Zcash Protocol Specification
Version 2.0-draft-2

Sean Bowe — Daira Hopwood — Taylor Hornby

February 25, 2016

Contents

1 Introduction

Zcash is an implementation of the *Decentralized Anonymous Payment* scheme **Zerocash** [2] with some adjustments to terminology, functionality and performance. It bridges the existing *transparent* payment scheme used by **Bitcoin** with a *confidential* payment scheme protected by zero-knowledge succinct non-interactive arguments of knowledge (*zk-SNARKs*).

Changes from the original **Zerocash** are highlighted in magenta.

2 Caution

Zcash security depends on consensus. Should your program diverge from consensus, its security is weakened or destroyed. The cause of the divergence doesn't matter: it could be a bug in your program, it could be an error in this documentation which you implemented as described, or it could be you do everything right but other software on the network behaves unexpectedly. The specific cause will not matter to the users of your software whose wealth is lost.

Having said that, a specification of *intended* behaviour is essential for security analysis, understanding of the protocol, and maintenance of Zcash Core and related software. If you find any mistake in this specification, please contact TODO: address. While the production **Zcash** network has yet to be launched, please feel free to do so in public even if you believe the mistake may indicate a security weakness.

3 Conventions

3.1 Integers, Bit Sequences, and Endianness

All integers visible in **Zcash**-specific encodings are unsigned, have a fixed bit length, and are encoded as big-endian (except in the definition of AEAD_CHACHA20_POLY1305 [6] which internally uses length fields encoded as little-endian).

In bit layout diagrams, each box of the diagram represents a sequence of bits. If the content of the box is a byte sequence, it is implicitly converted to a sequence of bits using big endian order. The bit sequences are then concatenated in the order shown from left to right, and the result is converted to a sequence of bytes, again using big-endian order.

Nathan: An example would help here. It would be illustrative if it had a few differently-sized fields.

$\mathtt{Leading}_k(x)$, where k is an integer and x is a bit sequence, returns the leading (initial) k bits of its input.

The notation 1..N, used as a subscript, means the sequence of values with indices 1 through N inclusive. For example, $\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},1..\mathrm{N}^{\mathsf{new}}}$ means the sequence $[\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},1}, \mathsf{a}^{\mathsf{new}}_{\mathsf{pk},2}, \ldots\ \mathsf{a}^{\mathsf{new}}_{\mathsf{pk},\mathrm{N}^{\mathsf{new}}}]$.

3.2 Cryptographic Functions

CRH is a collision-resistant hash function. In **Zcash**, the *SHA-256 compression* function is used which takes a 512-bit block and produces a 256-bit hash. This is different from the *SHA-256* function, which hashes arbitrary-length strings. [7]

PRF_x is a pseudo-random function seeded by x. Four *independent* PRF_x are needed in our scheme: $\mathsf{PRF}^{\mathsf{addr}}_x$, $\mathsf{PRF}^{\mathsf{sn}}_x$, $\mathsf{PRF}^{\mathsf{pk}}_x$, and PRF^{ρ}_x. It is required that $\mathsf{PRF}^{\mathsf{sn}}_x$ and PRF^{ρ}_x be collision-resistant across all x — i.e. it should not be feasible to find $(x, y) \neq (x', y')$ such that $\mathsf{PRF}^{\mathsf{sn}}_x(y) = \mathsf{PRF}^{\mathsf{sn}}_{x'}(y')$, and similarly for PRF^{ρ}.

In **Zcash**, the *SHA-256 compression* function is used to construct all four of these functions. The bits `00`, `01`, `10`, and `11` are included (respectively) within the blocks that are hashed, ensuring that the functions are independent.

Nathan: Note: If we change input or output arity (i.e. $\mathrm{N}^{\mathsf{old}}$ or $\mathrm{N}^{\mathsf{new}}$), we need to be aware of how it is associated with this bit-packing.

$$\mathsf{a_{vk}} := \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{sk}}}(0) = \mathsf{CRH}\left(\boxed{256 \text{ bit } \mathsf{a_{sk}}}\boxed{0}\boxed{0}\boxed{0^{252}}\boxed{0}\boxed{0}\right)$$

$$\mathsf{a_{pk}} := \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{vk}}}(1) = \mathsf{CRH}\left(\boxed{256 \text{ bit } \mathsf{a_{vk}}}\boxed{0}\boxed{0}\boxed{0^{252}}\boxed{0}\boxed{1}\right)$$

$$\mathsf{sk_{enc}}' := \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{sk}}}(2) = \mathsf{CRH}\left(\boxed{256 \text{ bit } \mathsf{a_{sk}}}\boxed{0}\boxed{0}\boxed{0^{252}}\boxed{1}\boxed{0}\right)$$

$$\mathsf{sk_{enc}} := \mathsf{clamp}_{\mathsf{Curve25519}}(\mathsf{sk_{enc}}')$$

$$\mathsf{sn} := \mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a_{sk}}}(\rho) = \mathsf{CRH}\left(\boxed{256 \text{ bit } \mathsf{a_{sk}}}\boxed{0}\boxed{1}\boxed{\mathtt{Leading}_{254}(\rho)}\right)$$

$$\mathsf{h}_i := \mathsf{PRF}^{\mathsf{pk}}_{\mathsf{a_{sk}}}(i, \mathsf{h_{Sig}}) = \mathsf{CRH}\left(\boxed{256 \text{ bit } \mathsf{a_{sk}}}\boxed{1}\boxed{0}\boxed{i\text{-}1}\boxed{\mathtt{Leading}_{253}(\mathsf{h_{Sig}})}\right)$$

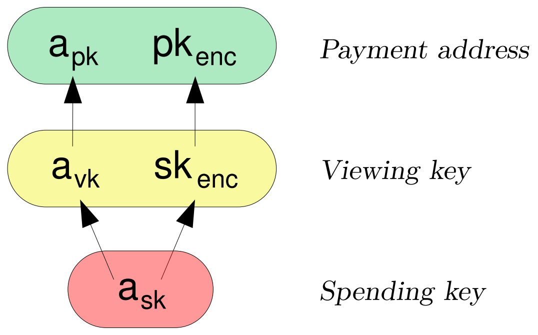
$$\rho_i^{\mathsf{new}} := \mathsf{PRF}^{\rho}_{\varphi}(i, \mathsf{h_{Sig}}) = \mathsf{CRH}\left(\boxed{256 \text{ bit } \varphi}\boxed{1}\boxed{1}\boxed{i\text{-}1}\boxed{\mathtt{Leading}_{253}(\mathsf{h_{Sig}})}\right)$$

Daira: Should we instead define ρ to be 254 bits and $\mathsf{h_{Sig}}$ to be 253 bits?

3.3 Payment Addresses, Viewing Keys, and Spending Keys

A *key tuple* $(\mathsf{addr_{sk}}, \mathsf{addr_{vk}}, \mathsf{addr_{pk}})$ is generated by users who wish to receive payments under this scheme. The *viewing key* $\mathsf{addr_{vk}}$ is derived from the *spending key* $\mathsf{addr_{sk}}$, and the *payment address* $\mathsf{addr_{pk}}$ is derived from the *viewing key*.

The following diagram depicts the relations between key components. Arrows point from a component to any other component(s) that can be derived from it.



$\mathsf{a_{pk}}$ $\mathsf{pk_{enc}}$
Payment address
$\mathsf{a_{vk}}$ $\mathsf{sk_{enc}}$
Viewing key
$\mathsf{a_{sk}}$
Spending key

Note that a *spending key* holder can derive the other components, and a *viewing key* holder can derive $(\mathsf{a_{pk}}, \mathsf{pk_{enc}})$, even though these components are not formally part of the respective keys. Implementations MAY cache these derived components, provided that they are deleted if the corresponding source component is deleted.

The composition of *payment addresses*, *viewing keys*, and *spending keys* is a cryptographic protocol detail that should not normally be exposed to users. However, user-visible operations should be provided to:

- obtain a *payment address* from a *viewing key*; and
- obtain a *payment address* or *viewing key* from a *spending key*.

Each key component, i.e. each of $\mathsf{a_{pk}}$, $\mathsf{pk_{enc}}$, $\mathsf{a_{vk}}$, $\mathsf{sk_{enc}}$, and $\mathsf{a_{sk}}$, is a sequence of 32 bytes. $\mathsf{a_{pk}}$, $\mathsf{a_{vk}}$, and $\mathsf{sk_{enc}}$ are derived as follows:

$$\begin{aligned}
\mathsf{a_{vk}} &:= \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{sk}}}(0) \\
\mathsf{a_{pk}} &:= \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{vk}}}(1) \\
\mathsf{sk_{enc}} &:= \mathsf{clamp}_{\mathsf{Curve25519}}(\mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{sk}}}(2))
\end{aligned}$$

$\mathsf{clamp}_{\mathsf{Curve25519}}$ performs the clamping of Curve25519 private key bits, and $\mathsf{Curve25519}$ performs point multiplication, both as defined in [3].

Let $\mathsf{pk_{enc}} := \mathsf{Curve25519}(\mathsf{sk_{enc}})$, i.e. the public key corresponding to the private key $\mathsf{sk_{enc}}$.

Users can accept payment from multiple parties with a single $\mathsf{addr_{pk}}$ and the fact that these payments are destined to the same payee is not revealed on the blockchain, even to the paying parties. *However* if two parties collude to compare a $\mathsf{addr_{pk}}$ they can trivially determine they are the same. In the case that a payee wishes to prevent this they should create a distinct *payment address* for each payer.

3.4 Coins

A *coin* (denoted $\mathbf{c}$) is a tuple $(\mathsf{a_{pk}}, \mathsf{v}, \mathsf{\rho}, \mathsf{r})$ which represents that a value v is spendable by the recipient who holds the *authorization* key pair $(\mathsf{a_{pk}}, \mathsf{a_{sk}})$ such that $\mathsf{a_{pk}} = \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a_{sk}}}(0)$.

r is randomly generated by the sender. $\mathsf{\rho}$ is generated from a random seed φ using $\mathsf{PRF}^{\rho}_{\varphi}$. Only a commitment to these values is disclosed publicly, which allows the tokens r and $\mathsf{\rho}$ to blind the value and recipient *except* to those who possess these tokens.

3.4.1 In-band secret distribution

In order to transmit the secret v, $\mathsf{\rho}$, and r (necessary for the recipient to later spend) and also a *memo field* to the recipient *without* requiring an out-of-band communication channel, the *transmission* public key $\mathsf{pk_{enc}}$ is used to encrypt these secrets. The recipient's possession of the associated $(\mathsf{addr_{pk}}, \mathsf{addr_{sk}})$ (which contains both $\mathsf{a_{pk}}$ and $\mathsf{sk_{enc}}$) is used to reconstruct the original *coin* and *memo field*. To also transmit these values to a *viewing key* holder for outgoing *Pour transfers*, the *disclosure key* $\mathsf{a_{vk}}$ is used to symmetrically encrypt them, and also to encrypt the ephemeral secret and address public keys (to allow the *viewing key* holder to check whether the other encryptions are valid). All of these encryptions are combined to form a *transmitted coins ciphertext*.

Let $\mathsf{SymEncrypt_K}(\mathbf{P})$ be the $\mathsf{AEAD\_CHACHA20\_POLY1305}$ encryption [6] of plaintext $\mathbf{P}$ with empty "additional data", empty nonce, and key K.

Let $\mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},1..\mathrm{N}^{\mathsf{new}}}$ be the Curve25519 public keys for the intended recipient addresses of each new *coin*, let $\mathsf{a_{vk}}$ be the sender's *disclosure key*, and let $\mathbf{P}1..\mathrm{N}^{\mathsf{new}}$ be the *coin plaintexts*.

Define:

$$\mathsf{KDF}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i) := \mathtt{SHA256}\left(\begin{array}{|c|c|c|c|}\hline 256 \text{ bit } \mathsf{dhsecret}_i & 256 \text{ bit } \mathsf{epk} & 256 \text{ bit } \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i} & 8 \text{ bit } i-1 \\ \hline\end{array}\right)$$

$$\mathbf{P}^{\mathsf{shared}} := \begin{array}{|c|c|c|c|}\hline 256 \text{ bit } \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},1} & \cdots & 256 \text{ bit } \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},\mathrm{N}^{\mathsf{new}}} & 256 \text{ bit } \mathsf{esk} \\ \hline\end{array}$$

Then to encrypt:

- Generate a new Curve25519 (public, private) key pair: $(\mathsf{epk}, \mathsf{esk})$.
- For i in $\{1..\mathrm{N}^{\mathsf{new}}\}$,
  - Let $\mathsf{dhsecret}_i := \mathsf{Curve25519}(\mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, \mathsf{esk})$.

  - Let $\mathsf{K}_i^{\mathsf{enc}} := \mathsf{KDF}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i)$.
  - Let $\mathbf{C}_i^{\mathsf{enc}} := \mathsf{SymEncrypt}_{\mathsf{K}_i^{\mathsf{enc}}}(\mathbf{P}_i^{\mathsf{enc}})$.

- Let $\mathsf{K}^{\mathsf{shared}} := \ldots$.
- Let $\mathbf{C}^{\mathsf{shared}} := \mathsf{SymEncrypt}_{\mathsf{K}^{\mathsf{shared}}}(\mathbf{P}^{\mathsf{shared}})$.
- For i in $\{1..\mathrm{N}^{\mathsf{old}}\}$,
  - Let $\mathbf{C}_i^{\mathsf{disclose}} := \mathsf{SymEncrypt}_{\mathsf{a}_{\mathsf{vk}}i}(\mathsf{K}^{\mathsf{shared}})$.

The resulting *transmitted coins ciphertext* is $(\mathsf{epk}, \mathbf{C}^{\mathsf{enc}}_{1..\mathrm{N}^{\mathsf{new}}}, \mathbf{C}^{\mathsf{disclose}}_{1..\mathrm{N}^{\mathsf{old}}}, \mathbf{C}^{\mathsf{shared}})$.

Let $(\mathsf{pk}_{\mathsf{enc}}, \mathsf{sk}_{\mathsf{enc}})$ be the recipient's Curve25519 (public, private) key pair, and let $\mathsf{cm}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}$ be the coin commitments of each output coin. Then for each i in $\{1..\mathrm{N}^{\mathsf{new}}\}$, the recipient will attempt to decrypt that ciphertext component as follows:

- Let $\mathsf{dhsecret}_i := \mathsf{Curve25519}(\mathsf{epk}, \mathsf{sk}_{\mathsf{enc}})$.
- Return $\texttt{DecryptCoin}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i, \mathbf{C}_i^{\mathsf{enc}}, \mathsf{cm}_i^{\mathsf{new}})$.

$\texttt{DecryptCoin}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i, \mathbf{C}_i^{\mathsf{enc}}, \mathsf{cm}_i^{\mathsf{new}})$ is defined as follows:

- Let $\mathsf{K}_i^{\mathsf{enc}} := \mathsf{KDF}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i)$.
- Let $\mathbf{P}_i^{\mathsf{enc}} := \mathsf{SymDecrypt}_{\mathsf{K}_i^{\mathsf{enc}}}(\mathbf{C}_i^{\mathsf{enc}})$.
- If $\mathbf{P}_i^{\mathsf{enc}} = \bot$, return $\bot$.
- Extract $\mathbf{c}_i := (\mathsf{a}_{\mathsf{pk}}, \mathsf{v}, \rho, \mathsf{r})$ and memo_i from $\mathbf{P}_i^{\mathsf{enc}}$.
- If $\texttt{CoinCommitment}(\mathbf{c}_i) \neq \mathsf{cm}_i^{\mathsf{new}}$, return $\bot$, else return $(\mathbf{c}_i, \mathsf{memo}_i)$.

Note that this corresponds to step 3 (b) i. and ii. (first bullet point) of the Receive algorithm shown in Figure 2 of [2].

To test whether a *coin* is unspent in a particular *blockchain view* also requires the *authorization* private key a_{sk}; the coin is unspent if and only if $\mathsf{sn} = \mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a}_{\mathsf{sk}}}(\rho)$ is not in the *spent serial number set* for that *blockchain view*.

Note that a coin may change from being unspent to spent on a given *blockchain view*, as transactions are added to that view. Also, blockchain reorganisations may cause the transaction in which a coin was output to no longer be on the consensus blockchain.

Let a_{vk} be a *viewing key* holder's *disclosure key*. Then for each *Pour description* in its *blockchain view*, the *viewing key* holder will attempt to decrypt the corresponding *transmitted coins ciphertext* as follows:

1. Set $\mathbf{P}^{\mathsf{shared}} := \bot$.
2. For i in $\{1..\mathrm{N}^{\mathsf{new}}\}$,
   - Let $\mathsf{K}_i^{\mathsf{shared}} := \mathsf{SymDecrypt}_{\mathsf{a}_{\mathsf{vk}}}(\mathbf{C}_i^{\mathsf{disclose}}, \mathsf{tag}_i)$.
   - If $\mathsf{K}_i^{\mathsf{shared}} = \bot$ then continue with the next i.
   - Let $\mathbf{P}_i^{\mathsf{shared}} := \mathsf{SymDecrypt}_{\mathsf{K}_i^{\mathsf{shared}}}(\mathbf{C}^{\mathsf{shared}})$.
   - If $\mathbf{P}_i^{\mathsf{shared}} = \bot$ then continue with the next i.
   - Set $\mathbf{P}^{\mathsf{shared}} := \mathbf{P}_i^{\mathsf{shared}}$ and exit the loop.

3. If $\mathbf{P}^{\mathsf{shared}} = \bot$ (i.e. it was not set in the loop), then this transaction does not contain any information decryptable by the *viewing key*; return $\bot$.
4. Extract $\mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},1..\mathrm{N}^{\mathsf{new}}}$ and esk from $\mathbf{P}^{\mathsf{shared}}$.
5. For i in $\{1..\mathrm{N}^{\mathsf{new}}\}$,
   - Let $\mathsf{dhsecret}_i := \mathsf{Curve25519}(\mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, \mathsf{esk})$.
   - Let $\mathbf{c}_i := \mathtt{DecryptCoin}(\mathsf{dhsecret}_i, \mathsf{epk}, \mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},i}, i, \mathbf{C}^{\mathsf{enc}}_i, \mathsf{cm}^{\mathsf{new}}_i)$.
6. Return $(\mathbf{c}_{1..\mathrm{N}^{\mathsf{new}}}, \mathsf{memo}_{1..\mathrm{N}^{\mathsf{new}}})$.

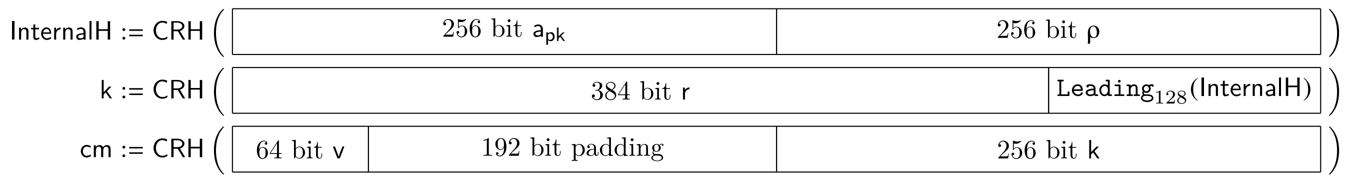
If a party holds more than one *viewing key*, it may optimize the above procedure by performing the loop in step 2 for the a_{vk} of each *viewing key*. It may be assumed that the first $\mathbf{P}^{\mathsf{shared}}_i$ that decrypts correctly is the one that should be used in step 4 onward. (However, additional information is provided by which *viewing key* was able to decrypt each $\mathbf{C}^{\mathsf{disclose}}_i$.)

The public key encryption used in this part of the protocol is based loosely on the crypto_box_seal algorithm defined in libsodium [5], but with the following differences:

- The same ephemeral key is used for all encryptions to the recipient keys in a given *Pour description*.
- The nonce for each ciphertext component depends on the index i. The particular nonce construction is chosen so that a known-nonce distinguisher for Salsa20 would not directly lead to a break of the IK-CCA (key privacy) property.
- `SHA256` (the full hash, not the compression function) is used instead of blake2b.
- The ephemeral secret esk is included together with the *transmission* public keys of the recipients, encrypted to the *disclosure key*. This allows a *viewing key* holder to check whether the indicated recipients would be able to decrypt a given component, and if so to decrypt the memo field. (We do not rely on this to ensure that a *viewing key* holder can decrypt the other components of the output coins; instead, those are symmetrically encrypted to the *viewing key* and the correctness of this encryption is checked by the *`POUR` circuit*.)

3.4.2 Coin Commitments

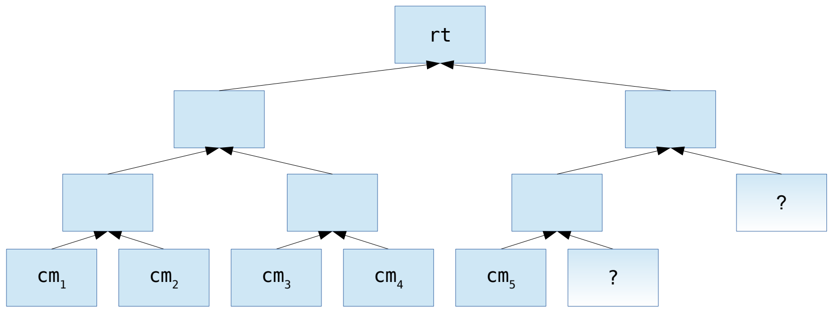
The underlying v and a_{pk} are blinded with ρ and r using the collision-resistant hash function CRH in a multi-layered process. The resulting hash $\mathsf{cm} = \mathtt{CoinCommitment}(\mathbf{c})$.



3.4.3 Serial numbers

A *serial number* (denoted sn) equals $\mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a}_{\mathsf{sk}}}(\rho)$. A *coin* is spent by proving knowledge of ρ and a_{sk} in zero knowledge while disclosing sn, allowing sn to be used to prevent double-spending.

3.5 Coin Commitment Tree



The *coin commitment tree* is an *incremental merkle tree* of depth d used to store *coin commitments* that *Pour transfers* produce. Just as the *unspent transaction output set* (UTXO) used in Bitcoin, it is used to express the existence of value and the capability to spend it. However, unlike the UTXO, it is *not* the job of this tree to protect against double-spending, as it is append-only.

Blocks in the blockchain are associated (by all nodes) with the root of this tree after all of its constituent *Pour descriptions*' *coin commitments* have been entered into the tree associated with the previous block.

3.6 Spent Serials Map

Transactions insert *serial numbers* into a *spent serial numbers map* which is maintained alongside the UTXO by all nodes.

Eli: a tx is just a string, so it doesn't insert anything. Rather, nodes process tx's and the "good" ones lead to the addition of serials to the spent serials map.

Transactions that attempt to insert a *serial number* into this map that already exists within it are invalid as they are attempting to double-spend.

Eli: After defining *transaction*, one should define what a *legal tx* is (this definition depends on a particular blockchain [view]) and only then can one talk about "attempts" of transactions, and insertions of serial numbers into the spent serials map.

3.7 The Blockchain

At a given point in time, the *blockchain view* of each *full node* consists of a sequence of one or more valid *blocks*. Each *block* consists of a sequence of one or more *transactions*. In a given node's *blockchain view*, *treestates* are chained in an obvious way:

- The input *treestate* of the first *block* is the empty *treestate*.
- The input *treestate* of the first *transaction* of a *block* is the final *treestate* of the immediately preceding *block*.
- The input *treestate* of each subsequent *transaction* in a *block* is the output *treestate* of the immediately preceding *transaction*.
- The final *treestate* of a *block* is the output *treestate* of its last *transaction*.

An *anchor* is a Merkle tree root of a *treestate*, and uniquely identifies that *treestate* given the assumed security properties of the Merkle tree's hash function.

Each *transaction* is associated with a sequence of *Pour descriptions*. TODO: They also have a transparent value flow that interacts with the Pour $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ and $\mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}$. Inputs and outputs are associated with a value.

The total value of the outputs must not exceed the total value of the inputs.

The *anchor* of the first *Pour description* in a *transaction* must refer to some earlier *block*'s final *treestate*.

The *anchor* of each subsequent *Pour description* may refer either to some earlier *block*'s final *treestate*, or to the output *treestate* of the immediately preceding *Pour description*.

These conditions act as constraints on the blocks that a *full node* will accept into its *blockchain view*.

We rely on Bitcoin-style consensus for *full nodes* to eventually converge on their views of valid *blocks*, and therefore of the sequence of *treestates* in those *blocks*.

Value pool Transaction inputs insert value into a *value pool*, and transaction outputs remove value from this pool. The remaining value in the pool is available to miners as a fee.

4 Pour Transfers and Descriptions

A *Pour description* is data included in a *block* that describes a *Pour transfer*, i.e. a confidential value transfer. This kind of value transfer is the primary **Zerocash**-specific operation performed by transactions; it uses, but should not be confused with, the *POUR circuit* used for the *zk-SNARK* proof and verification.

A *Pour transfer* spends $\mathrm{N}^{\mathsf{old}}$ *coins* $\mathbf{c}^{\mathsf{old}}_{1..\mathrm{N}^{\mathsf{old}}}$ and creates $\mathrm{N}^{\mathsf{new}}$ *coins* $\mathbf{c}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}$. **Zcash** transactions have an additional field `vpour`, which is a sequence of *Pour descriptions*.

Each *Pour description* consists of:

`vpub_old` which is a value $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ that the *Pour transfer* removes from the value pool.

`vpub_new` which is a value $\mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}$ that the *Pour transfer* inserts into the value pool.

`anchor` which is a merkle root rt of the *coin commitment tree* at some block height in the past, or the merkle root produced by a previous pour in this transaction. Sean: We need to be more specific here.

`scriptSig` which is a *script* that creates conditions for acceptance of a *Pour description* in a transaction.

`scriptPubKey` which is a *script* used to satisfy the conditions of the `scriptSig`.

`serials` which is an $\mathrm{N}^{\mathsf{old}}$ size sequence of serials $\mathsf{sn}^{\mathsf{old}}_{1..\mathrm{N}^{\mathsf{old}}}$.

`commitments` which is a $\mathrm{N}^{\mathsf{new}}$ size sequence of *coin commitments* $\mathsf{cm}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}$.

`ephemeralKey` which is a Curve25519 public key epk.

`encCiphertexts` which is a $\mathrm{N}^{\mathsf{new}}$ size sequence of ciphertext components, $\mathbf{C}^{\mathsf{enc}}_{1..\mathrm{N}^{\mathsf{new}}}$.

`discloseCiphertexts` which is a $\mathrm{N}^{\mathsf{old}}$ size sequence of ciphertext components, $\mathbf{C}^{\mathsf{disclose}}_{1..\mathrm{N}^{\mathsf{old}}}$.

`sharedCiphertext` which is the ciphertext component $\mathbf{C}^{\mathsf{shared}}$.
(The preceding four fields together form the *transmitted coins ciphertext*.)

`vmacs` which is a $\mathrm{N}^{\mathsf{old}}$ size sequence of message authentication tags $\mathsf{h}_{1..\mathrm{N}^{\mathsf{old}}}$ that bind $\mathsf{h}_{\mathsf{Sig}}$ to each a_{sk} of the *Pour description*.

`zkproof` which is the zero-knowledge proof $\pi_{\mathtt{POUR}}$.

Computation of $\mathsf{h_{Sig}}$ Given a *Pour description*, we define:

$$\mathsf{h_{Sig}} := \mathtt{SHA256}\left(\begin{array}{|c|c|c|c|c|}\hline \mathbf{0x00} & 256 \text{ bit } \mathsf{sn}^{\mathsf{old}}_{0} & \cdots & 256 \text{ bit } \mathsf{sn}^{\mathsf{old}}_{\mathrm{N}^{\mathsf{old}}-1} & \mathtt{scriptPubKey} \\ \hline \end{array}\right)$$

Merkle root validity A *Pour description* is valid if rt is a *coin commitment tree* root found in either the blockchain or a merkle root produced by inserting the *coin commitments* of a previous *Pour description* in the transaction to the *coin commitment tree* identified by that previous *Pour description*'s *anchor*.

Non-malleability A *Pour description* is valid if the script formed by appending `scriptPubKey` to `scriptSig` returns *true*. The `scriptSig` is cryptographically bound to $\pi_{\mathtt{POUR}}$.

Balance A *Pour transfer* can be seen, from the perspective of the transaction, as an input and an output simultaneously. $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ takes value from the value pool and $\mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}$ adds value to the value pool. As a result, $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ is treated like an *output* value, whereas $\mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}$ is treated like an *input* value.

Note that unlike original **Zerocash** [2], **Zcash** does not have a distinction between Mint and Pour transfers. The addition of $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}$ to a *Pour description* subsumes the functionality of Mint. Also, *Pour descriptions* are indistinguishable regardless of the number of real input *coins*.

Commitments and Serials A *transaction* that contains one or more *Pour descriptions*, when entered into the blockchain, appends to the *coin commitment tree* with all constituent *coin commitments*. All of the constituent *serial numbers* are also entered into the *spent serial numbers map* of the *blockchain view and mempool*. A *transaction* is not valid if it attempts to add a *serial number* to the *spent serial numbers map* that already exists in the map.

4.1 Pour Circuit and Proofs

In **Zcash**, $\mathrm{N}^{\mathsf{old}}$ and $\mathrm{N}^{\mathsf{new}}$ are both 2.

A valid instance of $\pi_{\mathtt{POUR}}$ assures that given a *primary input* $(\mathsf{rt}, \mathsf{sn}^{\mathsf{old}}_{1..\mathrm{N}^{\mathsf{old}}}, \mathsf{cm}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}, \mathsf{v}^{\mathsf{old}}_{\mathsf{pub}}, \mathsf{v}^{\mathsf{new}}_{\mathsf{pub}}, \mathsf{h_{Sig}}, \mathsf{h}_{1..\mathrm{N}^{\mathsf{old}}})$, a witness of *auxiliary input* $(\mathsf{path}_{1..\mathrm{N}^{\mathsf{old}}}, \mathbf{c}^{\mathsf{old}}_{1..\mathrm{N}^{\mathsf{old}}}, \mathsf{a}^{\mathsf{old}}_{\mathsf{sk},1..\mathrm{N}^{\mathsf{old}}}, \mathbf{c}^{\mathsf{new}}_{1..\mathrm{N}^{\mathsf{new}}}, \varphi)$ exists, where:

for each $i \in \{1..\mathrm{N}^{\mathsf{old}}\}$: $\mathbf{c}^{\mathsf{old}}_i = (\mathsf{a}^{\mathsf{old}}_{\mathsf{pk},i}, \mathsf{v}^{\mathsf{old}}_i, \rho^{\mathsf{old}}_i, \mathsf{r}^{\mathsf{old}}_i)$

for each $i \in \{1..\mathrm{N}^{\mathsf{new}}\}$: $\mathbf{c}^{\mathsf{new}}_i = (\mathsf{a}^{\mathsf{new}}_{\mathsf{pk},i}, \mathsf{v}^{\mathsf{new}}_i, \rho^{\mathsf{new}}_i, \mathsf{r}^{\mathsf{new}}_i)$

The following conditions hold:

Merkle path validity for each $i \in \{1..\mathrm{N}^{\mathsf{old}}\} \mid \mathsf{v}^{\mathsf{old}}_i \neq 0$: path_i must be a valid path of depth d from $\mathtt{CoinCommitment}(\mathbf{c}^{\mathsf{old}}_i)$ to Coin commitment merkle tree root rt.

Balance $\mathsf{v}^{\mathsf{old}}_{\mathsf{pub}} + \sum_{i=1}^{\mathrm{N}^{\mathsf{old}}} \mathsf{v}^{\mathsf{old}}_i = \mathsf{v}^{\mathsf{new}}_{\mathsf{pub}} + \sum_{i=1}^{\mathrm{N}^{\mathsf{new}}} \mathsf{v}^{\mathsf{new}}_i$.

Serial integrity for each $i \in \{1..\mathrm{N}^{\mathsf{new}}\}$: $\mathsf{sn}^{\mathsf{old}}_i = \mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a}^{\mathsf{old}}_{\mathsf{sk},i}}(\rho^{\mathsf{old}}_i)$.

Spend authority for each $i \in \{1..\mathrm{N}^{\mathsf{old}}\}$: $\mathsf{a}^{\mathsf{old}}_{\mathsf{pk},i} = \mathsf{PRF}^{\mathsf{addr}}_{\mathsf{a}^{\mathsf{old}}_{\mathsf{sk},i}}(0)$.

Non-malleability for each $i \in \{1..\mathrm{N}^{\mathsf{old}}\}$: $\mathsf{h}_i = \mathsf{PRF}^{\mathsf{pk}}_{\mathsf{a}^{\mathsf{old}}_{\mathsf{sk},i}}(i, \mathsf{h}_{\mathsf{Sig}})$

Uniqueness of ρ^{new}_i for each $i \in \{1..\mathrm{N}^{\mathsf{new}}\}$: $\rho^{\mathsf{new}}_i = \mathsf{PRF}^{\rho}_{\varphi}(i, \mathsf{h}_{\mathsf{Sig}})$

Commitment integrity for each $i \in \{1..\mathrm{N}^{\mathsf{new}}\}$: $\mathsf{cm}^{\mathsf{new}}_i = \mathtt{CoinCommitment}(\mathbf{c}^{\mathsf{new}}_i)$

5 Encoding Addresses, Private keys, Coins, and Pour descriptions

This section describes how **Zcash** encodes public addresses, private keys, coins, and *Pour descriptions*.

Addresses, keys, and coins, can be encoded as a byte string; this is called the *raw encoding*. This byte string can then be further encoded using Base58Check. The Base58Check layer is the same as for upstream **Bitcoin** addresses [1].

SHA-256 compression function outputs are always represented as strings of 32 bytes.

The language consisting of the following encoding possibilities is prefix-free.

5.1 Transparent Public Addresses

These are encoded in the same way as in **Bitcoin** [1].

5.2 Transparent Private Keys

These are encoded in the same way as in **Bitcoin** [1].

5.3 Confidential Public Addresses

A *payment address* consists of a_{pk} and $\mathsf{pk}_{\mathsf{enc}}$. a_{pk} is a SHA-256 compression function output. $\mathsf{pk}_{\mathsf{enc}}$ is a Curve25519 public key, for use with the encryption scheme defined in section "In-band secret distribution".

5.3.1 Raw Encoding

The raw encoding of a confidential address consists of:

0x92	a_{pk} (32 bytes)	A 32-byte encoding of $\mathsf{pk}_{\mathsf{enc}}$

- A byte, **0x92**, indicating this version of the raw encoding of a **Zcash** public address.
- 32 bytes specifying a_{pk}.
- 32 bytes specifying $\mathsf{pk}_{\mathsf{enc}}$, using the normal encoding of a Curve25519 public key [3].

Daira: check that this lead byte is distinct from other Bitcoin stuff, and produces 'z' as the Base58Check leading character.

Nathan: what about the network version byte?

5.4 Confidential Address Secrets

A confidential address secret consists of $\mathsf{a_{sk}}$ and $\mathsf{sk_{enc}}$. $\mathsf{a_{sk}}$ is a SHA-256 compression function output. $\mathsf{sk_{enc}}$ is a Curve25519 private key, for use with the encryption scheme defined in section "In-band secret distribution".

5.4.1 Raw Encoding

The raw encoding of a confidential address secret consists of, in order:

0x93	$\mathsf{a_{sk}}$ (32 bytes)	$\mathsf{sk_{enc}}$ (32 bytes)

- A byte **0x93** indicating this version of the raw encoding of a **Zcash** private key.
- 32 bytes specifying $\mathsf{a_{sk}}$.
- 32 bytes specifying $\mathsf{sk_{enc}}$.

Daira: check that this lead byte is distinct from other Bitcoin stuff, and produces 'z' as the Base58Check leading character.

Nathan: what about the network version byte?

5.5 Coins

Transmitted coins are stored on the blockchain in encrypted form, together with a *coin commitment* cm.

The *coin plaintexts* associated with a *Pour description* are encrypted to the respective *transmission* keys $\mathsf{pk}^{\mathsf{new}}_{\mathsf{enc},1..\mathrm{N}^{\mathsf{new}}}$, and the result forms a *transmitted coins ciphertext*.

Each *coin plaintext* consists of $(\mathsf{a_{pk}}, \mathsf{v}, \rho, \mathsf{r}, \mathsf{memo})$, where:

- $\mathsf{a_{pk}}$ is a 32-byte *authorization* public key of the recipient.
- v is a 64-bit unsigned integer representing the value of the *coin* in *zatoshi* (1 **ZEC** $= 10^8$ *zatoshi*).
- ρ is a 32-byte $\mathsf{PRF}^{\mathsf{sn}}_{\mathsf{a_{sk}}}$ preimage.
- r is a 48-byte *COMM trapdoor*.
- memo is a 64-byte *memo field* associated with this *coin*.

The usage of the *memo field* is by agreement between the sender and recipient of the *coin*. It should be encoded as a UTF-8 human-readable string [4], padded with zero bytes. Wallet software is expected to strip any trailing zero bytes and then display the resulting UTF-8 string to the recipient user, where applicable. Incorrect UTF-8-encoded byte sequences should be displayed as replacement characters (U+FFFD). This does not preclude uses of the *memo field* by automated software, but specification of such usage is not in the scope of this document.

Note that the value s described as being part of a *coin* in the **Zerocash** paper is not encoded because the instantiation of $\mathsf{COMM_s}$ does not use it.

5.5.1 Raw Encoding

The raw encoding of a *coin plaintext* consists of, in order:

0x00	$\mathsf{a_{pk}}$ (32 bytes)	v (8 bytes)	ρ (32 bytes)	r (48 bytes)	memo (64 bytes)

- A byte **0x00** indicating this version of the raw encoding of a *coin plaintext*.
- 32 bytes specifying $\mathsf{a_{pk}}$.
- 8 bytes specifying a big-endian encoding of v.
- 32 bytes specifying ρ.
- 48 bytes specifying r.
- 64 bytes specifying memo.

6 Pours (within a transaction on the blockchain)

TBD.

Describe case where there are fewer than $\mathrm{N}^{\mathsf{old}}$ real input coins.

7 Transactions

TBD.

8 Differences from the Zerocash paper

- Instead of ECIES, we use an encryption scheme based on $\mathsf{crypto\_box}$, defined in section "In-band secret distribution".
- Faerie Gold fix (TBD).
- The paper defines a coin as a tuple $(\mathsf{a_{pk}}, \mathsf{v}, \rho, \mathsf{r}, \mathsf{s}, \mathsf{cm})$, whereas this specification defines it as $(\mathsf{a_{pk}}, \mathsf{v}, \rho, \mathsf{r})$. This is just a clarification, because the instantiation of $\mathsf{COMM_s}$ in section 5.1 of the paper does not use s, and cm can be computed from the other fields.

9 References

[1] Base58Check encoding. `https://en.bitcoin.it/wiki/Base58Check_encoding`. Accessed: 2016-01-26.

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland) 2014*, pages 459–474. IEEE, 2014.

[3] Daniel Bernstein. Curve25519: new Diffie-Hellman speed records. In *Public Key Cryptography - PKC 2006. Proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26*. Springer-Verlag, 2006. Document ID: 4230efdfa673480fc079449d90f322c0. Date: 2006-02-09. `http://cr.yp.to/papers.html#curve25519`.

[4] The Unicode Consortium. *The Unicode Standard*. The Unicode Consortium, 2015. `http://www.unicode.org/versions/latest/`.

[5] libsodium documentation: Sealed boxes. `https://download.libsodium.org/doc/public-key_cryptography/sealed_boxes.html`. Accessed: 2016-02-01.

[6] Yoav Nir and Adam Langley. Request for Comments 7539: ChaCha20 and Poly1305 for IETF Protocols. Internet Research Task Force (IRTF). `https://tools.ietf.org/html/rfc7539`. As modified by verified errata at `https://www.rfc-editor.org/errata_search.php?rfc=7539`.

[7] NIST. FIPS 180-4: Secure Hash Standard (SHS). `http://csrc.nist.gov/publications/PubsFIPS.html#180-4`, August 2015. DOI: 10.6028/NIST.FIPS.180-4.