I. Introduction

Zcash is an implementation of the Decentralized Anonymous Payment scheme Zerocash, with security fixes and improvements to performance and functionality. It bridges the existing transparent payment scheme used by Bitcoin [] with a shielded payment scheme secured by zero-knowledge succinct non-interactive arguments of knowledge. In this document, we will talk about:

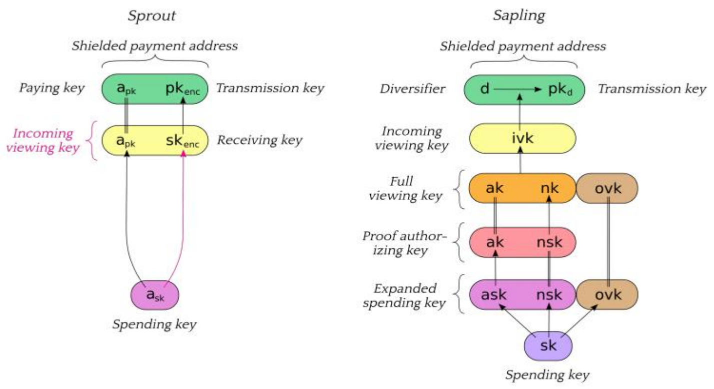
- The concept including: Payment Address and Keys in Zcash protocol, Blockchain Technology and Transaction type in Zcash.

II. Concepts

1. Payment Addresses and keys

A shielded payment address is necessary when a user's want to receive payment in the Zcash protocol, which is generated from a spending key.

The diagram below show the relation between key components in Sprout and Sapling. Arrows point from a component to any other component(s) that can be derived from it. Double lines indicate that the same component is used in multiple abstractions



[Sprout] The receiving key sk_{enc}, incoming viewing key ivk = (a_{pk}, sk_{enc}), and shielded payment address $addr_{pk}$ = (apk, pk_{enc}) are derived from the spending key ask.

[Sapling onward] An expanded spending key is composed of a Spend authorizing key ask, a nullifier private key nsk, and an outgoing viewing key ovk. From these components we can derive an proof authorizing key (ak, nsk), a full viewing key (ak, nk, ovk), an incoming viewing key ivk, and a set of diversified payment addresses addrd = (d, pkd).

The consensus protocol does not depend on how an expanded spending key is constructed. Two methods of doing so are defined:

- Generate a spending key sk at random and derive the expanded spending key (ask, nsk, ovk) from it, as shown in the diagram above.
- Obtain an extended spending key this includes a superset of the components of an expanded spending key. This method is used in the context of a Hierarchical Deterministic Wallet.

The composition of shielded payment addresses, incoming viewing keys, full 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 shielded payment address or incoming viewing key or full viewing key from a spending key or extended spending key.

Users can accept payment from multiple parties with a single shielded payment address and the fact that these payments are destined to the same payee is not revealed on the block chain, even to the paying parties. However if two parties collude to compare a shielded payment address they can trivially determine they are the same. In the case that a payee wishes to prevent this they should create a distinct shielded payment address for each payer. [Sapling onward] Sapling provides a mechanism to allow the efficient creation of diversified payment addresses with the same spending authority. A group of such addresses shares the same full viewing key and incoming viewing key, and so creating as many unlinkable addresses as needed does not increase the cost of scanning the block chain for relevant transactions.

2. Blockchain

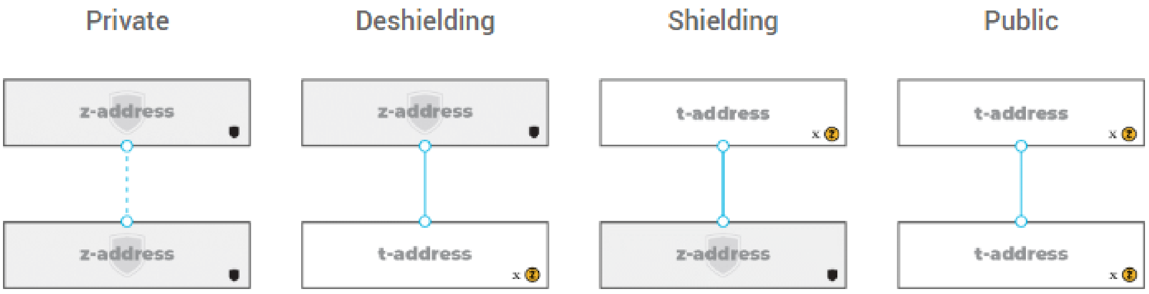
At a given point in time, each full validator is aware of a set of candidate blocks. These form a tree rooted at the genesis block, where each node in the tree refers to its parent via the hashPrevBlock block header field. A path from the root toward the leaves of the tree consisting of a sequence of one or more valid blocks consistent with consensus rules, is called a valid block chain. Each block in a block chain has a block height. The block height of the genesis block is 0, and the block height of each subsequent block in the block chain increments by 1. In order to choose the best valid block chain in its view of the overall block tree, a node sums the work. To break ties between leaf blocks, a node will prefer the block that it received first. The consensus protocol is designed to ensure that for any given block height, the vast majority of nodes should eventually agree on their best valid block chain up to that height.

3. Transactions

Each block contains one or more transactions. Transparent inputs to a transaction insert value into a transparent transaction value pool associated with the transaction, and transparent outputs remove value from this pool. As in Bitcoin, the remaining value in the pool is available to miners as a fee. Consensus rule: The remaining value in the transparent transaction value pool MUST be nonnegative.

3. 1 Multiple transaction types

Four type of transaction has exist the figure below show it:



Zcash addresses are either private (z-addresses) or transparent (t-addresses). Z-addresses start with a “z,” and t-addresses start with a "t."

A Z-to-Z transaction appears on the public blockchain, so it is known to have occurred and that the fees were paid. But the addresses, transaction amount and the memo field are all encrypted and not publicly visible. Using encryption on a blockchain is only possible through the use of zero-knowledge proofs

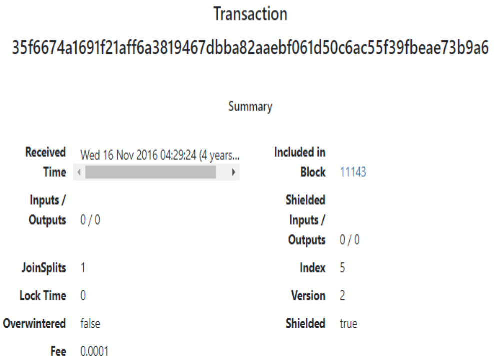
The owner of an address may choose to disclose z-address and transaction details with trusted third parties — think auditory and compliance needs — through the use of view keys and payment disclosure.

Transactions between two transparent addresses (t-addresses) work just like Bitcoin: The sender, receiver and transaction value are publicly visible. While many wallets and exchanges exclusively use t-addresseses today, many are moving to shielded addresses to better protect user privacy.

The two Zcash address types are interoperable. Funds can be transferred between z-addresses and t-addresses. However, is important that users understand the privacy implications of shielding or de-shielding information through these transactions

Furthermore the figure bellows show the different types of the addresses in Zcash Protocol:

Figure 1: Private address



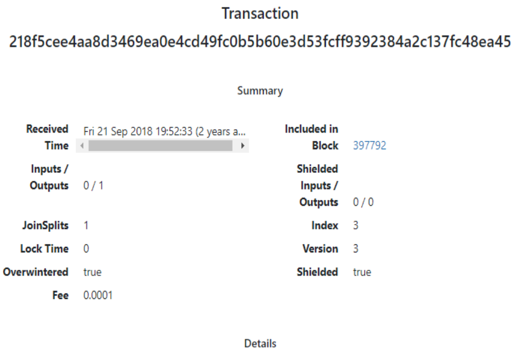
Transaction

35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbeae73b9a6

Summary

Received Time	Wed 16 Nov 2016 04:29:24 (4 years...	Included in Block	11143
Inputs / Outputs	0 / 0	Shielded Inputs / Outputs	0 / 0
JoinSplits	1	Index	5
Lock Time	0	Version	2
Overwintered	false	Shielded	true
Fee	0.0001		

Figure 2: Deshielding address



Transaction

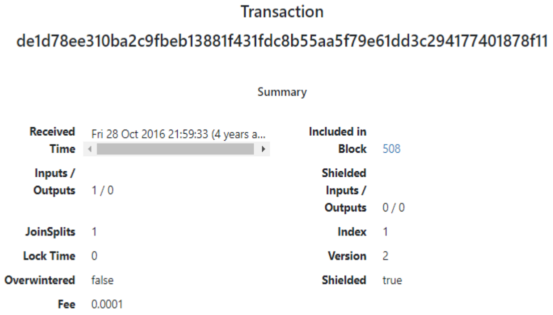
218f5cee4aa8d3469ea0e4cd49fc0b5b60e3d53fcff9392384a2c137fc48ea45

Summary

Received Time	Fri 21 Sep 2018 19:52:33 (2 years a...	Included in Block	397792
Inputs / Outputs	0 / 1	Shielded Inputs / Outputs	0 / 0
JoinSplits	1	Index	3
Lock Time	0	Version	3
Overwintered	true	Shielded	true
Fee	0.0001		

Details

Figure 3: Shielding address



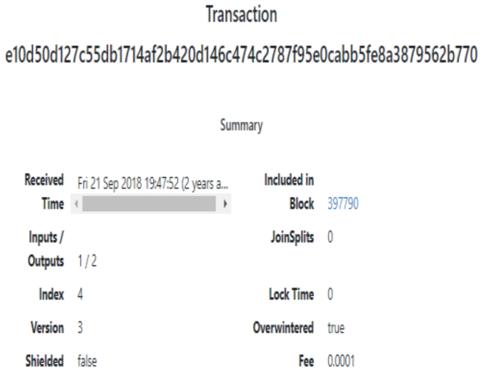
Transaction

de1d78ee310ba2c9fbeb13881f431fdc8b55aa5f79e61dd3c294177401878f11

Summary

Received Time	Fri 28 Oct 2016 21:59:33 (4 years a...	Included in Block	508
Inputs / Outputs	1 / 0	Shielded Inputs / Outputs	0 / 0
JoinSplits	1	Index	1
Lock Time	0	Version	2
Overwintered	false	Shielded	true
Fee	0.0001		

Figure 4: public address address



Transaction

e10d50d127c55db1714af2b420d146c474c2787f95e0cabb5fe8a3879562b770

Summary

Received Time	Fri 21 Sep 2018 19:47:52 (2 years a...	Included in Block	397790
Inputs / Outputs	1 / 2	JoinSplits	0
Index	4	Lock Time	0
Version	3	Overwintered	true
Shielded	false	Fee	0.0001