.

A general problem for any anonymous blockchain transaction is that transactions need to be relayed to either the miners or the delegators without revealing the original sender's identity. This problem can be alleviated through anonymous communication networks like Tor [Tor].

Zether as a native token. Zether can be viewed as a mechanism to do private transactions in an account-based currency. If a currency like Ethereum [etha], Ripple [Rip], EOS [EOS] or Stellar [Maz15] or even a private blockchain like Sequence [Seq] wanted to introduce private transactions then they can use a Zether style system. While we have presented Zether as a smart contract token that can be run on a smart contract platform, it is also possible to envision Zether becoming the native token of such a platform. Using Zether as a native token has several advantages. As discussed in the previous paragraph, it is important for Zether's anonymity that miners receive fees in ZTH. This is automatically ensured if ZTH is the native token in which fees are denominated. An additional benefit of Zether as a native token is that denial-of-service protection becomes simpler. Miners can process transactions in an arbitrary order. For example the proofs can be verified *before* the account balances are transferred. We can potentially remove the requirement of having separate stable and temporary accounts as the ordered processing allows a user to spend ZTH even if they receive funds in the same block. Depending on the block-time, it may still be useful to maintain a temporary and a stable account to allow slightly outdated transactions to be processed correctly.

In Section 7.3, we discuss multiple optimizations that would benefit Zether. If Zether were a native token then these optimizations can be used to make transactions more efficient and scalable. For example, miners can run optimized proof validation software using efficient elliptic curves instead of using Ethereum's general purpose state machine. Further, Bulletproofs used in our instantiation of Zether can be verified more efficiently when processed in batches [BBB+18]. This is beneficial as a fully verifying node can now more efficiently process a proposed block. This property is important in order to protect against the miners' dilemma [Eya15], where miners are disincentivized to verify blocks if verification becomes too expensive.

Locking mechanism. When a Zether account is locked to a smart contract, it will only be affected by transactions coming from that contract. Specifically, no one else can deposit or withdraw money from the account. There could be other more flexible ways of locking accounts though. For instance, one could allow locked accounts to be funded from *any* address.

G   Proofs and Σ-Bullets

Transfer and AnonTransfer are medium-sized relations that involve proofs on encrypted data. We, therefore, want to use a proving system which a) is efficient, i.e. has short proofs and efficient verification and b) allows proofs on cryptographically encoded data. Bulletproofs [BBB+18] is a generic zero-knowledge proof system that produces short (logarithmic sized) proofs without relying on a trusted setup. Bulletproofs was specifically designed to work well with Confidential Transactions [Max15] as it directly proofs of statements which include values that are committed to in a Pedersen commitment. Its short proofs and trustless setup make Bulletproofs an intriguing choice for Zether's underlying proof system. However, unlike UTXO-based Confidential Transactions Zether relies on ElGamal encryptions instead of Pedersen commitments. We, therefore, aim to use a proving system similar to Bulletproofs but where we can prove statements on ElGamal encrypted values. Simply replacing Pedersen commitments with ElGamal encryptions is insufficient as ElGamal encryptions cannot be 'opened' like a commitment and are also not additively homomorphic if encryptions are under different keys, as is the case in Zether. Further for AnonTransfer we need to combine a one-out-of-many proof[6] with range proofs. The one-out of many proof is used to select the receiver and sender transfer encryption and the range proof ensures that no overdraft is created. Bulletproofs enables efficient range proofs and there are logarithmic sized efficient Σ protocols [CD98] for doing one-out-of-many proofs [GK15, BCC+15].

To efficiently prove these statements and instantiate Zether we design Σ-Bullets. Σ-Bullets is an extension of Bulletproofs. It enables the combination of Σ-protocols and Bulletproofs. Concretely given an arithmetic circuit, a Σ-Bullets proof ensures that a public linear combination of the circuit's wires is equal to some witness of a Σ protocol. This enhancement in turn enables proofs on many different encodings such as ElGamal encryptions, ElGamal commitments or Pedersen commitments in different groups or using different generators. Further it allows the combination of different specialized Σ-protocols such as one-out-of-many proofs or accumulator proofs [CL02] with the generic circuit-base proof system Bulletproofs. This will benefit other systems that want to prove statements on additively encoded witnesses.

Σ-Bullets. Bulletproofs [BBB+18] enable proofs on Pedersen committed values by computing a linear combination of commitments and opening that combination. This uses the homomorphic property of Pedersen commitments that use the same commitment key. The core idea of Σ-Bullets is to replace this linear combination with a Σ protocol. The Σ protocol ensures that the linear combination of the encoded values is equal to some public value. The efficient composability of Σ protocols allows us to combine the opening with other proofs.

We first present a high-level overview of the Bulletproofs protocol and then discuss how we modify it to construct Σ-Bullets. The prover first commits to the circuit's wires in A and to a vector of blinding values in S. The commitments are Pedersen vector commitments [BCC+16]. The prover then receives challenges y, z and commits to polynomial $t(X)$ using a

---

[6]A non-interactive one-out-of-many proof can be used to instantiate a ring-signature in which a signer reveals that she knows a private key out of

polynomial commitment that can be verifiably opened to an evaluation of $t(X)$. The prover does not commit to one of the coefficients of the polynomial, e.g. the 0 coefficient. If the prover is honest then the verifier can compute said coefficient from just the challenges and the commitments to wire values v_is which are committed to in V_i. Finally the prover convinces the verifier that $t(X)$ is equal to the inner product of two polynomials with vector coefficients. The two polynomials can be homomorphically constructed from A, S and the challenges. This final step uses an inner product argument which requires only $O(\log(n))$ communication where n is the size of the circuit. The protocol can be made non-interactive using the Fiat-Shamir heuristic. Concretely assume that given an arithmetic circuit $\mathsf{Circuit} : \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \{0,1\}$ the prover wants to prove the following that she knows $\vec{a} \in \mathbb{Z}_p^n, \vec{v} \in \mathbb{Z}_p^m$ such that:

$$V_i = \mathsf{Encode}(v_i) \forall i \in [1, m], \mathsf{Circuit}(\vec{a}, \vec{v}) = 1$$

Prover		**Verifier**
Commit to wires values $\vec{a}$ in A		
Commit to randomness in S		
	$\xrightarrow{\quad A, S \quad}$	
		$y, z \leftarrow_\$ \mathbb{Z}_q$
	$\xleftarrow{\quad y, z \quad}$	
Use y to combine constraints		
Such that they can be written as:		
$t(X) + \sum_{i=1}^n z^i v_i = \langle l(X), r(X)\rangle \in \mathbb{Z}_q$		
$\wedge\, t(0) = \delta(y, z)$		
$l(X), r(X) \in \mathbb{Z}_q^n \wedge deg(l, r) \le 3$		
$T = \mathrm{Commit}(t(X))$		
	$\xrightarrow{\quad T \quad}$	
		$x \leftarrow_\$ \mathbb{Z}_q$
	$\xleftarrow{\quad x \quad}$	
$\hat{t} = t(x), \vec{l} = l(x), \vec{r} = r(x)$		
	$\xrightarrow{\quad \hat{t}, \vec{l}, \vec{r} \quad}$	
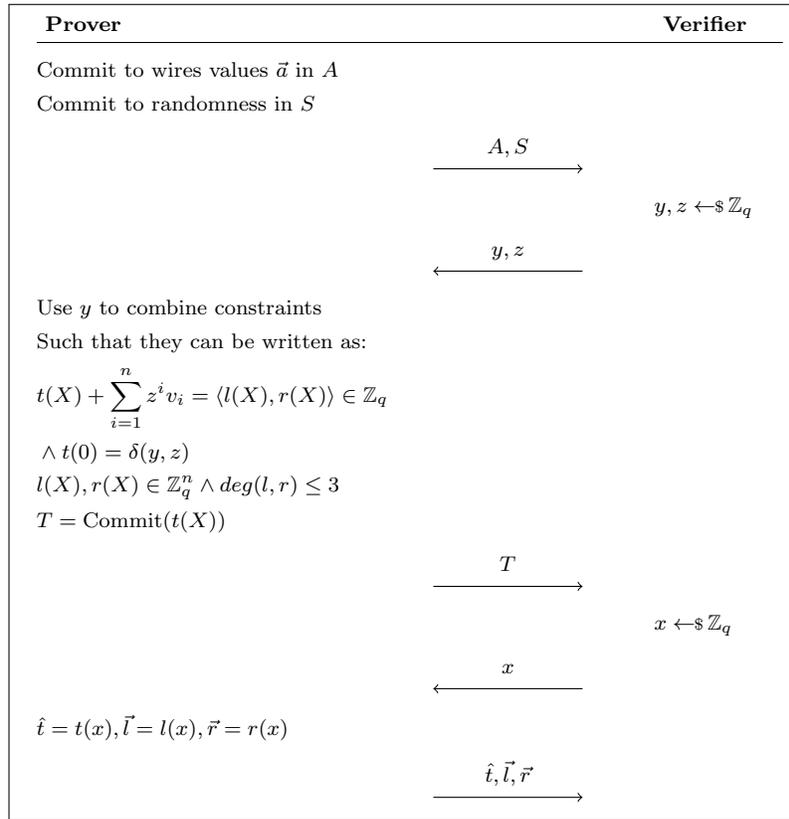
Now the verifier creates commitment P to $l(X), r(X)$ from A, S, y, z and checks the following condition:

1. $T(0) = t_0$
2. $Open(T \cdot \prod_{i=1}^m V_i^{z^i}) + \delta(y, z) = \hat{t}$
3. $Open(P) = \vec{l}, \vec{r}$
4. $\langle \vec{l}, \vec{r}\rangle = \hat{t}$

Note that the second condition requires that T and the V_i's are additively homomorphic. We can therefore not simply replace T and V_i with ElGamal encryptions as they are not homomorphic if done under different keys. We generalize the protocol by simply requiring
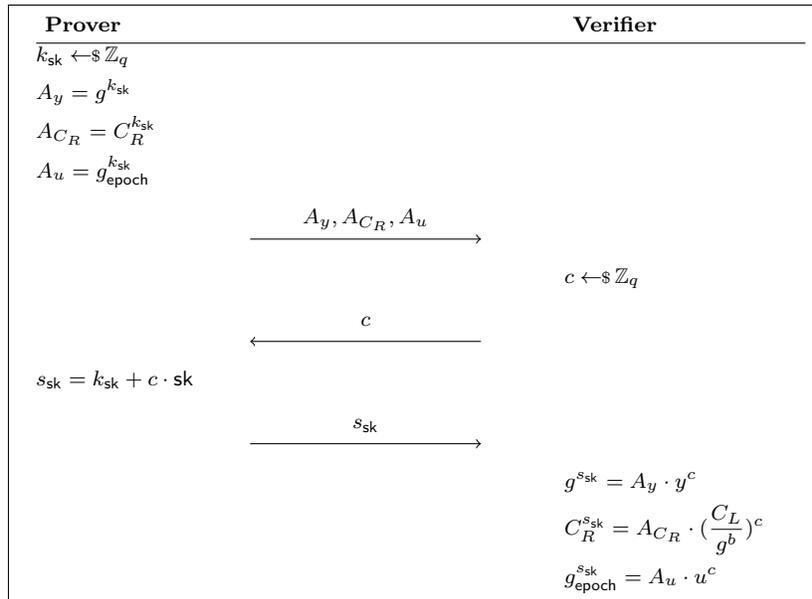
that the prover *proves* that

$$\hat{t} = \sum_{i=1}^{m} v_i \cdot z^i + \delta(y, z) + Open(T). \tag{9}$$

This can be achieved through a simple Σ protocol. We show concretely how this can be achieved for $m = 2$ and V_1, V_2 being ElGamal encryptions in the burn proof. We further provide a security proof for that protocol. The security proof for the overall protocol is straightforward if the Σ protocol proves a statement that implies (9) while having special-soundness and zero-knowledge properties. The Bulletproof extractor simply extracts the openings of the V's from the Σ protocol and otherwise proceeds as described in [BBB+18]. The simulator uses the Σ protocol's simulator to generate a valid looking Σ protocol as a sub-routine.

We now proceed by presenting two Σ protocols that are vital for Zether.

Burn proof. Σ protocol for proving Statement $\mathsf{st_{Burn}}$

Prover	**Verifier**
$k_{\mathsf{sk}} \leftarrow\!\!\$\ \mathbb{Z}_q$	
$A_y = g^{k_{\mathsf{sk}}}$	
$A_{C_R} = C_R^{k_{\mathsf{sk}}}$	
$A_u = g_{\mathsf{epoch}}^{k_{\mathsf{sk}}}$	

$$\xrightarrow{\quad A_y, A_{C_R}, A_u \quad}$$

$$c \leftarrow\!\!\$\ \mathbb{Z}_q$$

$$\xleftarrow{\quad c \quad}$$

$$s_{\mathsf{sk}} = k_{\mathsf{sk}} + c \cdot \mathsf{sk}$$

$$\xrightarrow{\quad s_{\mathsf{sk}} \quad}$$

$$g^{s_{\mathsf{sk}}} = A_y \cdot y^c$$
$$C_R^{s_{\mathsf{sk}}} = A_{C_R} \cdot (\frac{C_L}{g^b})^c$$
$$g_{\mathsf{epoch}}^{s_{\mathsf{sk}}} = A_u \cdot u^c$$

Proof sketch. We will show that the sigma protocol is perfectly complete, honest-verifier zero-knowledge and has special-soundness. Completeness is immediate. For zero-knowledge we build a simulator S that constructs valid and indistinguishable transcripts given a valid statement $(y, C_L, C_R, u, b, g, g_{\mathsf{epoch}})$ and access to the verifier's state. The simulator will first samples a random challenge c a random s_{sk} and computes $A_y = g^{s_{\mathsf{sk}}} y^{-c}$, $A_{C_R} = C_R^{s_{\mathsf{sk}}} (\frac{C_L}{g^b})^{-c}$ and $A_u = g_{\mathsf{epoch}}^{s_{\mathsf{sk}}} u^{-c}$. If the verifier is honest, i.e. generates random challenges then c, s_{sk} are uniformly distributed and A_y, A_{C_R}, A_u form DDH tuples. The simulated transcripts are identically distributed. To prove special-soundness we build an extractor that can compute the witness from two accepting transcripts with the same first round message A_y, A_{C_R}, A_u. The transcripts also contain (c, s_{sk}) and (c', s'_{sk}) respectively. If both transcripts are accepting then the extractor can output $\hat{\mathsf{sk}} = \frac{s_{\mathsf{sk}} - s'_{\mathsf{sk}}}{c - c'}$ as a valid witness. We can directly deduce from the verification equations that $g^{\hat{\mathsf{sk}}} = y \wedge C_R^{\mathsf{sk}} = \frac{C_L}{g^b} \wedge g_{\mathsf{epoch}}^{\hat{\mathsf{sk}}} = u$

47

Σ-Bullets ConfTransfer proof. We will now describe how exactly we use the Σ Bullets construction to create an efficient proof for $\mathsf{st_{Transfer}}$ the statement which proofs that a ConfTransfer transaction is valid. We will use Bulletproofs to perform the range proofs and use a sigma protocol to proof that the balances are properly encrypted. The conjunction of these two is $\mathsf{st_{ConfTransfer}}$.

The Σ protocol takes as input the senders public key y the receiver's public key $\hat{y}$ and an encryption of the senders balance *after* the transfer $C_{L,n} = \frac{C_L}{C}, C_{R,n} = \frac{C_R}{D}$. Further it takes the encryption of the in and outgoing amounts as input, i.e. $C, D, \overline{C}$. Then the bulletproof protocol is run as described above. The Σ then also takes in T the commitment to $t(X)$ as well as an opening of it at the challenge x: $(\hat{t}, \tau)$. The protocol Note that it is important that the Σ protocol is run after the Bulletproofs protocol. In the non-interactive variant this means that the whole Bulletproofs transcript is also hashed in order to generate the Σ protocol challenge.

$$\left\{ (y, \overline{y}, C_{L,n}, C_{R,n}, C, D, \overline{C}, z, \hat{t}, \delta(y,z), \tau; \mathsf{sk}, b^\star, b', r) : \right.$$
$$C = g^{b^\star} y^r \wedge \overline{C} = g^{b^\star} \overline{y}^r \wedge D = g^r \wedge$$
$$C_{L,n} = g^{b'} C_{R,n}^{\mathsf{sk}} \wedge g^{\mathsf{sk}} = y \wedge$$
$$\left. t = \hat{t} - \delta(y,z) \wedge g^{t - b^\star \cdot z^2 - b' \cdot z^3} h^\tau = T_{1,2} \right\} \quad (10)$$

Proof Sketch. We now provide a sketch of our Zether-Σ protocol is secure and is a proof of

Σ-Bullets ConfTransfer proof. We will now describe how exactly we use the Σ Bullets construction to create an efficient proof for $\mathsf{st_{Transfer}}$ the statement which proofs that a ConfTransfer transaction is valid. We will use Bulletproofs to perform the range proofs and use a sigma protocol to proof that the balances are properly encrypted. The conjunction of these two is $\mathsf{st_{ConfTransfer}}$.

The Σ protocol takes as input the senders public key y the receiver's public key $\hat{y}$ and an encryption of the senders balance *after* the transfer $C_{L,n} = \frac{C_L}{C}, C_{R,n} = \frac{C_R}{D}$. Further it takes the encryption of the in and outgoing amounts as input, i.e. $C, D, \overline{C}$. Then the bulletproof protocol is run as described above. The Σ then also takes in T the commitment to $t(X)$ as well as an opening of it at the challenge x: $(\hat{t}, \tau)$. The protocol Note that it is important that the Σ protocol is run after the Bulletproofs protocol. In the non-interactive variant this means that the whole Bulletproofs transcript is also hashed in order to generate the Σ protocol challenge.

$$\left\{ (y, \overline{y}, C_{L,n}, C_{R,n}, C, D, \overline{C}, z, \hat{t}, \delta(y,z), \tau; \mathsf{sk}, b^\star, b', r) : \right.$$
$$C = g^{b^\star} y^r \wedge \overline{C} = g^{b^\star} \overline{y}^r \wedge D = g^r \wedge$$
$$C_{L,n} = g^{b'} C_{R,n}^{\mathsf{sk}} \wedge g^{\mathsf{sk}} = y \wedge$$
$$\left. t = \hat{t} - \delta(y,z) \wedge g^{t - b^\star \cdot z^2 - b' \cdot z^3} h^\tau = T_{1,2} \right\} \quad (10)$$

Proof Sketch. We now provide a sketch of our Zether-Σ protocol is secure and is a proof of

knowledge for Relation (10). The protocol is honest verifier zero knowledge because there exists a simulator that can simulate verifying transcripts without access to the witness. The simulator generates a random challenge c and random $s_{\mathsf{sk}}, s_r, s_b$. He then computes $A_y, A_D, A_b, A_{\hat{y}}$ and A_t according to the verification equations. Note that they will be identically distributed to the honestly generated ones.

We prove that the protocol is a proof of knowledge by showing that we can build an extractor. The extractor rewinds the sigma protocol once to receive two accepting transcripts with different challenges and the same first message. Let $c_2, s_{\mathsf{sk},2}, s_{r,2}, s_{b,2}$ be the second transcript. From them he computes $\mathsf{sk} = \frac{s_{\mathsf{sk}} - s_{\mathsf{sk},2}}{c - c_2}, r = \frac{s_r - s_{r,2}}{c - c_2}, b = \frac{s_b - s_{b,2}}{c - c_2}$. From the verification equations we can deduce that $y = g^{\mathsf{sk}}, D^r, g^b = (\frac{C}{D^{\mathsf{sk}}})^{z^2}(\frac{C_{L,n}}{C_{R,n}^{\mathsf{sk}}})^{z^3}$ Further we also have that $g^{\hat{t}} = g^{b + \delta(y,z)} T_{1,2}$. In order to extract $b^\star$ and b' we need to rewind the whole Σ-Bullets protocol twice to get three executions with different zs: (z_1, z_2, z_3). Using the same extraction procedure for the Σ protocol we get the extracted witnesses $(\mathsf{sk}_i, r_i, b_i), i \in \{1, 2\}$. First note that $\mathsf{sk}_1 = \mathsf{sk}_2$ since $g^{\mathsf{sk}_1} = g^{\mathsf{sk}_2} = y$. We can now form the equations:

$$g^{b_1} = (\frac{C}{D^{\mathsf{sk}}})^{z_1^2}(\frac{C_{L,n}}{C_{R,n}^{\mathsf{sk}}})^{z_1^3}$$

$$g^{b_2} = (\frac{C}{D^{\mathsf{sk}}})^{z_2^2}(\frac{C_{L,n}}{C_{R,n}^{\mathsf{sk}}})^{z_2^3}$$

One can now easily find a linear combination of these equations to compute $b^\star$ such that $g^{b^\star} = \frac{C}{D^{\mathsf{sk}}}$ and b' such that $g^{b'} = \frac{C_{L,n}}{C_{R,n}^{\mathsf{sk}}}$. This shows that we can successfully extract a witness $(\mathsf{sk}, b^\star, b', r)$ such that the statement $(y, \overline{y}, C_{L,n}, C_{R,n}, C, D, \overline{C}, z, \hat{t}, \delta(y,z), \tau; \mathsf{sk}, b^\star, b', r)$ is in Relation (10).

G.1 Signatures

Zether not only uses zero-knowledge proofs but also heavily relies on signatures. Instead of instantiating a separate signature scheme we can leverage our zero-knowledge proofs to also provide signature functionality. All of the ZK-proofs in our instantiation of Zether are derived from interactive proofs and then transformed to non-interactive proofs using the Fiat-Shamir heuristic [FS87, BCS16]. The Fiat-Shamir heuristic and its extension to multi-round protocol transform an interactive public-coin proof into a non-interactive proof by generating the verifiers' messages from the hash of the transcript. There exists a simple transformation that creates a signature scheme from such a proof system [AABN02]. Concretely, if the prover shows knowledge of a private key and then appends the message to the transcript before generating the challenge, then the proof also acts as a signature. This leads to signatures that can be generated and verified at almost no additional cost.