Zcash Protocol Specification

Version 2017.0-beta-2.9

Daira Hopwood*†*

Sean Bowe*†* — Taylor Hornby*†* — Nathan Wilcox*†*

December 17, 2017

**Abstract. Zcash** is an implementation of the *Decentralized Anonymous Payment* scheme **Zerocash**, with security fixes and adjustments to terminology, functionality and performance. It bridges the exist- ing *transparent* payment scheme used by **Bitcoin** with a *shielded* payment scheme secured by zero- knowledge succinct non-interactive arguments of knowledge (*zk-SNARKs*). It attempts to address the problem of mining centralization by use of the Equihash memory-hard proof-of-work algorithm.

This specification defines the **Zcash** consensus protocol and explains its differences from **Zerocash**

and **Bitcoin**.

**Keywords:** anonymity, applications, cryptographic protocols, electronic commerce and payment, financial privacy, proof of work, zero knowledge.

# [Contents](#_bookmark0) 1

#### [Introduction](#_bookmark1) 5

* 1. [Caution](#_bookmark3) 5
  2. [High-level Overview](#_bookmark4) 5

#### [Notation](#_bookmark7) 6

#### [Concepts](#_bookmark10) 8

* 1. [Payment Addresses and Keys](#_bookmark11) 8
  2. [Notes](#_bookmark12) 9
     1. [Note Plaintexts and Memo Fields](#_bookmark13) 9
  3. [The Block Chain](#_bookmark14) 9
  4. [Transactions and Treestates](#_bookmark15) 10
  5. [JoinSplit Transfers and Descriptions](#_bookmark16) 10
  6. [Note Commitment Trees](#_bookmark17) 11
  7. [Nullifier Sets](#_bookmark18) 11
  8. [Block Subsidy and Founders’ Reward](#_bookmark19) 12
  9. [Coinbase Transactions](#_bookmark20) 12

*†* Zerocoin Electric Coin Company

1. [Abstract Protocol](#_bookmark21) 12
   1. [Abstract Cryptographic Schemes](#_bookmark22) 12
      1. [Hash Functions](#_bookmark23) 12
      2. [Pseudo Random Functions](#_bookmark24) 12
      3. [Authenticated One-Time Symmetric Encryption](#_bookmark26) 13
      4. [Key Agreement](#_bookmark27) 13
      5. [Key Derivation](#_bookmark28) 13
      6. [Signature](#_bookmark30) 14
      7. [Commitment](#_bookmark32) 15
      8. [Represented Group](#_bookmark33) 15
      9. [Represented Pairing](#_bookmark34) 16
      10. [Zero-Knowledge Proving System](#_bookmark35) 16
   2. [Key Components](#_bookmark37) 17
   3. [JoinSplit Descriptions](#_bookmark38) 17
   4. [Sending Notes](#_bookmark39) 18
      1. [Dummy Notes](#_bookmark40) 19
   5. [Merkle path validity](#_bookmark41) 19
   6. [Non-malleability](#_bookmark43) 20
   7. [Balance](#_bookmark44) 20
   8. [Note Commitments and Nullifiers](#_bookmark45) 21
   9. [Zk-SNARK Statements](#_bookmark47) 21
      1. [JoinSplit Statement](#_bookmark48) 21
   10. [In-band secret distribution](#_bookmark54) 22
       1. [Encryption](#_bookmark55) 22
       2. [Decryption by a Recipient](#_bookmark57) 23
2. [Concrete Protocol](#_bookmark58) 23
   1. [Caution](#_bookmark59) 23
   2. [Integers, Bit Sequences, and Endianness](#_bookmark60) 24
   3. [Constants](#_bookmark61) 24
   4. [Concrete Cryptographic Schemes](#_bookmark62) 25
      1. [Hash Functions](#_bookmark64) 25
         1. [Merkle Tree Hash Function](#_bookmark65) 25
         2. [hSig Hash Function](#_bookmark66) 25
         3. [Equihash Generator](#_bookmark67) 25
      2. [Pseudo Random Functions](#_bookmark69) 26
      3. [Authenticated One-Time Symmetric Encryption](#_bookmark70) 26
      4. [Key Agreement](#_bookmark72) 27
      5. [Key Derivation](#_bookmark73) 27
      6. [Signature](#_bookmark74) 27
      7. [Commitment](#_bookmark75) 28
      8. [Represented Groups and Pairings](#_bookmark76) 28

[5.4.8.1 BN-254](#_bookmark77) 28

* + 1. [Zero-Knowledge Proving Systems](#_bookmark79) 29

[5.4.9.1 PHGR13](#_bookmark80) 29

* 1. [Note Plaintexts and Memo Fields](#_bookmark82) 30
  2. [Encodings of Addresses and Keys](#_bookmark83) 31
     1. [Transparent Payment Addresses](#_bookmark85) 31
     2. [Transparent Private Keys](#_bookmark86) 31
     3. [Shielded Payment Addresses](#_bookmark87) 32
     4. [Incoming Viewing Keys](#_bookmark89) 32
     5. [Spending Keys](#_bookmark90) 33
  3. [zk-SNARK Parameters](#_bookmark92) 33

#### [Consensus Changes from Bitcoin](#_bookmark93) 34

* 1. [Encoding of Transactions](#_bookmark94) 34
  2. [Encoding of JoinSplit Descriptions](#_bookmark96) 36
  3. [Block Header](#_bookmark97) 37
  4. [Proof of Work](#_bookmark100) 38
     1. [Equihash](#_bookmark101) 39
     2. [Difficulty filter](#_bookmark103) 40
     3. [Difficulty adjustment](#_bookmark104) 40
     4. [nBits conversion](#_bookmark106) 41
     5. [Definition of Work](#_bookmark107) 41
  5. [Calculation of Block Subsidy and Founders’ Reward](#_bookmark108) 42
  6. [Payment of Founders’ Reward](#_bookmark109) 42
  7. [Changes to the Script System](#_bookmark111) 44
  8. [Bitcoin Improvement Proposals](#_bookmark113) 44

#### [Differences from the Zerocash paper](#_bookmark114) 44

* 1. [Transaction Structure](#_bookmark115) 44
  2. [Memo Fields](#_bookmark116) 44
  3. [Unification of Mints and Pours](#_bookmark117) 44
  4. [Faerie Gold attack and fix](#_bookmark119) 45
  5. [Internal hash collision attack and fix](#_bookmark121) 46
  6. [Changes to PRF inputs and truncation](#_bookmark122) 46
  7. [In-band secret distribution](#_bookmark124) 47
  8. [Omission in **Zerocash** security proof](#_bookmark126) 48
  9. [Miscellaneous](#_bookmark127) 49

#### [Acknowledgements](#_bookmark129) 49

#### [Change history](#_bookmark130) 49

#### [References](#_bookmark133) 54

# 1 Introduction

**Zcash** is an implementation of the *Decentralized Anonymous Payment* scheme **Zerocash** [[BCG+2014],](#_bookmark137) with some security fixes and adjustments to terminology, functionality and performance. It bridges the existing *transparent* payment scheme used by **Bitcoin** [[Naka2008]](#_bookmark184) with a *shielded* payment scheme secured by zero-knowledge suc- cinct non-interactive arguments of knowledge (*zk-SNARKs*).

Changes from the original **Zerocash** are explained in [§7](#_bookmark114) *‘Differences from the Zerocash paper’* on p. 44, and high- lighted in magenta throughout the document.

Technical terms for concepts that play an important role in **Zcash** are written in *slanted text* . *Italics* are used for emphasis and for references between sections of the document.

The key words **MUST**, **MUST NOT**, **SHOULD**, and **SHOULD NOT** in this document are to be interpreted as described in [[RFC-2119]](#_bookmark187) when they appear in **ALL CAPS**. These words may also appear in this document in lower case as plain English words, absent their normative meanings.

This specification is structured as follows:

* Notation — definitions of notation used throughout the document;
* Concepts — the principal abstractions needed to understand the protocol;
* Abstract Protocol — a high-level description of the protocol in terms of ideal cryptographic components;
* Concrete Protocol — how the functions and encodings of the abstract protocol are instantiated;
* Consensus Changes from **Bitcoin** — how **Zcash** differs from **Bitcoin** at the consensus layer, including the Proof of Work;
* Differences from the **Zerocash** protocol — a summary of changes from the protocol in [[BCG+2014].](#_bookmark137)

## Caution

**Zcash** security depends on consensus. Should a program interacting with the **Zcash** network diverge from con- sensus, its security will be 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 that 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** and related software. If you find any mistake in this specification, please contact [<security@z.cash>](mailto:security@z.cash).

## High-level Overview

The following overview is intended to give a concise summary of the ideas behind the protocol, for an audience already familiar with *block chain*-based cryptocurrencies such as **Bitcoin**. It is imprecise in some aspects and is not part of the normative protocol specification.

Value in **Zcash** is either *transparent* or *shielded* . Transfers of *transparent* value work essentially as in **Bitcoin** and have the same privacy properties. *Shielded* value is carried by *notes* [1](#_bookmark5), which specify an amount and a *paying key* . The *paying key* is part of a *payment address*, which is a destination to which *notes* can be sent. As in **Bitcoin**, this is associated with a private key that can be used to spend *notes* sent to the address; in **Zcash** this is called a *spending key* .

Zcash中的值是透明或者屏蔽。 转让透明价值的工作基本上与比特币一样，并具有相同的隐私属性。 屏蔽值由票据携带，票据指定金额和支付密钥。 支付密钥是支付地址的一部分，支付地址是票据可以发送到的目的地。 和比特币一样，这与一个私钥相关联，该私钥可用于将票据发送到该地址（该私钥可用来花费发送到该地址的票据）; 在Zcash中这被称为支出密钥。

1  In **Zerocash** [[BCG+2014],](#_bookmark137) *notes* were called “coins”, and *nullifiers* were called “serial numbers”.

To each *note*there is cryptographically associated a *note commitment* , and a *nullifier* [1](#_bookmark5) (so that there is a 1:1:1 re- lation between *notes*, *note commitments*, and *nullifiers*). Computing the *nullifier* requires the associated private *spending key* . It is infeasible to correlate the *note commitment* with the corresponding *nullifier* without knowl- edge of at least this *spending key* . An unspent valid *note*, at a given point on the *block chain*, is one for which the *note commitment* has been publically revealed on the *block chain* prior to that point, but the *nullifier* has not.

对于每个票据，都存在密码相关的票据承诺和否定器（因此票据，票据承诺和否定器之间存在1：1：1的关系）。 计算否定器需要相关的私人支出密钥（spending key）。 在不知道至少这个支出密钥的情况下，将票据承诺与相应的否定器相关联是不可行的。 在区块链的给定点处，未使用的有效票据是票据承诺已经在该点之前在区块链上公开发布的，但是否定器没有。

A *transaction* can contain *transparent* inputs, outputs, and scripts, which all work as in **Bitcoin** [[Bitc-Protoc](#_bookmark169)ol]. It also contains a sequence of zero or more *JoinSplit descriptions*. Each of these describes a *JoinSplit transfer* [2](#_bookmark8) which takes in a *transparent* value and up to two input *notes*, and produces a *transparent* value and up to two output *notes*. The *nullifiers* of the input *notes* are revealed (preventing them from being spent again) and the commitments of the output *notes* are revealed (allowing them to be spent in future). Each *JoinSplit description* also includes a computationally sound *zk-SNARK* proof, which proves that all of the following hold except with negligable probability:

一个交易可以包含透明的输入，输出和脚本，所有这些都可以像比特币一样工作[Bitc-Protocol]。 它还包含零个或多个JoinSplit描述。 其中每一个都描述了一个JoinSplit转移，它接受一个透明值和最多两个输入票据，并产生一个透明值和最多两个输出票据。 揭示输入票据的否定器（防止它们再次被花费），并揭示输出票据的承诺（允许它们在将来花费）。 每个JoinSplit描述还包含一个计算完善的zk-SNARK证明，证明除了可忽略的概率之外，以下所有内容都成立：

* + - The input and output values balance (individually for each *JoinSplit transfer* ).
    - For each input *note* of non-zero value, some revealed *note commitment* exists for that *note*.
    - The prover knew the private *spending keys* of the input *notes*.
    - The *nullifiers* and *note commitments* are computed correctly.
    - The private *spending keys* of the input *notes* are cryptographically linked to a signature over the whole *trans- action*, in such a way that the *transaction* cannot be modified by a party who did not know these private keys.
    - Each output *note* is generated in such a way that it is infeasible to cause its *nullifier* to collide with the *nullifier*

of any other *note*.

•输入和输出值平衡（对于每个JoinSplit传输都是单独的）。

•对于每个非零值的输入票据，存在一些已经揭示的票据承诺。

•证明者知道输入票据的私人支出密钥。

•否定器和票据承诺的计算正确。

•输入票据的私人支出密钥与整个交易中的签名加密链接，这样交易不能由不知道这些私人密钥的一方修改。

•每个输出票据的生成不可能导致其 否定器与任何其他票据的否定器相冲突。

Outside the *zk-SNARK* , it is also checked that the *nullifiers* for the input *notes* had not already been revealed (i.e. they had not already been spent).

A *payment address* includes two public keys: a *paying key* matching that of *notes* sent to the address, and a *transmission key* for a key-private asymmetric encryption scheme. “Key-private” means that ciphertexts do not reveal information about which key they were encrypted to, except to a holder of the corresponding private key, which in this context is called the *receiving key* . This facility is used to communicate encrypted output *notes* on the *block chain* to their intended recipient, who can use the *receiving key* to scan the *block chain* for *notes* addressed to them and then decrypt those *notes*.

支付地址包括两个公共密钥：与发送到地址的票据匹配的支付密钥和用于密钥 - 私有非对称加密方案的传输密钥。 “密钥 - 私有”意味着密文不会泄露关于他们被加密的密钥的信息，在这种情况下解密秘钥称为接收密钥。 该工具用于将块链上加密的输出票据传送给预期收件人，该收件人可以使用接收密钥扫描区块链中的票据，然后找到并解密发送给他的票据。

The basis of the privacy properties of **Zcash** is that when a *note* is spent, the spender only proves that some commitment for it had been revealed, without revealing which one. This implies that a spent *note* cannot be linked to the *transaction* in which it was created. That is, from an adversary’s point of view the set of possibilities for a given *note* input to a *transaction*—its *note traceability set* — includes *all* previous notes that the adversary does not control or know to have been spent. This contrasts with other proposals for private payment systems, such as CoinJoin [[Bitc-CoinJoin]](#_bookmark163) or **CryptoNote** [[vanS2014],](#_bookmark191) that are based on mixing of a limited number of transactions and that therefore have smaller *note traceability sets*.

Zcash的隐私属性的基础是，当一张票据被花费时，花费者只证明一些能够揭示其来源的承诺已经被揭示，而没有透露哪一个。 这意味着已使用的票据不能与输出其的交易链接。 也就是说，从对手的角度来看，交易中给定票据输入的一系列可能性 （ “票据可追溯性集合”）包括对手无法控制或已知花费的所有先前票据。 这与私人支付系统的其他提案形成对比，例如CoinJoin [Bitc-CoinJoin]或CryptoNote [vanS2014]，它们基于混合有限数量的交易并因此具有较小的票据可追溯性集合。

The *nullifiers* are necessary to prevent double-spending: each note only has one valid *nullifier* , and so attempting to spend a *note* twice would reveal the *nullifier* twice, which would cause the second *transaction* to be rejected.

为了防止双重消费，必须使用否定器：每个注释只有一个有效的否定器，因此试图两次使用票据将会两次显示否定器，这会导致第二个交易被拒绝。

# Notation

B means the type of bit values, i.e. *{*0*,* 1*}*.

N means the type of nonnegative integers. N+ means the type of positive integers. Q means the type of rationals（有理数）.

*x* ◦ *T* is used to specify that *x* has type *T* . A cartesian product type is denoted by *S × T* , and a function type by

◦

*S → T* . An argument to a function can determine other argument or result types.

2  *JoinSplit transfers* in **Zcash** generalize “Mint” and “Pour” *transactions* in **Zerocash**; see [§7.1](#_bookmark115) *‘Transaction Structure’* on p. 44 for differences.

The type of a randomized algorithm is denoted by *S* R

*→*

R

*T* . The domain of a randomized algorithm may be (),

indicating that it requires no arguments. Given *f* ◦ *S → T* and *s* ◦ *S*, sampling a variable *x* ◦ *T* from the output of *f*

◦ ◦ ◦

applied to *s* is denoted by *x* R *f* (*s*).

*←*

Initial arguments to a function or randomized algorithm may be written as subscripts, e.g. if *x* ◦

◦

◦

*X*, *y* ◦

*Y* , and

*f* ◦ *X × Y → Z*, then an invocation of *f* (*x, y*) can also be written *f*x (*y*).

◦

*T* [ 亿 ], where *T* is a type and is an integer, means the type of sequences of length with elements in *T* . For example,

B[ 亿 ] means the set of sequences of bits.

length(*S*) means the length of (number of elements in) *S*.

*T ⊆ U* indicates that *T* is an inclusive subset or subtype of *U* .

*S ∪ T* means the type corresponding to the set union of *S* and *T* .

B[8*·*N] means the type of bit sequences constrained to be of length a multiple of 8 bits.

**0x** followed by a string of **boldface** hexadecimal digits means the corresponding integer converted from hexadec- imal.

**“..."** means the given string represented as a sequence of bytes in US-ASCII. For example, **“abc"** represents the byte sequence [**0x61***,* **0x62***,* **0x63**].

[0] 亿 means the sequence of zero bits.

*a..b*, used as a subscript, means the sequence of values with indices *a* through *b* inclusive. For example, anew

new

new

new

new

pk,1..N

means the sequence [apk,1*,* apk,2*, ...* apk,Nnew ]. (For consistency with the notation in [[BCG+2014]](#_bookmark137) and in [[BK2016],](#_bookmark170) this specification uses 1-based indexing and inclusive ranges, notwithstanding the compelling arguments to the con- trary made in [[EWD-831].)](#_bookmark174)

*{a .. b}* means the set or type of integers from *a* through *b* inclusive.

[ *f* (*x*) for *x* from *a* up to *b* ] means the sequence formed by evaluating *f* on each integer from *a* to *b* inclusive, in ascending order. Similarly, [ *f* (*x*) for *x* from *a* down to *b* ] means the sequence formed by evaluating *f* on each integer from *a* to *b* inclusive, in descending order.

*a || b* means the concatenation of sequences *a* then *b*.

concatB (*S*) means the sequence of bits obtained by concatenating the elements of *S* viewed as bit sequences. If the elements of *S* are byte sequences, they are converted to bit sequences with the *most significant* bit of each

byte first.

concatB（S）表示通过连接被视为位序列的S的元素而获得的位序列。 如果S的元素是字节序列，则将它们转换为每个字节的最高有效位在前的位序列。

sorted(*S*) means the sequence formed by sorting the elements of *S*.

Fn means the finite field with *n* elements, and F*∗*n means its group under multiplication. Fn[*z*] means the ring of polynomials over *z* with coefficients in Fn.

Fn表示有n个元素的有限域，F \* n表示它的乘积。 Fn [z]是指系数为Fn的z上的多项式环。

*a b* means the result of multiplying *a* and *b*. This may refer to multiplication of integers, rationals, or finite field elements according to context.

*·*

*a*b, for *a* an integer or finite field element and *b* an integer, means the result of raising *a* to the exponent *b*. *a* mod *q*, for *a* ◦ N and *q* ◦ N+, means the remainder on dividing *a* by *q*.

◦

◦

*a b* means the bitwise-exclusive-or of *a* and *b*, and *a* 笭 *b* means the bitwise-and of *a* and *b*. These are defined either on integers or bit sequences according to context.

*⊕*

N



*a*i means the sum of *a*1..N .

i=1

N

*a*i means the bitwise exclusive-or of *a*1..N .

尘

i=1

The binary relations *<*, , =, , and *>* have their conventional meanings on integers and rationals, and are defined lexicographically on sequences of integers.

*≤ ≥*

floor(*x*) means the largest integer *≤ x*. ceiling (*x*) means the smallest integer *≥ x*.

bitlength(*x*), for *x* ◦ N, means the smallest integer such that 2 l *> x*.

◦

The symbol *⊥* is used to indicate unavailable information or a failed decryption.

The following integer constants will be instantiated in [§5.3](#_bookmark61) *‘Constants’* on p. 24: dMerkle, Nold, Nnew, Merkle, hSig, PRF,

r, Seed, ask , ϕ, MAX\_MONEY, SlowStartInterval, HalvingInterval, MaxBlockSubsidy, NumFounderAddresses, PoWLimit, PoWAveragingWindow, PoWMedianBlockSpan, PoWDampingFactor, PoWTargetSpacing. The bit sequence constant Uncommitted ◦ B[亿Merkle ] and the rational constants FoundersFraction, PoWMaxAdjustDown, and PoWMaxAdjustUp will

◦

also be defined in that section.

# Concepts

## Payment Addresses and Keys

Users who wish to receive payments under this scheme first generate a random *spending key* ask.

The *receiving key* skenc, the *incoming viewing key* ivk = (apk*,* skenc ), and the *payment address* addrpk = (apk*,* pkenc )

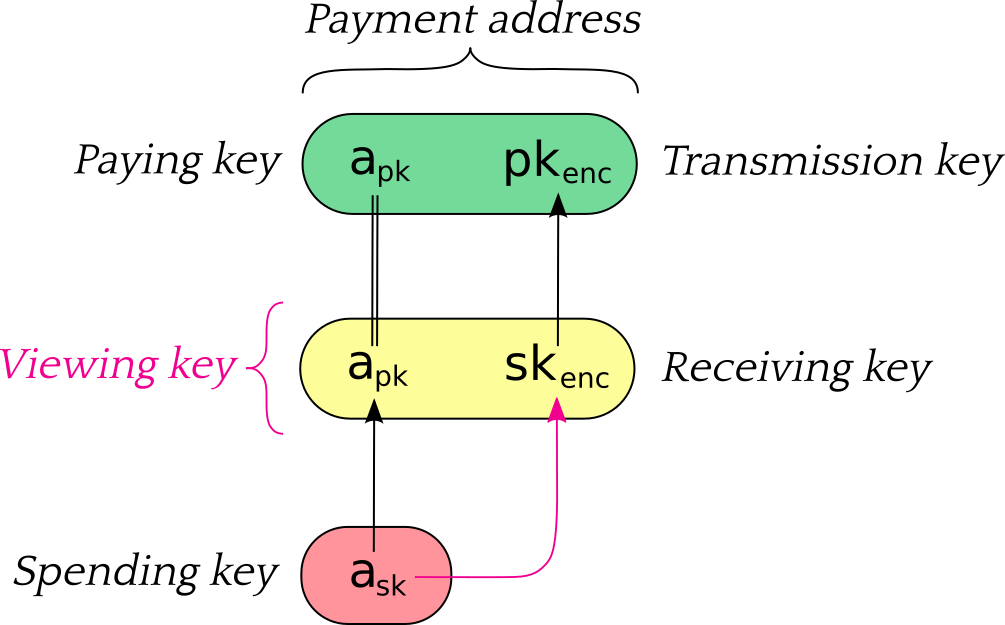
are derived from ask, as described in [§4.2](#_bookmark37) *‘Key Components’* on p. 17.

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.

希望根据此方案接收付款的用户首先会生成随机支出密钥a。

接收密钥skenc，收入密钥ivk =（apk，skenc）和付款地址addrpk =（apk，pkenc）是从a中导出的，如§4.2'Key Components'的p。中所述。17。

下图描述了关键组件之间的关系。 箭头从一个组件指向任何其他可以从它派生的组件。



The derivation of these components is detailed in [§4.2](#_bookmark37) *‘Key Components’* on p. 17.

The composition of *payment addresses*, *incoming 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* or *incoming viewing key* from a *spending key* .

支付地址，收入密钥和支出密钥的组成是通常不会公开给用户的密码协议详细信息。 但是，应该提供用户可视化操作以从支出密钥获得支付地址或收入密钥。

Users can accept payment from multiple parties with a single *payment address* addrpk 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 *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 *payment address* for each payer.

用户可以使用单一付款地址addrpk接受来自多方的付款，并且这些付款注定给同一收款人的事实并未透露给区块链，甚至付给付款方。 然而，如果双方串通比较付款地址，他们可以自然地确定它们是相同的。 在收款人希望防止这种情况下，他们应该为每个付款人创建一个不同的付款地址。

**Note:** It is conventional in cryptography to refer to the key used to encrypt a message in an asymmetric encryp- tion scheme as the “public key". However, the public key used as the *transmission key* component of an address (pkenc) need not be publically distributed; it has the same distribution as the *payment address* itself. As men- tioned above, limiting the distribution of the *payment address* is important for some use cases. This also helps to reduce reliance of the overall protocol on the security of the cryptosystem used for *note* encryption (see [§4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22), since an adversary would have to know pkenc in order to exploit a hypo- thetical weakness in that cryptosystem.

传统的密码学方法是将非对称加密方案中用于加密消息的密钥称为“公钥”，然而，用作地址传输关键组件的公钥（pkenc）不需要完全公布。 它与支付地址本身具有相同的分布，如上所述，限制支付地址的分配对于某些用例很重要，这也有助于减少整个协议对所用密码系统安全性的依赖 （参见第22页§4.10'带内秘密分配'），因为攻击者必须知道pkenc才能利用该密码系统中的弱点。

## Notes

A *note* (denoted **n**) is a tuple (apk*,* v*,* ρ*,* r). It represents that a value v is spendable by the recipient who holds the

*spending key* ask corresponding to apk, as described in the previous section.

*Note是一个四元组，n={* apk*,* v*,* ρ*,* r *}，表示持有与*apk*对应的*ask

* apk ◦◦ B[亿PRF ] is the *paying key* of the recipient;
* v ◦ *{*0 *..* MAX\_MONEY*}* is an integer representing the value of the *note* in *zatoshi* (1 **ZEC** = 108 *zatoshi* );

◦

* ρ ◦ B[亿PRF ] is used as input to PRFnf to derive the *nullifier* of the *note*;
  + ask
* r ◦ B[亿r ] is a random bit sequence used as a *commitment trapdoor* as defined in [§4.1.7](#_bookmark32) *‘Commitment’* on p. 15.

◦

Let Note be the type of a *note*, i.e. B[亿PRF ] *× {*0 *..* MAX\_MONEY*} ×* B[亿PRF ] *×* B[亿r ].

Creation of new *notes* is described in [§4.4](#_bookmark39) *‘Sending Notes’* on p. 18. When *notes* are sent, only a commitment (see

[§4.1.7](#_bookmark32) *‘Commitment’* on p. 15) to the above values is disclosed publically. This allows the value and recipient to be kept private, while the commitment is used by the *zero-knowledge proof* when the *note* is spent, to check that it exists on the *block chain*.

创建新的票据在§4.4'发送注释'的页面中进行了介绍。 当票据发送时，只有一个针（见第4.1.7节“承诺” 15）对上述金额的票据被公开披露。 这允许交易金额和收款人保持私密性，而票据使用时用零知识证明来验证其承诺，以检查它是否存在于区块链上。

The *note commitment* is computed as NoteCommitment(**n**) = COMMr (apk*,* v*,* ρ), where COMM is instantiated in

[§5.4.7](#_bookmark75) *‘Commitment’* on p. 28.

A *nullifier* (denoted nf) is derived from the ρ component of a *note* and the recipient’s *spending key* , using a *Pseudo Random Function* (see [§ 4.1.2](#_bookmark24) *‘Pseudo Random Functions’* on p. 12). Specifically it is derived as PRFnf (ρ) where

PRFnf

is instantiated in [§5.4.2](#_bookmark69) *‘Pseudo Random Functions’* on p. 26.

ask

A *note* is spent by proving knowledge of ρ and ask in zero knowledge while publically disclosing its *nullifier* nf, allowing nf to be used to prevent double-spending.

#### 3.2.1 Note Plaintexts and Memo Fields

Transmitted *notes* are stored on the *block chain* in encrypted form, together with a *note commitment* cm.

The *note plaintexts* in a *JoinSplit description* are encrypted to the respective *transmission keys* pknew

enc,1..N

new , and

the result forms part of a *transmitted notes ciphertext* (see [§4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22 for further details).

传输的票据以加密的形式存储在块链上，并附有票据承诺cm。

JoinSplit描述中的票据明文被相应的传输密钥pk 加密，并且结果形成发送的票据密文的一部分（参见第22页的§4.10'带内秘密分发'以获得进一步的细节）。

Each *note plaintext* (denoted **np**) consists of (v*,* ρ*,* r*,* memo). The first three of these fields are as defined earlier.

memo represents a *memo field* associated with this *note*. The usage of the *memo field* is by agreement between the sender and recipient of the *note*.

备注表示与本票据相关的备注字段。 备注字段的使用是通过票据的发送者和接收者之间的协商决定的。

## The Block Chain

At a given point in time, each *full node* 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 (see [§6.3](#_bookmark97) *‘Block Header’* on p. 37).

在给定的时间点，每个完整的节点都知道一组候选块。 这些形成了一棵植根于创世块的树，树中的每个节点通过hashPrevBlock块头字段引用其父节点

A path from the root toward the leaves of the tree consisting of a sequence of one or valid *blocks* consistent with consensus rules, is called a valid *block chain*.

从符合共识规则的由一个或多个有效块序列组成的树的 根部到树叶的路径被称为有效的块链。

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.

块链中的每个块都具有块高度。 生成块的块高度为0，块链中每个后续块的块高度递增1。

In order to choose the “best” valid *block chain* in its view of the overall *block* tree, a node sums the work, as defined in [§6.4.5](#_bookmark107) *‘Definition of Work’* on p. 41, of all *blocks* in each chain, and considers the chain with greatest total work to be best. To break ties between leaf *blocks*, a node will prefer the *block* that it received first.

为了在其整个块树的视图中选择“最佳”有效块链，节点对每个链中所有块的工作进行求和，并且将具有最大总工作量的链视为最好。 为了断开叶块之间的联系，节点将首选首先接收的块。

The consensus protocol is designed to ensure that for any given *block height* , the vast majority of nodes should eventually agree on their “best” *block chain* up to that height.

共识协议旨在对于任意给定的块高度，大多数的节点都能够最终就该高度下的最佳 块链达成一致。

## Transactions and Treestates

Each *block* contains one or more *transactions*.

Inputs to a *transaction* insert value into a *transparent value pool* , and outputs remove value from this pool. As in

**Bitcoin**, the remaining value in the pool is available to miners as a fee.

交易的输入值添加金额到交易金额池中，输出从币池中删除值。 和比特币一样，币池中的剩余价值可作为交易费提供给矿工。

**Consensus rule:** The remaining value in the *transparent value pool* **MUST** be nonnegative.

共识的规则：在透明值池的剩余价值必须为非负数。

To each *transaction* there is associated an initial *treestate*. 每个交易都有一个初始树状态。

A *treestate* consists of:

* + - a *note commitment tree* [(§3.6](#_bookmark17) *‘Note Commitment Trees’* on p. 11); 票据承诺树；
    - a *nullifier set* [(§3.7](#_bookmark18) *‘Nullifier Sets’* on p. 11); 否定器集合；
    - data structures associated with **Bitcoin** such as the UTXO (Unspent Transaction Output) set.

和比特币相关的数据结构；

An *anchor* is a Merkle tree root of a *note commitment tree*. It uniquely identifies a *note commitment tree* state given the assumed security properties of the Merkle tree’s hash function. Since the *nullifier set* is always updated together with the *note commitment tree*, this also identifies a particular state of the *nullifier set* .

锚点是票据承诺树的Merkle树根。 在给定的Merkle树散列函数的安全属性下，它唯一地标识了票据承诺树状态。由于否定器集合总是与票据承诺树一起更新，所以这也标识了否定器集合的特定状态。

In a given *block chain*, *treestates* are chained as follows:

* + - The input *treestate* of the first *block* is the empty *treestate*.
    - 第一个块的输入树状态是空的树状态。
    - The input *treestate* of the first *transaction* of a *block* is the final *treestate* of the immediately preceding *block* .
    - 块的第一个事务的输入树状态是前一个块的最终树状态。
    - The input *treestate* of each subsequent *transaction* in a *block* is the output *treestate* of the immediately preceding *transaction*.
    - 块中每个后续事务的输入树状态都是前一个事务的输出树状态。
    - The final *treestate* of a *block* is the output *treestate* of its last *transaction*.
    - 块的最终树状态是其最后一个事务的输出树状态。

*JoinSplit descriptions* also have interstitial input and output *treestates*, explained in the following section.

## JoinSplit Transfers and Descriptions

A *JoinSplit description* is data included in a *transaction* that describes a *JoinSplit transfer* , i.e. a *shielded* value transfer. This kind of value transfer is the primary **Zcash**-specific operation performed by *transactions*; it uses, but should not be confused with, the *JoinSplit statement* used for the *zk-SNARK* proof and verification.

JoinSplit描述是包含在描述JoinSplit交易中的数据，即屏蔽值传输。 这种价值转移是交易执行的主要Zcash特定操作; 它使用但不应该混淆用于zk-SNARK证明和验证的JoinSplit语句。

A *JoinSplit transfer* spends Nold *notes* **n**old old and *transparent* input vold , and creates Nnew *notes* **n**new new and *trans-*

*parent* output vnew.

pub

1..N

pub

1..N

Each *transaction* is associated with a sequence of *JoinSplit descriptions*.

The total vnew value adds to, and the total vold

value subtracts from the *transparent value pool* of the containing

pub

*transaction*.

pub

The *anchor* of each *JoinSplit description* in a *transaction* refers to a *treestate*. For the first *JoinSplit description*, this **MUST** be the output *treestate* of a previous *block* .

事务中每个JoinSplit描述的锚都引用一个状态树。 对于第一个JoinSplit描述，这必须是前一个块的输出状态树。

For each *JoinSplit description* in a *transaction*, an interstitial output *treestate* is constructed which adds the *note commitments* and *nullifiers* specified in that *JoinSplit description* to the input *treestate* referred to by its *anchor* .

对于交易中的每个JoinSplit描述，一个 中间输出状态树构造如下，其将该JoinSplit描述中指定的票据承诺和否定器添加到由其锚点引用的输入状态树中。

This interstitial output *treestate* is available for use as the *anchor* of subsequent *JoinSplit descriptions* in the same

*transaction*.

此中间输出状态树可用作同一交易中后续JoinSplit描述的锚点。

Interstitial *treestates* are necessary because when a *transaction* is constructed, it is not known where it will even- tually appear in a mined *block* . Therefore the *anchors* that it uses must be independent of its eventual position.

中间状态树是必要的，因为在创建交易时，不知道它将在哪里最终出现在区块中。 因此，它使用的锚必须独立于其最终位置。

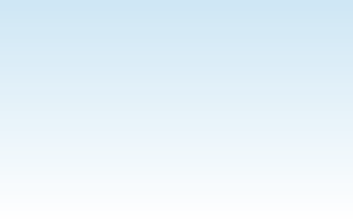
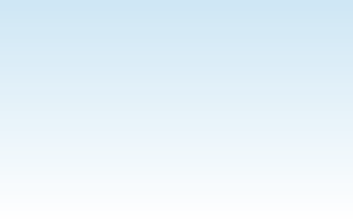
#### Consensus rules:

* + - The input and output values of each *JoinSplit transfer* **MUST** balance exactly.
    - 输入输出平衡
    - The *anchor* of each *JoinSplit description* in a *transaction* **MUST** refer to either some earlier *block* ’s final

*treestate*, or to the interstitial output *treestate* of any prior *JoinSplit description* in the same *transaction*.

•交易中每个JoinSplit描述的锚必须引用某个早期块的最终状态树，或者引用同一交易中之前任何JoinSplit描述的中间输出树状态。

## Note Commitment Trees



rt

?

cm1

cm2

cm3

cm4

cm5

?

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

票据承诺树是一个固定深度的增量Merkle树，用于存储JoinSplit传输产生的票据承诺。 就像比特币中使用的未使用的交易输出集合（UTXO集合）一样，它用于表示价值的存在和花费能力。 然而，与UTXO不同，树的工作不是防止双重支出，因为它只能追加。

A *root* of this tree is associated with each *treestate*, as described in [§3.4](#_bookmark15) *‘Transactions and Treestates’* on p. 10. Each *node* in the *incremental Merkle tree* is associated with a *hash value* of size lMerkle bits. The *layer* numbered *h*, counting from *layer* 0 at the *root* , has 2h *nodes* with *indices* 0 to 2h 1 inclusive. The *hash value* associated ith the *node* at *index i* in *layer h* is denoted Mh.

*−*

i

增量Merkle树中的每个节点都与一个大小为 l 比特值相关联。 编号为h的层（从根层的第0层起算）具有2h个节点，其索引为0到2h -1（含）。 与层h中的索引i处的节点相关联的散列值被表示为。

## Nullifier Sets

Each *full node* maintains a *nullifier set* logically associated with each *treestate*. As valid *transactions* containing

*JoinSplit transfers* are processed, the *nullifiers* revealed in *JoinSplit descriptions* are inserted into this *nullifier set* .

每个完整节点维护一个逻辑上与每个状态树关联的否定器集合。 由于处理了包含JoinSplit传输的有效交易，因此在JoinSplit描述中揭示的Nullifier将插入到此Nullifier集合中。

*Nullifiers* are enforced to be unique within a valid *block chain*, in order to prevent double-spends.

**Consensus rule:** A *nullifier* **MUST NOT** repeat either within a *transaction*, or across *transactions* in a valid *block chain*.

## Block Subsidy and Founders’ Reward

Like **Bitcoin**, **Zcash** creates currency when *blocks* are mined. The value created on mining a *block* is called the *block subsidy* . It is composed of a *miner subsidy* and a *Founders’ Reward* . As in **Bitcoin**, the miner of a *block* also receives *transaction fees*.

和比特币一样，Zcash在块开采时创建货币。 挖掘一个区块创造的价值被称为区块补贴。 它由矿工补贴和创始人的奖励组成。 和比特币一样，一个区块的矿工也收到交易费用。

The calculations of the *block subsidy* , *miner subsidy* , and *Founders’ Reward* depend on the *block height* , as defined in [§3.3](#_bookmark14) *‘The Block Chain’* on p. 9.

区块补贴，矿工补贴和创始人奖励的计算取决于区块高度

These calculations are described in [§6.5](#_bookmark108) *‘Calculation of Block Subsidy and Founders’ Reward’* on p. 42.

## Coinbase Transactions

The first *transaction* in a block must be a *coinbase transaction*, which should collect and spend any *miner subsidy* and *transaction fees* paid by *transactions* included in this *block* . The *coinbase transaction* must also pay the *Founders’ Reward* as described in [§6.6](#_bookmark109) *‘Payment of Founders’ Reward’* on p. 42.

在一个区块中的第一笔交易必须是一个coinbase交易（基础交易），该交易应该收集并花费任何矿工的补贴和交易费用。 coinbase交易还必须支付创始人的奖励。

区块的第一个交易必须是coinbase交易，声明发现这个块的奖励和块里所有多余的交易费都要转到矿工指定的账户中去—柯。

# Abstract Protocol

## Abstract Cryptographic Schemes

#### Hash Functions

MerkleCRH ◦ B[亿Merkle ] B[亿Merkle ] B[亿Merkle ] is a collision-resistant hash function used in [§4.5](#_bookmark41) *‘Merkle path validity’*

◦

*× →*

on p. 19. It is instantiated in [§5.4.1.1](#_bookmark65) *‘Merkle Tree Hash Function’* on p. 25.

hSigCRH ◦ B[亿Seed ] *×* B[亿PRF ][N ] *×* JoinSplitSig*.*Public *→* B[亿hSig ] is a collision-resistant hash function used in [§ 4.3](#_bookmark38)

◦

old

*‘JoinSplit Descriptions’* on p. 17. It is instantiated in [§5.4.1.2](#_bookmark66) *‘*hSig *Hash Function’* on p. 25.

EquihashGen ◦ (*n* ◦ N+ ) *×* N+ *×* B[8*·*N] *×* N+ *→* B[n] is another hash function, used in [§ 6.4.1](#_bookmark101) *‘Equihash’* on p. 39 to

◦

◦

generate input to the Equihash solver. The first two arguments, representing the Equihash parameters *n* and *k*, are

written subscripted. It is instantiated in [§5.4.1.3](#_bookmark67) *‘Equihash Generator’* on p. 25.

#### Pseudo Random Functions

PRFx is a *Pseudo Random Function* keyed by *x*. Four *independent* PRFx are needed in our protocol:

PRFaddr ◦

◦

PRFnf ◦

◦

PRFpk ◦

◦

PRFρ ◦

◦

B[亿ask ] *× {*0 *..* 255*} →* B[亿PRF ]

B[亿ask ] *×* B[亿PRF ] *→* B[亿PRF ]

B[亿ask ] *× {*1*..*Nold*} ×* B[亿hSig ] *→* B[亿PRF ]

B[亿ϕ] *× {*1*..*Nnew*} ×* B[亿hSig ] *→* B[亿PRF ]

These are used in [§ 4.9.1](#_bookmark48) *‘JoinSplit Statement’* on p. 21; PRFaddr is also used to derive a *payment address* from a

*spending key* in [§4.2](#_bookmark37) *‘Key Components’* on p. 17.

They are instantiated in [§5.4.2](#_bookmark69) *‘Pseudo Random Functions’* on p. 26.

**Security requirement:** In addition to being *Pseudo Random Functions*, it is required that PRFnf , PRFaddr, and

x x

PRFρ be collision-resistant across all *x* — i.e. it should not be feasible to find (*x, y*) \* (*xt, yt* ) such that PRFnf (*y*) =

x

x

PRFnf (*yt* ), and similarly for PRFaddr and PRFρ.

x*I*

**Note:** PRFnf was called PRFsn in **Zerocash** [[BCG+2014].](#_bookmark137)

#### Authenticated One-Time Symmetric Encryption

Let Sym be an *authenticated one-time symmetric encryption scheme* with keyspace Sym*.***K**, encrypting plaintexts in Sym*.***P** to produce ciphertexts in Sym*.***C**.

Sym*.*Encrypt ◦ Sym*.***K** *×* Sym*.***P** *→* Sym*.***C** is the encryption algorithm.

◦

Sym*.*Decrypt ◦ Sym*.***K** *×* Sym*.***C** *→* Sym*.***P** *∪ {⊥}* is the corresponding decryption algorithm, such that for any

◦

K Sym*.***K** and P Sym*.***P**, Sym*.*DecryptK (Sym*.*EncryptK (P)) = P. is used to represent the decryption of an invalid ciphertext.

*∈ ∈ ⊥*

**Security requirement:** Sym must be one-time (INT-CTXT IND-CPA)-secure. “One-time” here means that an honest protocol participant will almost surely encrypt only one message with a given key; however, the attacker may make many adaptive chosen ciphertext queries for a given key. The security notions INT-CTXT and IND-CPA are as defined in [[BN2007].](#_bookmark171)

*∧*

#### Key Agreement

A *key agreement scheme* is a cryptographic protocol in which two parties agree a shared secret, each using their private key and the other party’s public key.

A *key agreement scheme* KA defines a type of public keys KA*.*Public, a type of private keys KA*.*Private, and a type of shared secrets KA*.*SharedSecret.

Let KA*.*FormatPrivate ◦ B[亿PRF ] *→* KA*.*Private be a function that converts a bit string of length PRF to a KA private

◦

key.

Let KA*.*DerivePublic ◦ KA*.*Private *→* KA*.*Public be a function that derives the KA public key corresponding to a

◦

given KA private key.

Let KA*.*Agree ◦ KA*.*Private *×* KA*.*Public *→* KA*.*SharedSecret be the agreement function.

◦

**Note:** The range of KA*.*DerivePublic may be a strict subset of KA*.*Public.

#### Security requirements:

* + - * KA*.*FormatPrivate must preserve sufficient entropy from its input to be used as a secure KA private key.
      * The key agreement and the KDF defined in the next section must together satisfy a suitable adaptive security assumption along the lines of [[Bern2006,](#_bookmark144) section 3] or [[ABR1999,](#_bookmark134) Definition 3].

More precise formalization of these requirements is beyond the scope of this specification.

#### Key Derivation

A *Key Derivation Function* is defined for a particular *key agreement scheme* and *authenticated one-time sym- metric encryption scheme*; it takes the shared secret produced by the key agreement and additional arguments, and derives a key suitable for the encryption scheme.

Let KDF ◦ 1*..*Nnew B[ 亿 hSig ] KA*.*SharedSecret KA*.*Public KA*.*Public Sym*.***K** be a *Key Derivation Function*

◦

*{ } × × × × →*

suitable for use with KA, deriving keys for Sym*.*Encrypt.

**Security requir****ement:** In addition to adaptive security of the key agreement and KDF, the following security property is required:

enc

Let sk1

enc

and sk2

each be chosen uniformly and independently at random from KA*.*Private.

Let pkj := KA*.*DerivePublic(skjenc ).

enc

An adversary can adaptively query a function *Q* ◦ *{*1 *..* 2*} ×* B[亿hSig ] *→* KA*.*Public *×* Sym*.***K**1..Nnew where *Q*j (hSig ) is

◦

defined as follows:

1. Choose esk uniformly at random from KA*.*Private.
2. Let epk := KA*.*DerivePublic(esk).
3. For *i ∈ {*1*..*Nnew*}*, let Ki := KDF(*i,* hSig*,* KA*.*Agree(esk*,* pkj

enc

)*,* epk*,* pkj

enc

)).

1. Return (epk*,* K1..Nnew ).

Then the adversary must make another query to *Q*j with random unknown *j* 1 *..* 2 , and guess *j* with probability greater than chance.

*∈ { }*

If the adversary’s advantage is negligible, then the asymmetric encryption scheme constructed from KA, KDF and

Sym in [§4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22 will be key-private as defined in [[BBDP2001].](#_bookmark136)

**Note:** The given definition only requires ciphertexts to be indistinguishable between *transmission keys* that are outputs of KA*.*DerivePublic (which includes all keys generated as in [§ 4.2](#_bookmark37) *‘Key Components’* on p. 17). If a *trans- mission key* not in that range is used, it may be distinguishable. This is not considered to be a significant security weakness.

#### Signature

A signature scheme Sig defines:

* + - * a type of signing keys Sig*.*Private;
      * a type of verifying keys Sig*.*Public;
      * a type of messages Sig*.*Message;
      * a type of signatures Sig*.*Signature;
      * a randomized key pair generation algorithm Sig*.*Gen ◦ () R Sig*.*Private *×* Sig*.*Public;
        + *→*
      * a randomized signing algorithm Sig*.*Sign ◦ Sig*.*Private *×* Sig*.*Message R Sig*.*Signature;
        + *→*
      * a verifying algorithm Sig*.*Verify ◦ Sig*.*Public *×* Sig*.*Message *×* Sig*.*Signature *→* B;

◦

such that for any key pair (sk*,* vk) R

Sig*.*Gen(), and any *m* ◦ Sig*.*Message and *s* ◦ Sig*.*Signature R Sig*.*Sign

(*m*),

Sig*.*Verifyvk (*m, s*) = 1. *←*

* ◦ *←* sk

**Zcash** uses two signature schemes, one used for signatures that can be verified by script operations such as OP\_CHECKSIG and OP\_CHECKMULTISIG as in **Bitcoin**, and one called JoinSplitSig which is used to sign *transactions* that contain at least one *JoinSplit description*. The latter is instantiated in [§5.4.6](#_bookmark74) *‘Signature’* on p. 27. The following defines only the security properties needed for JoinSplitSig.

**Security requirement:** JoinSplitSig must be Strongly Unforgeable under (non-adaptive) Chosen Message Attack (SU-CMA), as defined for example in [[BDEHR2011,](#_bookmark141) Definition 6]. This allows an adversary to obtain signatures on chosen messages, and then requires it to be infeasible for the adversary to forge a previously unseen valid (message, signature) pair without access to the signing key.

#### Notes:

* + Since a fresh key pair is generated for every *transaction* containing a *JoinSplit description* and is only used for one signature (see [§ 4.6](#_bookmark43) *‘Non-malleability’* on p. 20), a one-time signature scheme would suffice for JoinSplitSig. This is also the reason why only security against *non-adaptive* chosen message attack is needed. In fact the instantiation of JoinSplitSig uses a scheme designed for security under adaptive attack even when multiple signatures are signed under the same key.
  + SU-CMA security requires it to be infeasible for the adversary, not knowing the private key, to forge a distinct signature on a previously seen message. That is, *JoinSplit signatures* are intended to be nonmalleable in the sense of [[BIP-62].](#_bookmark157)

#### Commitment

A *commitment scheme* is a function that, given a random *commitment trapdoor* and an input, can be used to commit to the input in such a way that:

* + - * no information is revealed about it without the *trapdoor* (“hiding”),
      * given the *trapdoor* and input, the commitment can be verified to “open” to that input and no other (“binding”).

A *commitment scheme* COMM defines a type of inputs COMM*.*Input, a type of commitments COMM*.*Output, and a type of *commitment trapdoors* COMM*.*Trapdoor.

Let COMM ◦ COMM*.*Trapdoor *×* COMM*.*Input *→* COMM*.*Output be a function satisfying the security requirements

◦

below.

#### Security requirements:

* + - * **Computational hiding:** For all *x, xt* ◦ COMM*.*Input, the distributions *{* COMM (*x*) *| r* R

COMM*.*Trapdoor *}*

* + - * + r *←*

and *{* COMM (*xt* ) *| r* R COMM*.*Trapdoor *}* are computationally indistinguishable.

r *←*

* + - * **Computational binding:** It is infeasible to find *x, xt* ◦ COMM*.*Input and *r, rt* ◦ COMM*.*Trapdoor such that *x* \* *xt*

◦ ◦

and COMMr (*x*) = COMMr*I* (*xt* ).

#### Represented Group

A *represented group* G consists of:

* + - * a subgroup order parameter *r*G ◦◦ N+, which must be prime;
      * a cofactor parameter *h*G ◦◦ N+;
      * a group G of order *h*G *· r*G, written additively with operation + ◦ G *×* G *→* G, and additive identity *O*G ;

◦

* + - * a generator *P*G of the subgroup of G of order *r*G;
      * a bit-length parameter G ◦ N;

◦

* + - * a representation function reprG ◦ G *→* B[亿G ];

◦

* + - * an abstraction function abstG ◦ B[亿G ] *→* G *∪ {⊥}*;

◦

such that abstG is the left inverse of reprG , i.e. for all *P ∈* G, abstG (reprG (*P* )) = *P* , and for all *S* not in the image of

reprG , abstG (*S*) = *⊥*.

We extend the  notation to addition on group elements. For *G* ◦ G and *s* ◦ N (or *s* ◦ FrG ) we write **[***s***]***G* for  *G*.

s

◦

◦

◦

i=1

#### Represented Pairing

A *represented pairing* P consists of:

* + - * a group order parameter *r*P ◦◦ N+ which must be prime;
      * two *represented groups* P1..2, both of order *r*P;
      * a group PT of order *r*P, written multiplicatively with operation *·* ◦ PT *×* PT *→* PT and multiplicative identity

◦

**1**P;

* + - * a pairing function *e*ˆP ◦ P1 *×* P2 *→* PT satisfying:

◦

* (Bilinearity) for all *a, b* ◦◦ Fr*∗*, *P* ◦◦ P1, and *Q* ◦◦ P2, *e*ˆP (**[***a***]***P,* **[***b***]***Q*) = *e*ˆP (*P, Q*)a*·*b, and
* (Nondegeneracy) there does not exist *P* ◦ P1 *\ O*P1 such that for all *Q* ◦ P2*, e*ˆP (*P, Q*) = **1**P;

◦

◦

#### Zero-Knowledge Proving System

A *zero-knowledge proving system* is a cryptographic protocol that allows proving a particular *statement* , de- pendent on *primary* and *auxiliary inputs*, in zero knowledge — that is, without revealing information about the *auxiliary inputs* other than that implied by the *statement* . The type of *zero-knowledge proving system* needed by **Zcash** is a *preprocessing zk-SNARK* .

A *preprocessing zk-SNARK* instance ZK defines:

* + - * a type of *zero-knowledge proving keys*, ZK*.*ProvingKey;
      * a type of *zero-knowledge verifying keys*, ZK*.*VerifyingKey;
      * a type of *primary inputs* ZK*.*PrimaryInput;
      * a type of *auxiliary inputs* ZK*.*AuxiliaryInput;
      * a type of proofs ZK*.*Proof;
      * a type ZK*.*SatisfyingInputs *⊆* ZK*.*PrimaryInput *×* ZK*.*AuxiliaryInput of inputs satisfying the *statement* ;
      * a randomized key pair generation algorithm ZK*.*Gen ◦ () R ZK*.*ProvingKey *×* ZK*.*VerifyingKey;
        + *→*
      * a proving algorithm ZK*.*Prove ◦ ZK*.*ProvingKey *×* ZK*.*SatisfyingInputs *→* ZK*.*Proof;

◦

* + - * a verifying algorithm ZK*.*Verify ◦ ZK*.*VerifyingKey *×* ZK*.*PrimaryInput *×* ZK*.*Proof *→* B;

◦

The security requirements below are supposed to hold with overwhelming probability for (pk*,* vk) R ZK*.*Gen().

*←*

#### Security requirements:

* + - * **Completeness:** An honestly generated proof will convince a verifier: for any (*x, w*) ZK*.*SatisfyingInputs, if

*∈*

ZK*.*Provepk (*x, w*) outputs *π*, then ZK*.*Verifyvk (*x, π*) = 1.

* + - * **Knowledge Soundness:** For any adversary *A* able to find an *x* ◦ ZK*.*PrimaryInput and proof *π* ◦ ZK*.*Proof

◦

◦

such that ZK*.*Verifyvk (*x, π*) = 1, there is an efficient extractor *E* such that if *E* (vk*,* pk) returns *w*, then the probability that (*x, w*) < ZK*.*SatisfyingInputs is negligable.

*A A*

* + - * **Statistical Zero Knowledge:** An honestly generated proof is statistical zero knowledge. That is, there is a feasible stateful simulator such that, for all stateful distinguishers , the following two probabilities are negligibly close:

*S D*

 (*x, w*) *∈* ZK*.*SatisfyingInputs

(pk*,* vk) *←*R ZK*.*Gen() 

R

R

*,* R

(*x, w*) *∈* ZK*.*SatisfyingInputs R

(pk vk) *← S* ()







R

Pr

*D*(*π*) = 1

(*x, w*) *← D*(pk*,* vk)

*π ←* ZK*.*Provepk (*x, w*)

 and Pr

*D*(*π*) = 1

(*x, w*) *← D*(pk*,* vk) 

*π ← S* (*x*)

These definitions are derived from those in [[BCTV2014,](#_bookmark139) Appendix C], adapted to state concrete security for a fixed circuit, rather than asymptotic security for arbitrary circuits. (ZK*.*Prove corresponds to *P* , ZK*.*Verify corresponds

to *V* , and ZK*.*SatisfyingInputs corresponds to *R*C in the notation of that appendix.)

The Knowledge Soundness definition is a way to formalize the property that it is infeasible to find a new proof *π* where ZK*.*Verifyvk (*x, π*) = 1 without *knowing* an *auxiliary input w* such that (*x, w*) ZK*.*SatisfyingInputs. Note that Knowledge Soundness implies Soundness — i.e. the property that it is infeasible to find a new proof *π* where

*∈*

ZK*.*Verifyvk (*x, π*) = 1 without *there existing* an *auxiliary input w* such that (*x, w*) *∈* ZK*.*SatisfyingInputs.

It is possible to replay proofs, but informally, a proof for a given (*x, w*) gives no information that helps to find a proof for other (*x, w*).

The *proving system* is instantiated in [§ 5.4.9.1](#_bookmark80) *‘PHGR13’* on p. 29. ZKJoinSplit refers to this *proving system* with the BN-254 pairing, specialized to the *JoinSplit statement* given in [§4.9.1](#_bookmark48) *‘JoinSplit Statement’* on p. 21. In this case we omit the key subscripts on ZKJoinSplit*.*Prove and ZKJoinSplit*.*Verify, taking them to be the particular *proving key* and *verifying key* defined by the *JoinSplit parameters* in [§5.7](#_bookmark92) *‘zk-SNARK Parameters’* on p. 33.

## Key Components

Let PRFaddr be a *Pseudo Random Function*, instantiated in [§5.4.2](#_bookmark69) *‘Pseudo Random Functions’* on p. 26. Let KA be a *key agreement scheme*, instantiated in [§5.4.4](#_bookmark72) *‘Key Agreement’* on p. 27.

A new *spending key* ask is generated by choosing a bit string uniformly at random from B[亿ask ].

apk, skenc and pkenc are derived from ask as follows:

apk := PRFaddr (0)

ask

skenc := KA*.*FormatPrivate(PRFaddr (1)) pkenc := KA*.*DerivePublic(skenc ).

ask

## JoinSplit Descriptions

A *JoinSplit transfer* , as specified in [§3.5](#_bookmark16) *‘JoinSplit Transfers and Descriptions’* on p. 10, is encoded in *transactions*

as a *JoinSplit description*.

Each *transaction* includes a sequence of zero or more *JoinSplit descriptions*. When this sequence is non-empty, the *transaction* also includes encodings of a JoinSplitSig public verification key and signature.

A *JoinSplit description* consists of (vold *,* vnew*,* rt*,* nfold

old *,* cmnew new *,* epk*,* randomSeed*,* h

old *, π*JoinSplit*,* Cenc new )

where

pub

pub

1..N

1..N

1..N

1..N

* + - vold
* *{*0 *..* MAX\_MONEY*}* is the value that the *JoinSplit transfer* removes from the *transparent value pool* ;

pub ◦

* + vnew ◦ *{*0 *..* MAX\_MONEY*}* is the value that the *JoinSplit transfer* inserts into the *transparent value pool* ;

pub ◦

* + rt ◦ B[ 亿 Merkle ] is an *anchor* , as defined in [§ 3.3](#_bookmark14) *‘The Block Chain’* on p. 9, for the output *treestate* of either a previous *block* , or a previous *JoinSplit transfer* in this *transaction*.

◦

* + nfold
* B[亿PRF ][Nold ] is the sequence of *nullifiers* for the input *notes*;

1..Nold ◦

* + cmnew new ◦ COMM*.*Output[Nnew ] is the sequence of *note commitments* for the output *notes*;

1..N ◦

* + epk ◦ KA*.*Public is a key agreement public key, used to derive the key for encryption of the *transmitted notes ciphertext* [(§4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22);

◦

* + randomSeed ◦ B[亿Seed ] is a seed that must be chosen independently at random for each *JoinSplit description*;

◦

* + h1..Nold ◦ B is a sequence of tags that bind hSig to each ask of the input *notes*;
* [亿PRF ][Nold ]
  + *π*JoinSplit ◦ ZKJoinSplit*.*Proof is the *zero-knowledge proof* for the *JoinSplit statement* ;

◦

* + Cenc new ◦ Sym*.***C**[Nnew ] is a sequence of ciphertext components for the encrypted output *notes*.

1..N ◦

The ephemeralKey and encCiphertexts fields together form the *transmitted notes ciphertext* .

The value hSig is also computed from randomSeed, nfold

1..N

old , and the joinSplitPubKey of the containing *transaction*:

hSig := hSigCRH(randomSeed*,* nfold

1..N

old *,* joinSplitPubKey).

hSigCRH is instantiated in [§5.4.1.2](#_bookmark66) *‘*hSig *Hash Function’* on p. 25.

#### Consensus rules:

* + Elements of a *JoinSplit description* **MUST** have the types given above (for example: 0 *≤* vold

*≤* MAX\_MONEY

and 0 *≤* vnew *≤* MAX\_MONEY).

pub

pub

* + Either vold or vnew **MUST** be zero.

pub

pub

* + The proof *π*JoinSplit **MUST** be valid given a *primary input* formed from the other fields and hSig. I.e. it must

be the case that ZKJoinSplit*.*Verify((rt*,* nfold old *,* cmnew new *,* vold *,* vnew*,* hSig*,* h old )*, π*JoinSplit) = 1.

1..N

1..N

pub

pub

1..N

## Sending Notes

In order to send *shielded* value, the sender constructs a *transaction* containing one or more *JoinSplit descriptions*. This involves first generating a new JoinSplitSig key pair:

(joinSplitPrivKey*,* joinSplitPubKey) R JoinSplitSig*.*Gen().

*←*

For each *JoinSplit description*, the sender chooses randomSeed uniformly at random on B[ 亿 Seed ], and selects the input *notes*. At this point there is sufficient information to compute hSig, as described in the previous section. The sender also chooses ϕ uniformly at random on B[亿ϕ]. Then it creates each output *note* with index *i* ◦ *{*1*..*Nnew*}* as

◦

follows:

* + - Choose rnew uniformly at random on B[ 亿 r ].

i

* + - Compute ρnew := PRFρ (*i,* h ).

i ϕ Sig

* + - Encrypt the *note* to the recipient *transmission key* pknew , as described in [§4.10](#_bookmark54) *‘In-band secret distribution’*

on p. 22, giving the ciphertext component Cenc.

i

enc,i

In order to minimize information leakage, the sender **SHOULD** randomize the order of the input *notes* and of the output *notes*. Other considerations relating to information leakage from the structure of *transactions* are beyond the scope of this specification.

After generating all of the *JoinSplit descriptions*, the sender obtains the dataToBeSigned [(§ 4.6](#_bookmark43) *‘Non-malleability’*

on p. 20), and signs it with the private *JoinSplit signing key* :

joinSplitSig R JoinSplitSig*.*Sign

*←*

joinSplitPrivKey

(dataToBeSigned)

Then the encoded *transaction* including joinSplitSig is submitted to the network.

#### Dummy Notes

The fields in a *JoinSplit description* allow for Nold input *notes*, and Nnew output *notes*. In practice, we may wish to encode a *JoinSplit transfer* with fewer input or output *notes*. This is achieved using *dummy notes*.

A *dummy* input *note*, with index *i* in the *JoinSplit description*, is constructed as follows:

* + - * Generate a new random *spending key* aold and derive its *paying key* aold .

sk,i

pk,i

* + - * Set vold := 0.

i

* + - * Choose ρold uniformly at random on B[ 亿 PRF ].

i

* + - * Choose rold uniformly at random on B[ 亿 r ].

i

* + - * Compute nfold := PRFnf (ρold ).

i old i

a

sk*,i*

* + - * Construct a *dummy path* pathi for use in the *auxiliary input* to the *JoinSplit statement* (this will not be checked).
      * When generating the *JoinSplit proof* , set enforceMerklePathi to 0.

A *dummy* output *note* is constructed as normal but with zero value, and sent to a random *payment address*.

## Merkle path validity

The depth of the *note commitment tree* is dMerkle (defined in [§5.3](#_bookmark61) *‘Constants’* on p. 24).

Each *node* in the *incremental Merkle tree* is associated with a *hash value*, which is a byte sequence. The *layer*

numbered *h*, counting from *layer* 0 at the *root* , has 2h *nodes* with *indices* 0 to 2h *−* 1 inclusive.

Let Mh be the *hash value* associated with the *node* at *index i* in *layer h*.

i

The *nodes* at *layer* dMerkle are called *leaf nodes*. When a *note commitment* is added to the tree, it occupies the *leaf node hash value* MdMerkle for the next available *i*. As-yet unused *leaf nodes* are associated with a distinguished *hash value* Uncommitted. It is assumed to be infeasible to find a preimage *note* **n** such that NoteCommitment(**n**) = Uncommitted.

i

The *nodes* at *layers* 0 to dMerkle *−* 1 inclusive are called *internal nodes*, and are associated with MerkleCRH outputs.

*Internal nodes* are computed from their children in the next *layer* as follows: for 0 *≤ h <* dMerkle and 0 *≤ i <* 2h,

Mh := MerkleCRH(Mh+1*,* Mh+1 ).

i 2i 2i+1

A *path* from *leaf* *node* MdMerkle in the *incremental Merkle tree* is the sequence

i

h

[ M

sibling

(h,i) for *h* from dMerkle down to 1 ],

where

sibling(*h, i*) := floor（ 2d

i *−h* ＼ *⊕* 1

Merkle

Given such a *path*, it is possible to verify that *leaf node* MdMerkle is in a tree with a given *root* rt = M0.

i 0

## Non-malleability

**Bitcoin** defines several *SIGHASH types* that cover various parts of a transaction. In **Zcash**, all of these *SIGHASH types* are extended to cover the **Zcash**-specific fields nJoinSplit, vJoinSplit, and (if present) joinSplitPubKey, described in [§6.1](#_bookmark94) *‘Encoding of Transactions’* on p. 34. They *do not* cover the field joinSplitSig.

比特币定义了几种SIGHASH类型，涵盖交易的各个部分。 在Zcash中，所有这些SIGHASH类型都被扩展以覆盖第6.1节“事务的编码”中描述的Zcash特定字段nJoinSplit，vJoinSplit和（如果存在）joinSplitPubKey。 34.他们不包括joinSplitSig字段。

**Consensus rule:** If nJoinSplit *>* 0, the *transaction* **MUST NOT** use *SIGHASH types* other than SIGHASH\_ALL.

如果nJoinSplit> 0，则交易不得使用SIGHASH\_ALL以外的SIGHASH类型

Let dataToBeSigned be the hash of the *transaction* using the SIGHASH\_ALL *SIGHASH type*. This *excludes* all of the

scriptSig fields in the non-**Zcash**-specific parts of the *transaction*.

让dataToBeSigned作为使用SIGHASH\_ALL SIGHASH类型的交易的散列。这排除了交易的非Zcash特定部分中的所有scriptSig字段。

In order to ensure that a *JoinSplit description* is cryptographically bound to the *transparent* inputs and outputs corresponding to vnew and vold , and to the other *JoinSplit descriptions* in the same *transaction*, an ephemeral

pub pub

JoinSplitSig key pair is generated for each *transaction*, and the dataToBeSigned is signed with the private sign- ing key of this key pair. The corresponding public verification key is included in the *transaction* encoding as joinSplitPubKey.

为了确保JoinSplit描述被密码绑定到与vnew和vold相对应的透明输入和输出以及同一交易中的其他JoinSplit描述，将为每个交易生成一个短暂的JoinSplitSig密钥对，并且dataToBeSigned 用这个密钥对的私钥签名。相应的公开验证密钥作为joinSplitPubKey包含在交易编码中。

JoinSplitSig is instantiated in [§5.4.6](#_bookmark74) *‘Signature’* on p. 27.

If nJoinSplit is zero, the joinSplitPubKey and joinSplitSig fields are omitted. Otherwise, a *transaction* has a correct *JoinSplit signature* if and only if JoinSplitSig*.*VerifyjoinSplitPubKey (dataToBeSigned*,* joinSplitSig) = 1.

If nJoinSplit = 0 , 则joinSplitPubKey 和 joinSplitSig 字段省略；

Else 签名正确的充要条件是 JoinSplitSig*.*VerifyjoinSplitPubKey (dataToBeSigned*,* joinSplitSig) = 1 。

Let hSig be computed as specified in [§ 4.3](#_bookmark38) *‘JoinSplit Descriptions’* on p. 17, and let PRFpk be as defined in [§ 4.1.2](#_bookmark24)

*‘Pseudo Random Functions’* on p. 12.

For each *i ∈ {*1*..*Nold*}*, the creator of a *JoinSplit description* calculates hi

= PRFpk

sk*,i*

aold

(*i,* hSig ).

The correctness of h1..Nold is enforced by the *JoinSplit statement* given in [§ 4.9.1](#_bookmark52) *‘Non-malleability’* on p. 22.

通过JoinSplit语句强制执行h1..Nold的正确性

This ensures that a holder of all of the aold old for every *JoinSplit description* in the *transaction* has authorized the use of the private signing key corresponding to joinSplitPubKey to sign this *transaction*.

sk,1..N

这确保了交易中每个JoinSplit描述的所有aold的持有者已经授权使用与joinSplitPubKey相对应的私人签名密钥来签署此交易。

## Balance

A *JoinSplit transfer* can be seen, from the perspective of the *transaction*, as an input and an output simultaneously.

vold takes value from the *transparent value pool* and vnew adds value to the *transparent value pool* . As a result, vold

pub

new

pub

pub

is treated like an *output* value, whereas vpub is treated like an *input* value.

**Note:** Unlike original **Zerocash** [[BCG+2014],](#_bookmark137) **Zcash** does not have a distinction between Mint and Pour operations. The addition of vold to a *JoinSplit description* subsumes the functionality of both Mint and Pour. Also, a difference in the number of real input *notes* does not by itself cause two *JoinSplit descriptions* to be distinguishable.

pub

与原Zerocash [BCG + 2014]不同，Zcash没有区分Mint和Pour操作。 向JoinSplit描述添加v包含了Mint和Pour的功能。 此外，实际输入票据数量的差异本身并不会导致可以区分两个JoinSplit描述。

As stated in [§4.3](#_bookmark38) *‘JoinSplit Descri ptions’* on p. 17, either vold or vnew **MUST** be zero. No generality is lost because,

pub

pub

if a *transaction* in which both vold and vnew were nonzero were allowed, it could be replaced by an equivalent

pub

pub

one in which min(vold *,* vnew ) is subtracted from both of these values. This restriction helps to avoid unnecessary

pub pub

distinctions between *transactions* according to client implementation.

正如§4.3“JoinSplit描述”中所述。 vold或vnew必须为零。 没有一般性损失，因为如果允许vold和vnew不为零的交易，它可以由相等的一个代替min（vold，vnew）从这两个值中减去。 这种限制有助于避免根据客户实施情况在交易之间进行不必要的区分

## Note Commitments and Nullifiers

A *transaction* that contains one or more *JoinSplit descriptions*, when entered into the *block chain*, appends to the *note commitment tree* with all constituent *note commitments*. All of the constituent *nullifiers* are also entered into the *nullifier set* of the associated *treestate*. A *transaction* is not valid if it attempts to add a *nullifier* to the *nullifier set* that already exists in the set.

包含一个或多个JoinSplit描述的交易（在加入到区块链中时）会将其对应的票据承诺附加到其票据承诺树中。 所有组成的否定器也被输入到相关状态树的否定器集合中。 如果交易尝试向否定器集合中添加已经存在的否定器，则该交易无效。

## Zk-SNARK Statements

#### JoinSplit Statement

A valid instance of *π*JoinSplit assures that given a *primary input* :

(rt ◦ B[亿Merkle ]*,*

◦

nfold ◦ B[亿PRF ][Nold ]*,*

1..Nold ◦

cmnew new ◦ COMM*.*Output[Nnew ]*,*

1..N ◦

vold

* *{*0 *..* 264 *−* 1*},*

pub ◦

vnew ◦ *{*0 *..* 264 *−* 1*},*

pub ◦

hSig ◦◦ B[亿hSig ]*,*

h ◦ B[亿PRF ][Nold ] ),

1..Nold ◦

the prover knows an *auxiliary input* :

(path

**n**old

* B[亿Merkle ][dMerkle ][Nold ]*,*
* Note[Nold ]*,*

1..Nold ◦

1..Nold ◦

aold

* B[亿ask ][Nold ]*,*

sk,1..Nold ◦

**n**new new ◦ Note[Nnew ]*,*

1..N ◦

ϕ ◦ B[亿ϕ]*,*

◦

enforceMerklePath

* B[Nold ] ),

1..Nold ◦

where:

for each *i ∈ {*1*..*Nold*}*: **n**old = (aold *,* vold*,* ρold*,* rold );

i

pk,i

i

i

i

for each *i ∈ {*1*..*Nnew*}*: **n**new = (anew *,* vnew*,* ρnew*,* rnew )

i

pk,i

i

i

i

such that the following conditions hold:

**Merkle path validity** for each *i* 1*..*Nold enforceMerklePathi = 1: path must be a valid *path* of depth dMerkle, as defined in [§4.5](#_bookmark41) *‘Merkle path validity’* on p. 19, from NoteCommitment(**n**old ) to *note commitment tree* root rt.

i

*∈ { } |* i

**Note:** Merkle path validity covers both conditions 1. (a) and 1. (d) of the NP statement given in [[BCG+2014,](#_bookmark137) section 4.2].

**Merkle path enforcement** for each *i ∈ {*1*..*Nold*}*, if vold \* 0 then enforceMerklePathi = 1.

i

Nold Nnew

pub

i

pub

i

**Balance** vold

+  vold = vnew +  vnew *∈ {*0 *..* 264 *−* 1*}*.

i=1

i=1

i=1

i=1

**Nullifier integrity** for each *i ∈ {*1*..*Nold*}*: nfold = PRFnf

i

aold

sk*,i*

i

(ρold ).

**Spend authority** for each *i ∈ {*1*..*Nold*}*: aold

pk,i

= PRFaddr (0).

sk*,i*

aold

**Non-malleability** for each *i ∈ {*1*..*Nold*}*: hi

= PRFpk

sk*,i*

aold

(*i,* hSig ).

**Uniqueness of** ρnew

i

for each *i ∈ {*1*..*Nnew*}*: ρnew = PRFρ (*i,* h ).

**Commitment integrity** for each *i ∈ {*1*..*Nnew*}*: cmnew = NoteCommitment(**n**new ). For details of the form and encoding of proofs, see [§5.4.9.1](#_bookmark80) *‘PHGR13’* on p. 29.

i

ϕ

Sig

i

i

## In-band secret distribution

In order to transmit the secret v, ρ, 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 key* pkenc is used to encrypt these secrets. The recipient’s possession of the associated *incoming viewing key* (apk*,* skenc ) is used to reconstruct the original *note* and *memo field* .

为了在不需要带外通信信道的情况下发送秘密v，ρ和r（对于接收者来说稍后花费是必需的）以及备忘录字段，传输密钥pkenc被用于加密这些秘密。 接收者拥有相关的传入查看键（apk，skenc）用于重建原始票据和备忘录字段。

All of the resulting ciphertexts are combined to form a *transmitted notes ciphertext* . For both encryption and decryption,

* + - Let Sym be the *encryption scheme* instantiated in [§5.4.3](#_bookmark70) *‘Authenticated One-Time Symmetric Encryption’*

on p. 26.

* + - Let KDF be the *Key Derivation Function* instantiated in [§5.4.5](#_bookmark73) *‘Key Derivation’* on p. 27.
    - Let KA be the *key agreement scheme* instantiated in [§5.4.4](#_bookmark72) *‘Key Agreement’* on p. 27.
    - Let hSig be the value computed for this *JoinSplit description* in [§4.3](#_bookmark38) *‘JoinSplit Descriptions’* on p. 17.

#### Encryption

new enc,1..N

Let pk

new be the *transmission keys* for the intended recipient addresses of each new *note*.

Let **np**1..Nnew be the *note plaintexts* as defined in [§5.5](#_bookmark82) *‘Note Plaintexts and Memo Fields’* on p. 30. Then to encrypt:

* + - * Generate a new KA (public, private) key pair (epk*,* esk).
      * For *i* 1*..*Nnew ,

*∈ { }*

* + - * + Let Penc be the raw encoding of **np** .

i i

* + - * + Let sharedSecreti := KA*.*Agree(esk*,* pknew ).

enc,i

* + - * + Let Kenc := KDF(*i,* hSig*,* sharedSecreti*,* epk*,* pknew ).

i

* + - * + Let Cenc := Sym*.*Encrypt

enc (Penc ).

enc,i

i K*i* i

The resulting *transmitted notes ciphertext* is (epk*,* Cenc new ).

1..N

**Note:** It is technically possible to replace Cenc for a given *note* with a random (and undecryptable) dummy ci- phertext, relying instead on out-of-band transmission of the *note* to the recipient. In this case the ephemeral key **MUST** still be generated as a random public key (rather than a random bit string) to ensure indistinguishability from other *JoinSplit descriptions*. This mode of operation raises further security considerations, for example of how to validate a *note* received out-of-band, which are not addressed in this document.

i

在技术上可以用一个随机的（和不可加密的）伪密文替换一个给定音符的Cenc，而不是将票据带外传输给接收者。 在这种情况下，临时密钥仍然必须作为随机公钥（而不是随机位串）生成，以确保与其他JoinSplit描述不可区分。 这种操作模式引发了进一步的安全考虑，例如如何验证带外收到的票据，本文没有涉及。

#### Decryption by a Recipient

Let ivk = (apk*,* skenc ) be the recipient’s *incoming viewing key* , and let pkenc be the corresponding *transmission key*

derived from skenc as specified in [§4.2](#_bookmark37) *‘Key Components’* on p. 17. Let cmnew new be the *note commitments* of each output coin.

1..N

Then for each *i ∈ {*1*..*Nnew*}*, the recipient will attempt to decrypt that ciphertext component as follows:

* + - * Let sharedSecreti := KA*.*Agree(skenc*,* epk).
      * Let Kenc := KDF(*i,* hSig*,* sharedSecreti*,* epk*,* pkenc ).

i

* + - * Return DecryptNote(Kenc*,* Cenc*,* cmnew*,* apk )*.*

i

i

i

DecryptNote(Kenc*,* Cenc*,* cmnew*,* apk ) is defined as follows:

i

i

i

* + - * Let Penc := Sym*.*Decrypt enc (Cenc ).

i K*i* i

* + - * If Penc = *⊥*, return *⊥*.

i

* + - * Extract **np** = (vnew*,* ρnew*,* rnew*,* memoi) from Penc.

i i i i i

* + - * If NoteCommitment((apk*,* vnew*,* ρnew*,* rnew )) \* cmnew, return *⊥*, else return **np** .

i

i

i

i

i

To test whether a *note* is unspent in a particular *block chain* also requires the *spending key* ask; the coin is unspent if and only if nf = PRFnf (ρ) is not in the *nullifier set* for that *block chain*.

ask

#### Notes:

* + - * The decryption algorithm corresponds to step 3 (b) i. and ii. (first bullet point) of the Receive algorithm shown in [[BCG+2014,](#_bookmark137) Figure 2].
      * A *note* can change from being unspent to spent as a node’s view of the best *block chain* is extended by new *transactions*. Also, *block chain* reorganisations can cause a node to switch to a different best *block chain* that does not contain the *transaction* in which a *note* was output.
      * •由于新交易扩展了最佳块链的节点视图，所以票据可以从未使用变为已花费。 此外，块链重组可能会导致节点切换到不包含输出票据的交易的不同最佳块链。

See [§ 7.7](#_bookmark124) *‘In-band secret distribution’* on p. 47 for further discussion of the security and engineering rationale behind this encryption scheme.

# Concrete Protocol

## Caution

TODO: Explain the kind of things that can go wrong with linkage between abstract and concrete protocol. E.g. [§ 7.5](#_bookmark121)

*‘Internal hash collision attack and fix’* on p. 46

## Integers, Bit Sequences, and Endianness

All integers in ***Zcash****-specific* encodings are unsigned, have a fixed bit length, and are encoded in little-endian byte order *unless otherwise specified*.

除非另有说明，Zcash特定编码中的所有整数都是无符号的，具有固定的位长度，并且按小端字节顺序编码。

In bit layout diagrams, each box of the diagram represents a sequence of bits. Diagrams are read from left-to-right, with lines read from top-to-bottom; the breaking of boxes across lines has no significance. The bit length is given explicitly in each box, except for the case of a single bit, or for the notation [0] 亿 representing the sequence of zero bits.

The entire diagram represents the sequence of *bytes* formed by first concatenating these bit sequences, and then treating each subsequence of 8 bits as a byte with the bits ordered from *most significant* to *least significant*. Thus the *most significant* bit in each byte is toward the left of a diagram. Where bit fields are used, the text will clarify their position in each case.

## Constants

Define:

dMerkle ◦ N := 29 Nold ◦ N := 2 Nnew ◦ N := 2

◦

◦

◦

Merkle ◦ N := 256

◦

hSig ◦ N := 256

◦

PRF ◦ N := 256

◦

r ◦ N := 256

◦

Seed ◦ N := 256

◦

ask ◦ N := 252

◦

ϕ ◦ N := 252

◦

Uncommitted ◦ B[ 亿 Merkle ] := [0] 亿 Merkle MAX\_MONEY ◦ N := 2*.*1 *·* 1015 (*zatoshi* ) SlowStartInterval ◦ N := 20000 HalvingInterval ◦ N := 840000 MaxBlockSubsidy ◦ N := 1*.*25 *·* 109 (*zatoshi* ) NumFounderAddresses ◦ N := 48 FoundersFraction ◦ Q := 1

◦

◦

◦

◦

◦

◦

* + - 5

PoWLimit N :

=

◦

（2243 *−* 1*,* for the production network

* 2251
* 1*,* for the test network

PoWAveragingWindow ◦ N := 17

◦

PoWMedianBlockSpan ◦ N := 11

◦

PoWMaxAdjustDown ◦ Q := 32

* + 100

PoWMaxAdjustUp ◦ Q := 16

* 100

PoWDampingFactor ◦ N := 4

◦

PoWTargetSpacing ◦ N := 150 (seconds).

◦

## Concrete Cryptographic Schemes

#### Hash Functions

#### Merkle Tree Hash Function

MerkleCRH is used to hash *incremental Merkle tree hash values*. It is instantiated by the *SHA-256 compression*

function, which takes a 512-bit block and produces a 256-bit hash. [[NIST2015]](#_bookmark185)

MerkleCRH(left*,* right) := SHA256Compress （ ＼.

256-bit left

256-bit right

**Note:** SHA256Compress is not the same as the SHA-256 function, which hashes arbitrary-length byte sequences.

**Security requirement:** SHA256Compress must be collision-resistant, and it must be infeasible to find a preimage

*x* such that SHA256Compress(*x*) = [0]256.

* + - 1. hSig **Hash Function**

hSigCRH is used to compute the value hSig in [§4.3](#_bookmark38) *‘JoinSplit Descriptions’* on p. 17.

hSigCRH(randomSeed*,* nfold old *,* joinSplitPubKey) := BLAKE2b-256(**“ZcashComputehSig"***,* hSigInput)

1..N

where

hSigInput := .

|  |  |  |  |
| --- | --- | --- | --- |
| 256-bit randomSeed | 256-bit nfold ...  1 | 256-bit nfold  Nold | 256-bit joinSplitPubKey |

BLAKE2b-256(*p, x*) refers to unkeyed BLAKE2b-256 [[ANWW2013]](#_bookmark135) in sequential mode, with an output digest length of 32 bytes, 16-byte personalization string *p*, and input *x*. This is not the same as BLAKE2b-512 truncated to 256 bits, because the digest length is encoded in the parameter block.

**Security requirement:** BLAKE2b-256(**“ZcashComputehSig"***, x*) must be collision-resistant.

#### Equihash Generator

EquihashGenn,k is a specialized hash function that maps an input and an index to an output of length *n* bits. It is used in [§6.4.1](#_bookmark101) *‘Equihash’* on p. 39.

Let powtag := .

|  |  |  |
| --- | --- | --- |
| 64-bit **“ZcashPoW"** | 32-bit *n* | 32-bit *k* |

Let powcount(*g*) := .

32-bit *g*

Let EquihashGenn,k (*S, i*) := *T*h+1 .. h+n, where

*m* := floor（ ）;

512

n

*h* := (*i −* 1 mod *m*) *· n*;

*T* := BLAKE2b-(*n · m*)(powtag*, S ||* powcount(floor（ i*−*1 ）)).

m

Indices of bits in *T* are 1-based.

BLAKE2b- (*p, x*) refers to unkeyed BLAKE2b- [[ANWW2013]](#_bookmark135) in sequential mode, with an output digest length of

*/*8 bytes, 16-byte personalization string *p*, and input *x*. This is not the same as BLAKE2b-512 truncated to bits, because the digest length is encoded in the parameter block.

BLAKE2b-（p，x）指序列模式下的无键BLAKE2b- [ANWW2013]，输出摘要长度为1/8字节，16字节个性化字符串p和输入x。 这与BLAKE2b-512截断为位不同，因为摘要长度在参数块中编码。

**Security requirement:** BLAKE2b- (powtag*, x*) must generate output that is sufficiently unpredictable to avoid short-cuts to the Equihash solution process. It would suffice to model it as a random oracle.

BLAKE2b-（powtag，x）必须产生足够不可预测的输出以避免Equihash解决方案过程的快捷方式。 将它建模为随机预言就足够了。

**Note:** When EquihashGen is evaluated for sequential indices, as in the Equihash solving process [(§6.4.1](#_bookmark101) *‘Equihash’*

on p. 39), the number of calls to BLAKE2b can be reduced by a factor of floor（ 512 ） in the best case (which is a factor

n

of 2 for *n* = 200).

#### Pseudo Random Functions

The four independent PRFs described in [§4.1.2](#_bookmark24) *‘Pseudo Random Functions’* on p. 12 are all instantiated using the

*SHA-256 compression* function:

PRFaddr (*t*) := SHA256Compress （ ＼

x

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 0 | 252-bit *x* | 8-bit *t* | [0]248 |

PRFnf (ρ) := SHA256Compress （ ＼

ask

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 0 | 252-bit ask | 256-bit ρ |

PRFpk (*i,* h ) := SHA256Compress （ ＼

ask

Sig

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | i-1 | 0 | 0 | 252-bit ask | 256-bit hSig |

PRFρ (*i,* h ) := SHA256Compress （ ＼

ϕ

Sig

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | i-1 | 1 | 0 | 252-bit ϕ | 256-bit hSig |

#### Security requirements:

* + - * The *SHA-256 compression* function must be collision-resistant.
      * The *SHA-256 compression* function must be a PRF when keyed by the bits corresponding to *x*, ask or ϕ in the above diagrams, with input in the remaining bits.

**Note:** The first four bits –i.e. the most significant four bits of the first byte– are used to distinguish different uses of SHA256Compress, ensuring that the functions are independent. In addition to the inputs shown here, the bits 1011 in this position are used to distinguish uses of the full SHA-256 hash function — see [§ 5.4.7](#_bookmark75) *‘Commitment’* on p. 28. (The specific bit patterns chosen here are motivated by the possibility of future extensions that either increase Nold and/or Nnew to 3, or that add an additional bit to ask to encode a new key type, or that require an additional PRF.)

前四位 - 即。 第一个字节的最重要的四位 - 用于区分SHA256Compress的不同用途，确保这些功能是独立的。 除了此处显示的输入外，位于此位置的位1011用于区分完整SHA-256散列函数的使用

#### Authenticated One-Time Symmetric Encryption

Let Sym*.***K** := B[256], Sym*.***P** := B[8*·*N], and Sym*.***C** := B[8*·*N].

Let Sym*.*EncryptK (P) be authenticated encryption using AEAD\_CHACHA20\_POLY1305 [[RFC-7539]](#_bookmark188) encryption of plaintext P *∈* Sym*.***P**, with empty “associated data", all-zero nonce [0]96, and 256-bit key K *∈* Sym*.***K**.

让Sym.EncryptK（P）使用AEAD\_CHACHA20\_POLY1305 [RFC-7539]加密明文P∈Sym.P，其组成为空的“关联数据”，全零nonce [0] 96和256位密钥K∈Sym.K。

Similarly, let Sym*.*DecryptK (C) be AEAD\_CHACHA20\_POLY1305 decryption of ciphertext C *∈* Sym*.***C**, with empty “associated data", all-zero nonce [0]96, and 256-bit key K *∈* Sym*.***K**. The result is either the plaintext byte sequence, or *⊥* indicating failure to decrypt.

类似地，令Sym.DecryptK（C）为AEAD\_CHACHA20\_POLY1305解密密文C∈Sym.C，其中有空的“关联数据”，全零nonce [0] 96和256位密钥K∈Sym.K..结果 是明文字节序列，或⊥指示解密失败。

**Note:** The “IETF" definition of AEAD\_CHACHA20\_POLY1305 from [[RFC-7539]](#_bookmark188) is used; this has a 32-bit block count and a 96-bit nonce, rather than a 64-bit block count and 64-bit nonce as in the original definition of ChaCha20.

#### Key Agreement

The *key agreement scheme* specified in [§4.1.4](#_bookmark27) *‘Key Agreement’* on p. 13 is instantiated using Curve25519 [[Bern2006]](#_bookmark144) as follows.

Let KA*.*Public and KA*.*SharedSecret be the type of Curve25519 public keys (i.e. a sequence of 32 bytes), and let

KA*.*Private be the type of Curve25519 secret keys.

让KA.Public和KA.SharedSecret成为Curve25519公钥的类型（即32字节的序列），并让KA.Private成为Curve25519密钥的类型。

Let Curve25519(*n, q*) be the result of point multiplication of the Curve25519 public key represented by the byte sequence *q* by the Curve25519 secret key represented by the byte sequence *n*, as defined in [[Bern2006,](#_bookmark144) section 2].

假设Curve25519（n，q）是由字节序列q表示的Curve25519公开密钥乘以字节序列n表示的Curve25519秘密密钥的点乘结果，如[Bern2006，第2节]

Curve25519（n，q）= Curve25519\_PubKey(用字节序列q表示) 点乘 Curve25519\_SecretKey(用字节序列n表示)

Let 9 be the public byte sequence representing the Curve25519 base point.

设9是表示Curve25519基点的公共字节序列。

Let clampCurve25519 (*x*) take a 32-byte sequence *x* as input and return a byte sequence representing a Curve25519 private key, with bits “clamped” as described in [[Bern2006,](#_bookmark144) section 3]: “clear bits 0*,* 1*,* 2 of the first byte, clear bit 7 of the last byte, and set bit 6 of the last byte.” Here the bits of a byte are numbered such that bit *b* has numeric weight 2b.

让clampCurve25519（x）将一个32字节的序列x作为输入，并返回一个表示Curve25519私钥的字节序列，并按照[Bern2006，section 3]中所述的“钳位”位进行清除：“清除0,1,2位 第一个字节，清除最后一个字节的第7位，并设置最后一个字节的第6位。“这里，一个字节的位编号使得位b具有数字权重2^b。

Define KA*.*FormatPrivate(*x*) := clampCurve25519 (*x*). Define KA*.*Agree(*n, q*) := Curve25519(*n, q*).

#### Key Derivation

The *Key Derivation Function* specified in [§ 4.1.5](#_bookmark28) *‘Key Derivation’* on p. 13 is instantiated using BLAKE2b-256 as follows:

KDF(*i,* hSig*,* sharedSecreti*,* epk*,* pknew ) := BLAKE2b-256(kdftag*,* kdfinput)

enc,i

where:

kdftag :=

|  |  |  |
| --- | --- | --- |
| 64-bit **“ZcashKDF"** | 8-bit *i−*1 | [0]56 |

kdfinput := .

|  |  |  |  |
| --- | --- | --- | --- |
| 256-bit hSig | 256-bit sharedSecreti | 256-bit epk | 256-bit pknew  enc,i |

BLAKE2b-256(*p, x*) refers to unkeyed BLAKE2b-256 [[ANWW2013]](#_bookmark135) in sequential mode, with an output digest length of 32 bytes, 16-byte personalization string *p*, and input *x*. This is not the same as BLAKE2b-512 truncated to 256 bits, because the digest length is encoded in the parameter block.

#### Signature

JoinSplitSig is specified in [§4.1.6](#_bookmark30) *‘Signature’* on p. 14.

It is instantiated as Ed25519 [[BDL+2012],](#_bookmark142) with the additional requirement that *S* (the integer represented by *S*) must be less than the prime = 2252 + 27742317777372353535851937790883648493, otherwise the signature is considered invalid. Ed25519 is defined as using SHA-512 internally.

The encoding of a signature is:

256-bit *R*

256-bit *S*

where *R* and *S* are as defined in [[BDL+2012].](#_bookmark142)

The encoding of a public key is as defined in [[BDL+2012].](#_bookmark142)

#### Commitment

The commitment scheme COMM specified in [§4.1.7](#_bookmark32) *‘Commitment’* on p. 15 is instantiated using SHA-256 as follows:

COMMr (apk*,* v*,* ρ) := SHA256 （ ＼.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 256-bit apk | 64-bit v | 256-bit ρ | 256-bit r |

**Note:** The leading byte of the SHA256 input is **0xB0**.

#### Security requirements:

* + - * The *SHA-256 compression* function must be collision-resistant.
      * The *SHA-256 compression* function must be a PRF when keyed by the bits corresponding to the position of r in the second block of SHA-256 input, with input to the PRF in the remaining bits of the block and the chaining variable.

#### Represented Groups and Pairings

**5.4.8.1 BN-254**

The *represented pairing* BN-254 is defined in this section.

Let *q*G = 21888242871839275222246405745257275088696311157297823662689037894645226208583. Let *r*G = 21888242871839275222246405745257275088548364400416034343698204186575808495617.

Let *b*G = 3.

(*q*G and *r*G are prime.)

Let G1 be the group of points on a Barreto–Naehrig curve *E*G1 over FqG with equation *y*2 = *x*3 + *b*G. This curve has embedding degree 12 with respect to *r*G.

Let G2 be the subgroup of order *r* in the sextic twist *E*G

of G1 over F 2 with equation *y*2 = *x*3 + bG , where *ξ* ◦ F 2 .

2 qG ξ qG

◦

We represent elements of F 2 as polynomials *a*1 *· t* + *a*0 ◦ FqG [*t*], modulo the irreducible polynomial *t*2 + 1; in this

G

q ◦

representation, *ξ* is given by *t* + 9.

Let GT be the subgroup of *r* th roots of unity in F*∗* 12 .

G qG

Let *e*ˆG be the optimized ate pairing of type G1 *×* G2 *→* GT .

For *i* ◦ *{*1 *..* 2*}*, let *O*G be the point at infinity (which is the additive identity) in Gi, and let Gi*∗* = Gi *\ {O*G *}*.

◦

*i*

*i*

Let *P*G1 ◦ G*∗*1 = (1*,* 2).

◦

Let *P*G2 ◦ G*∗*2 = (11559732032986387107991004021392285783925812861821192530917403151452391805634*· t* +

◦

10857046999023057135944570762232829481370756359578518086990519993285655852781*,*

4082367875863433681332203403145435568316851327593401208105741076214120093531*· t* +

8495653923123431417604973247489272438418190587263600148770280649306958101930)*.*

*P*G1 and *P*G2 are generators of G1 and G2 respectively.

Define I2OSP ◦ (*k* ◦ N) *× {*0 *..* 256k *−*1*} → {*0 *..* 255*}*[k] such that I2OSP亿(*n*) is the sequence of bytes representing *n*

◦

◦

in big-endian order.

For a point *P* ◦◦ G*∗*1 = (*x*P *, y*P ):

* + - * The field elements *x*P and *y*P ◦ Fq are represented as integers *x* and *y* ◦ *{*0 *.. q −*1*}*.

◦ ◦

* + - * Let *y*˜ = *y* mod 2.
      * *P* is encoded as .

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1-bit *y*˜ | 256-bit I2OSP32 (*x*) |

For a point *P* ◦◦ G*∗*2 = (*x*P *, y*P ):

* + - * Define FE2IP ◦ FqG [*t*]*/*(*t*2 + 1) *→ {*0 *.. q* 2 *−*1*}* such that FE2IP(*a*w,1 *· t* + *a*w,0 ) = *a*w,1 *· q* + *a*w,0.

◦

G

* + - * Let *x* = FE2IP(*x*P ), *y* = FE2IP(*y*P ), and *yt* = FE2IP(*−y*P ).
* Let *y* = （

˜ 1*,* if *y > yt*

0*,* otherwise*.*

* + - * *P* is encoded as .

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1-bit *y*˜ | 512-bit I2OSP64 (*x*) |

#### Non-normative notes:

* + - * The use of big-endian byte order is different from the encoding of most other integers in this protocol. The encodings for G*∗*1,2 are consistent with the definition of EC2OSP for compressed curve points in [[IEEE2004,](#_bookmark179) section 5.5.6.2]. The LSB compressed form (i.e. EC2OSP-XL) is used for points in G*∗*1, and the SORT com- pressed form (i.e. EC2OSP-XS) for points in G*∗*2.
      * The points at infinity *O*G1*,*2 never occur in proofs and have no defined encodings in this protocol.
      * Testing *y > yt* for the compression of G*∗*2 points is equivalent to testing whether (*a*y,1*, a*y,0 ) *>* (*a−*y,1*, a−*y,0 )

in lexicographic order.

* + - * Algorithms for decompressing points from the above encodings are given in [[IEEE2000,](#_bookmark178) Appendix A.12.8] for G*∗*1, and [[IEEE2004,](#_bookmark179) Appendix A.12.11] for G*∗*2.
      * A rational point *P* \* *O*G2 on the curve *E*G2 can be verified to be of order *r*G, and therefore in G*∗*2, by checking that *r*G *· P* = *O*G2 .

When computing square roots in FqG or Fq 2 in order to decompress a point encoding, the implementation **MUST NOT** assume that the square root exists, or that the encoding represents a point on the curve.

G

#### Zero-Knowledge Proving Systems

**5.4.9.1 PHGR13**

**Zcash** uses *zk-SNARKs* generated by its fork of *libsnark* [[libsnark-fork]](#_bookmark181) with the *proving system* described in [[BCTV2015],](#_bookmark140) which is a refinement of the systems in [[PGHR2013]](#_bookmark186) and [[BCGTV2013].](#_bookmark138)

* *∗*1 K
* *∗*1 H
* *∗*1

Zcash使用由libsnark [libsnark-fork]分支生成的zk-SNARK与[BCTV2015]中描述的验证系统，这是[PGHR2013]和[BCGTV2013]中系统的改进。

A proof consists of a tuple (*π*A ◦◦ G1*∗, π*A*t*

* G *, π*
* G *, πt*
* G1*, π*C
* G1*, π*C
* G *, π*
* G *, π*
* G ). It is

computed using the parameters above as described in [[BCTV2015,](#_bookmark140) Appendix B].

* *∗*1 B
* *∗*2 B
* *∗*
* *∗ t*

**Note:** Many details of the *proving system* are beyond the scope of this protocol document. For example, the *arithmetic circuit* verifying the *JoinSplit statement* , or its expression as a *Rank 1 Constraint System*, are not speci- fied here. In practice it will be necessary to use the specific proving and verification keys generated for the **Zcash** production *block chain* (see [§5.7](#_bookmark92) *‘zk-SNARK Parameters’* on p. 33), and a *proving system* implementation that is interoperable with the **Zcash** fork of *libsnark* , to ensure compatibility.

证明系统的许多细节超出了本协议文件的范围。 例如，验证JoinSplit语句的算术电路，或者它作为秩1约束系统的表达式，在这里没有指定。 在实践中，有必要使用针对Zcash生产模块链生成的具体证明和验证密钥（参见第33页第5.7节“zk-SNARK参数”），以及可与Zcash分支交互使用的证明系统实现 libsnark，以确保兼容性

**Encoding of PH****GR13 Proofs** A PHGR13 proof is encoded by concatenating the encodings of its elements:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 264-bit *π*A | 264-bit *π*A*t* | 520-bit *π*B | 264-bit *π*B*t* | 264-bit *π*C | 264-bit *π*C*t* | 264-bit *π*K | 264-bit *π*H |

The resulting proof size is 296 bytes.

In addition to the steps to verify a proof given in [[BCTV2015,](#_bookmark140) Appendix B], the verifier **MUST** check, for the encoding of each element, that:

* + the lead byte is of the required form;
  + the remaining bytes encode a big-endian representation of an integer in *{*0 *.. q*S *−*1*}* or (in the case of *π*B )

2

*{*0 *.. q*S *−*1*}*;

* + the encoding represents a point in G*∗*1 or (in the case of *π*B ) G*∗*2, including checking that it is of order *r*G in the latter case.

除了验证[BCTV2015，附录B]中给出的证明的步骤之外，验证者必须检查每个元素的编码：

•前导字节是必需的形式;

•其余字节编码{0..qS -1}或（在πB的情况下）{0 ... qS -1}的整数的大端表示;

•编码表示G \* 1中的一个点或（在πB的情况下）G \* 2，包括在后一种情况下检查它的阶数为rG。

## Note Plaintexts and Memo Fields

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

The *note plaintexts* associated with a *JoinSplit description* are encrypted to the respective *transmission keys*

pk

new enc,1..N

new , and the result forms part of a *transmitted notes ciphertext* (see [§ 4.10](#_bookmark54) *‘In-band secret distribution’*

on p. 22 for further details).

传送的票据以加密的形式存储在区块链中，并附有票据承诺cm。

与JoinSplit描述相关联的票据明文用对应的传输密钥pk加密，并且结果组成发送的票据密文的一部分（更多细节参见第22页第4.10节“带内秘密分发”）。

Each *note plaintext* (denoted **np**) consists of (v*,* ρ*,* r*,* memo).

The first three of these fields are as defined earlier. memo is a 512-byte *memo field* associated with this *note*.

The usage of the *memo field* is by agreement between the sender and recipient of the *note*. The *memo field*

**SHOULD** be encoded either as:

* + - a UTF-8 human-readable string [[Unicode],](#_bookmark190) padded by appending zero bytes; or

通过附加零字节填充的UTF-8人可读字符串[Unicode];

* + - an arbitrary sequence of 512 bytes starting with a byte value of **0xF5** or greater, which is therefore not a valid UTF-8 string.

512字节的任意序列，以字节值0xF5或更大开始，因此不是有效的UTF-8字符串。

In the former case, 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).

在前一种情况下，钱包软件需要去除任何尾随的零字节，然后在适用的情况下将结果UTF-8字符串显示给收件人用户。 不正确的UTF-8编码字节序列应显示为替换字符（U + FFFD）。

In the latter case, the contents of the *memo field* **SHOULD NOT** be displayed. A start byte of **0xF5** is reserved for use by automated software by private agreement. A start byte of **0xF6** or greater is reserved for use in future **Zcash** protocol extensions.

在后一种情况下，备忘录字段的内容不应显示。 0xF5的起始字节被专用协议保留供自动化软件使用。 0xF6或更大的起始字节被保留用于将来的Zcash协议扩展。

The encoding of a *note plaintext* consists of:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8-bit **0x00** | 64-bit v | 256-bit ρ | 256-bit r | memo (512 bytes) |

* + - A byte, **0x00**, indicating this version of the encoding of a *note plaintext* .
    - 8 bytes specifying v.
    - 32 bytes specifying ρ.
    - 32 bytes specifying r.
    - 512 bytes specifying memo.

## Encodings of Addresses and Keys

This section describes how **Zcash** encodes *payment addresses*, *incoming viewing keys*, and *spending keys*.

Addresses and keys can be encoded as a byte sequence; this is called the *raw encoding* . This byte sequence can then be further encoded using Base58Check. The Base58Check layer is the same as for upstream **Bitcoin** addresses [[Bitc-Base58].](#_bookmark161)

地址和密钥可以编码为一个字节序列; 这被称为原始编码。 然后可以使用Base58Check对该字节序列进行进一步编码。 Base58Check层与上游比特币地址[Bitc-Base58]相同。

*SHA-256 compression* outputs are always represented as sequences of 32 bytes. The language consisting of the following encoding possibilities is prefix-free.

#### Transparent Payment Addresses

*Transparent* payment addresses are either P2SH (Pay to Script Hash) [[BIP-13]](#_bookmark147) or P2PKH (Pay to Public Key Hash) [[Bitc-P2PKH]](#_bookmark167) addresses.

The raw encoding of a P2SH address consists of:

|  |  |  |
| --- | --- | --- |
| 8-bit **0x1C** | 8-bit **0xBD** | 160-bit script hash |

* + - * Two bytes [**0x1C***,* **0xBD**], indicating this version of the raw encoding of a P2SH address on the production network. (Addresses on the test network use [**0x1C***,* **0xBA**] instead.)
      * •两个字节[0x1C，0xBD]，表示生产网络中P2SH地址的原始编码版本。 （测试网络上的地址改为使用[0x1C，0xBA]。）
      * 160 bits specifying a script hash [[Bitc-P2SH].](#_bookmark168)

The raw encoding of a P2PKH address consists of:

|  |  |  |
| --- | --- | --- |
| 8-bit **0x1C** | 8-bit **0xB8** | 160-bit public key hash |

* + - * Two bytes [**0x1C***,* **0xB8**], indicating this version of the raw encoding of a P2PKH address on the production network. (Addresses on the test network use [**0x1D***,* **0x25**] instead.)
      * 160 bits specifying a public key hash, which is a RIPEMD-160 hash [[RIPEMD160]](#_bookmark189) of a SHA-256 hash [[NIST2015]](#_bookmark185) of an uncompressed ECDSA key encoding.

#### Notes:

* + - * In **Bitcoin** a single byte is used for the version field identifying the address type. In **Zcash** two bytes are used. For addresses on the production network, this and the encoded length cause the first two characters of the Base58Check encoding to be fixed as **“t3"** for P2SH addresses, and as **“t1"** for P2PKH addresses. (This does *not* imply that a *transparent* **Zcash** address can be parsed identically to a **Bitcoin** address just by removing the **“t"**.)
      * 在比特币中，一个字节用于标识地址类型的版本字段。 在Zcash中使用了两个字节。 对于生产网络中的地址，此编码长度导致Base58Check编码的前两个字符作为P2SH地址的“t3”固定，并且作为P2PKH地址的“t1”固定。 （这并不意味着透明的Zcash地址可以通过删除“t”来像解析比特币地址一样）。
      * **Zcash** does not yet support Hierarchical Deterministic Wallet addresses [[BIP-32].](#_bookmark152)

#### Transparent Private Keys

These are encoded in the same way as in **Bitcoin** [[Bitc-Base58],](#_bookmark161) for both the production and test networks.

#### Shielded Payment Addresses

A *payment address* consists of apk and pkenc.

apk is a *SHA-256 compression* output. pkenc is a KA*.*Public key (see [§5.4.4](#_bookmark72) *‘Key Agreement’* on p. 27), for use with the encryption scheme defined in [§ 4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22. These components are derived from a *spending key* as described in [§4.2](#_bookmark37) *‘Key Components’* on p. 17.

The raw encoding of a *payment address* consists of:

|  |  |  |  |
| --- | --- | --- | --- |
| 8-bit **0x16** | 8-bit **0x9A** | 256-bit apk | 256-bit pkenc |

* + - * Two bytes [**0x16***,* **0x9A**], indicating this version of the raw encoding of a **Zcash** *payment address* on the production network. (Addresses on the test network use [**0x16***,* **0xB6**] instead.)
      * 256 bits specifying apk.
      * 256 bits specifying pkenc, using the normal encoding of a Curve25519 public key [[Bern2006]](#_bookmark144).

**Note:** For addresses on the production network, the lead bytes and encoded length cause the first two characters of the Base58Check encoding to be fixed as **“zc"**. For the test network, the first two characters are fixed as **“zt"**.

#### Incoming Viewing Keys

An *incoming viewing key* consists of apk and skenc.

apk is a *SHA-256 compression* output. skenc is a KA*.*Private key (see [§ 5.4.4](#_bookmark72) *‘Key Agreement’* on p. 27), for use with the encryption scheme defined in [§ 4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22. These components are derived from a *spending key* as described in [§4.2](#_bookmark37) *‘Key Components’* on p. 17.

The raw encoding of an *incoming viewing key* consists of, in order:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8-bit **0xA8** | 8-bit **0xAB** | 8-bit **0xD3** | 256-bit apk | 256-bit skenc |

* + - * Three bytes [**0xA8***,* **0xAB***,* **0xD3**], indicating this version of the raw encoding of a **Zcash** *incoming viewing key* on the production network. (Addresses on the test network use [**0xA8***,* **0xAC***,* **0x0C**] instead.)
      * 256 bits specifying apk.
      * 256 bits specifying skenc, using the normal encoding of a Curve25519 private key [[Bern2006].](#_bookmark144)

skenc **MUST** be “clamped” using KA*.*FormatPrivate as specified in [§ 4.2](#_bookmark37) *‘Key Components’* on p. 17. That is, a de- coded *incoming viewing key* **MUST** be considered invalid if skenc \* KA*.*FormatPrivate(skenc ). (KA*.*FormatPrivate is defined in [§5.4.4](#_bookmark72) *‘Key Agreement’* on p. 27.)

**Note:** For addresses on the production network, the lead bytes and encoded length cause the first four characters of the Base58Check encoding to be fixed as **“ZiVK"**. For the test network, the first four characters are fixed as **“ZiVt"**.

#### Spending Keys

A *spending key* consists of ask, which is a sequence of 252 bits (see [§4.2](#_bookmark37) *‘Key Components’* on p. 17). The raw encoding of a *spending key* consists of:

|  |  |  |  |
| --- | --- | --- | --- |
| 8-bit **0xAB** | 8-bit **0x36** | [0]4 | 252-bit ask |

* + - * Two bytes [**0xAB***,* **0x36**], indicating this version of the raw encoding of a **Zcash** *spending key* on the pro- duction network. (Addresses on the test network use [**0xAC***,* **0x08**] instead.)
      * 4 zero padding bits.
      * 252 bits specifying ask.

The zero padding occupies the most significant 4 bits of the third byte.

#### Notes:

* + - * If an implementation represents ask internally as a sequence of 32 bytes with the 4 bits of zero padding intact, it will be in the correct form for use as an input to PRFaddr, PRFnf , and PRFpk without need for bit-shifting. Future key representations may make use of these padding bits.
      * •如果一个实现代表内部32字节的序列，并且4位零填充保持不变，则它将以正确的形式用作PRFaddr，PRFnf和PRFpk的输入，而无需位移。 未来的关键表示可能会使用这些填充位。
      * For addresses on the production network, the lead bytes and encoded length cause the first two characters of the Base58Check encoding to be fixed as **“SK"**. For the test network, the first two characters are fixed as **“ST"**.

## zk-SNARK Parameters

For the **Zcash** production *block chain* and testnet, the SHA-256 hashes of the *proving key* and *verifying key* for the

*JoinSplit statement* , encoded in *libsnark* format, are:

8bc20a7f013b2b58970cddd2e7ea028975c88ae7ceb9259a5344a16bc2c0eef7 sprout-proving.key 4bd498dae0aacfd8e98dc306338d017d9c08dd0918ead18172bd0aec2fc5df82 sprout-verifying.key

These parameters were obtained by a multi-party computation described in [[GitHub-mpc]](#_bookmark176) and [[BGG2016].](#_bookmark145)

# Consensus Changes from Bitcoin

## Encoding of Transactions

The **Zcash** *transaction* format is as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Bytes | Name | Data Type | Description |
| 4 | version | int32\_t | Transaction version number; either 1 or 2. |
| *Varies* | tx\_in\_count | compactSize uint | Number of *transparent* inputs in this transaction. |
| *Varies* | tx\_in | tx\_in | *Transparent* inputs, encoded as in  **Bitcoin**. |
| *Varies* | tx\_out\_count | compactSize uint | Number of *transparent* outputs in this transaction. |
| *Varies* | tx\_out | tx\_out | *Transparent* outputs, encoded as in  **Bitcoin**. |
| 4 | lock\_time | uint32\_t | A Unix epoch time (UTC) or block number, encoded as in **Bitcoin**. |
| *Varies †* | nJoinSplit | compactSize uint | The number of *JoinSplit descriptions*  in vJoinSplit. |
| 1802 *·*  nJoinSplit *†* | vJoinSplit | JoinSplitDescription [nJoinSplit] | A sequence of *JoinSplit descriptions*, each encoded as described in [§ 6.2](#_bookmark96) *‘Encoding of JoinSplit Descriptions’* on p. 36. |
| 32 *‡* | joinSplitPubKey | char[32] | An encoding of a JoinSplitSig public verification key. |
| 64 *‡* | joinSplitSig | char[64] | A signature on a prefix of the *trans- action* encoding, to be verified using joinSplitPubKey. |

*†* The nJoinSplit and vJoinSplit fields are present if and only if version *>* 1.

*‡* The joinSplitPubKey and joinSplitSig fields are present if and only if version *>* 1 and nJoinSplit *>* 0.

The encoding of joinSplitPubKey and the data to be signed are specified in [§4.6](#_bookmark43) *‘Non-malleability’* on p. 20.

#### Consensus rules:

* + - The *transaction version number* **MUST** be greater than or equal to 1.
    - If version = 1 or nJoinSplit = 0, then tx\_in\_count **MUST NOT** be 0.
    - A *transaction* with one or more coinbase inputs **MUST** have no *transparent* outputs (i.e. tx\_out\_count **MUST**

be 0).

•有一个或多个coinbase输入的交易必须没有透明输出（即tx\_out\_count必须为0）。

* + - If nJoinSplit *>* 0, then joinSplitSig **MUST** represent a valid signature over dataToBeSigned as defined in

[§4.6](#_bookmark43) *‘Non-malleability’* on p. 20.

* + - TODO: Coinbase maturity rule.
    - TODO: Other rules inherited from **Bitcoin**.

#### Notes:

* + - The semantics of *transactions* with *transaction version number* not equal to either 1 or 2 is not currently defined. Miners **MUST NOT** create *blocks* containing such *transactions*.
    - The exclusion of *transactions* with *transaction version number greater than* 2 is not a consensus rule. Such

*transactions* may exist in the *block chain* and **MUST** be treated identically to version 2 *transactions*.

•排除事务版本号大于2的事务不是一个共识规则。 这种交易可能存在于区块链中，并且必须与第2版交易的处理方式相同。

* + - Note that a future hard fork might use *any transaction version number* . It is likely that a hard fork that changes the *transaction version number* will also change the *transaction* format, and software that parses *transactions* **SHOULD** take this into account.
    - The version field is a signed integer. (It was incorrectly specified as unsigned in a previous version of this specification.) A future hard fork might use negative values for this field, or otherwise change its interpreta- tion.
    - A *transaction version number* of 2 does not have the same meaning as in **Bitcoin**, where it is associated with support for OP\_CHECKSEQUENCEVERIFY as specified in [[BIP-68].](#_bookmark160) **Zcash** was forked from **Bitcoin** v0.11.2 and does not currently support BIP 68, or the related BIPs 9, 112 and 113.

The changes relative to **Bitcoin** version 1 transactions as described in [[Bitc-Format]](#_bookmark164) are:

* + - *Transaction version* 0 is not supported.
    - A version 1 *transaction* is equivalent to a version 2 *transaction* with nJoinSplit = 0.
    - The nJoinSplit, vJoinSplit, joinSplitPubKey, and joinSplitSig fields have been added.
    - In **Zcash** it is permitted for a *transaction* to have no *transparent* inputs provided that nJoinSplit *>* 0.

Software that creates *transactions* **SHOULD** use version 1 for *transactions* with no *JoinSplit descriptions*.

## Encoding of JoinSplit Descriptions

An abstract *JoinSplit description*, as described in [§3.5](#_bookmark16) *‘JoinSplit Transfers and Descriptions’* on p. 10, is encoded in a *transaction* as an instance of a JoinSplitDescription type as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Bytes | Name | Data Type | Description |
| 8 | vpub\_old | uint64\_t | A value vold that the *JoinSplit transfer* removes from  pub  the *transparent value pool* . |
| 8 | vpub\_new | uint64\_t | A value vnew that the *JoinSplit transfer* inserts into the  pub  *transparent value pool* . |
| 32 | anchor | char[32] | A merkle root rt of the *note commitment tree* at some block height in the past, or the merkle root produced by a previous *JoinSplit transfer* in this *transaction*. |
| 64 | nullifiers | char[32][Nold] | A sequence of *nullifiers* of the input *notes* nfold old .  1..N |
| 64 | commitments | char[32][Nnew] | A sequence of *note commitments* for the output  *notes* cmnew new .  1..N |
| 32 | ephemeralKey | char[32] | A Curve25519 public key epk. |
| 32 | randomSeed | char[32] | A 256-bit seed that must be chosen independently at random for each *JoinSplit description*. |
| 64 | vmacs | char[32][Nold] | A sequence of message authentication tags h1..Nold  that bind hSig to each ask of the *JoinSplit description*. |
| 296 | zkproof | char[296] | An encoding of the *zero-knowledge proof π*JoinSplit  (see [§5.4.9.1](#_bookmark80) *‘PHGR13’* on p. 29). |
| 1202 | encCiphertexts | char[601][Nnew] | A sequence of ciphertext components for the en- crypted output *notes*, Cenc new .  1..N |

The vmacs field encodes h1..Nold which are computed as described in [§4.6](#_bookmark43) *‘Non-malleability’* on p. 20.

The ephemeralKey and encCiphertexts fields together form the *transmitted notes ciphertext* , which is computed as described in [§4.10](#_bookmark54) *‘In-band secret distribution’* on p. 22.

Consensus rules applying to a *JoinSplit description* are given in [§4.3](#_bookmark38) *‘JoinSplit Descriptions’* on p. 17.

## Block Header

The **Zcash** *block header* format is as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Bytes | Name | Data Type | Description |
| 4 | nVersion | int32\_t | The *block version number* indicates which set of *block* validation rules to follow. The cur- rent and only defined *block version number* for **Zcash** is 4. |
| 32 | hashPrevBlock | char[32] | A *SHA-256d* hash in internal byte order of the previous *block* ’s *header* . This ensures no previous *block* can be changed without also changing this *block* ’s *header* . |
| 32 | hashMerkleRoot | char[32] | A *SHA-256d* hash in internal byte order. The merkle root is derived from the hashes of all *transactions* included in this *block* , ensuring that none of those *transactions* can be modi- fied without modifying the *header* . |
| 32 | hashReserved | char[32] | A reserved field which should be ignored. |
| 4 | nTime | uint32\_t | The *block time* is a Unix epoch time (UTC) when the miner started hashing the *header* (ac- cording to the miner). |
| 4 | nBits | uint32\_t | An encoded version of the *target threshold* this *block* ’s *header* hash must be less than or equal to, in the same nBits format used by **Bitcoin**. [[Bitc-nBits]](#_bookmark166) |
| 32 | nNonce | char[32] | An arbitrary field miners change to modify the *header* hash in order to produce a hash less than or equal to the *target threshold* . |
| 3 | solutionSize | compactSize uint | The size of an Equihash solution in bytes (al- ways 1344). |
| 1344 | solution | char[1344] | The Equihash solution. |

A *block* consists of a *block header* and a sequence of *transactions*. How transactions are encoded in a *block* is part of the Zcash peer-to-peer protocol but not part of the consensus protocol.

Let ThresholdBits be as defined in [§6.4.3](#_bookmark104) *‘Difficulty adjustment’* on p. 40, and let PoWMedianBlockSpan be the con- stant defined in [§5.3](#_bookmark61) *‘Constants’* on p. 24.

#### Consensus rules:

* The *block version number* **MUST** be greater than or equal to 4.
* For a *block* at *block height* height, nBits **MUST** be equal to ThresholdBits(height).
* The *block* **MUST** pass the difficulty filter defined in [§6.4.2](#_bookmark103) *‘Difficulty filter’* on p. 40.
* solution **MUST** represent a valid Equihash solution as defined in [§6.4.1](#_bookmark101) *‘Equihash’* on p. 39.
* nTime **MUST** be strictly greater than the median time of the previous PoWMedianBlockSpan *blocks*.
* •nTime必须严格大于先前PoWMedianBlockSpan块的中位时间。
* The size of a *block* **MUST** be less than or equal to 2000000 bytes.
* TODO: Other rules inherited from **Bitcoin**.

In addition, a *full node* **MUST NOT** accept *blocks* with nTime more than two hours in the future according to its clock. This is not strictly a consensus rule because it is nondeterministic, and clock time varies between nodes. Also note that a *block* that is rejected by this rule at a given point in time may later be accepted.

#### Notes:

* The semantics of blocks with *block version number* not equal to 4 is not currently defined. Miners **MUST NOT** create such *blocks*, and **SHOULD NOT** mine other blocks on top of them.
* The exclusion of *blocks* with *block version number greater than* 4 is not a consensus rule; such *blocks* may exist in the *block chain* and **MUST** be treated identically to version 4 *blocks* by *full nodes*. Note that a future hard fork might use *block version number* either greater than or less than 4. It is likely that such a hard fork will change the *block* header and/or *transaction* format, and software that parses *blocks* **SHOULD** take this into account.
* The nVersion field is a signed integer. (It was incorrectly specified as unsigned in a previous version of this specification.) A future hard fork might use negative values for this field, or otherwise change its interpreta- tion.
* There is no relation between the values of the version field of a *transaction*, and the nVersion field of a

*block header* .

* Like other serialized fields of type compactSize uint, the solutionSize field **MUST** be encoded with the minimum number of bytes (3 in this case), and other encodings **MUST** be rejected. This is necessary to avoid a potential attack in which a miner could test several distinct encodings of each Equihash solution against the difficulty filter, rather than only the single intended encoding.
* As in **Bitcoin**, the nTime field **MUST** represent a time *strictly greater than* the median of the timestamps of the past PoWMedianBlockSpan *blocks*. The Bitcoin Developer Reference [[Bitc-Block]](#_bookmark162) was previously in error on this point, but has now been corrected.

The changes relative to **Bitcoin** version 4 blocks as described in [[Bitc-Block]](#_bookmark162) are:

* *Block versions* less than 4 are not supported.
* The hashReserved, solutionSize, and solution fields have been added.
* The type of the nNonce field has changed from uint32\_t to char[32].
* The maximum *block* size has been doubled to 2000000 bytes.

## Proof of Work

**Zcash** uses Equihash [[BK2016]](#_bookmark170) as its Proof of Work. Motivations for changing the Proof of Work from *SHA-256d*

used by **Bitcoin** are described in [[WG2016].](#_bookmark192)

A *block* satisfies the Proof of Work if and only if:

* The solution field encodes a *valid Equihash solution* according to [§6.4.1](#_bookmark101) *‘Equihash’* on p. 39.
* The *block header* satisfies the difficulty check according to [§6.4.2](#_bookmark103) *‘Difficulty filter’* on p. 40.

#### Equihash

An instance of the Equihash algorithm is parameterized by positive integers *n* and *k*, such that *n* is a multiple of

*k* + 1. We assume *k ≥* 3.

The Equihash parameters for the production and test networks are *n* = 200*, k* = 9.

The Generalized Birthday Problem is defined as follows: given a sequence *X*1..N of *n*-bit strings, find 2k distinct

2*k*

尘

*X*i*j* such that *X*i*j* = 0.

j=1

In Equihash, N = 2 *n* +1, and the sequence *X*1 N is derived from the *block header* and a nonce:

*k*+1

..

Let powheader :=

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 32-bit nVersion | 256-bit hashPrevBlock | | 256-bit hashMerkleRoot | |
| 256-bit hashReserved | | 32-bit nTime | 32-bit nBits |  |
| 256-bit nNonce | |  | | |

For *i ∈ {*1 *.. N }*, let *X*i = EquihashGenn,k (powheader*, i*).

EquihashGen is instantiated in [§5.4.1.3](#_bookmark67) *‘Equihash Generator’* on p. 25.

Define I2BSP ◦ (*u* ◦ N) *× {*0 *..* 2u *−*1*} →* B[u] such that I2BSPu (*x*) is the sequence of *u* bits representing *x* in big-

◦ ◦

endian order.

A *valid Equihash solution* is then a sequence *i* ◦ *{*1 *.. N }*2*k* that satisfies the following conditions:

◦

#### Generalized Birthday condition

2*k*

*X*i*j* = 0.

尘

j=1

#### Algorithm Binding conditions

2*r*

* + - * For all *r ∈ {*1 *.. k −*1*}*, for all *w ∈ {*0 *..* 2k*−*r *−*1*}* : 尘*X*

k+1

j=1

i*w·*2*r* +*j*

has n*·*r leading zeroes; and

* + - * For all *r ∈ {*1 *.. k}*, for all *w ∈ {*0 *..* 2k*−*r *−*1*}* : *i r r r−*1 *< i r r−*1 *r r* lexicographically.

w*·*2 +1..w*·*2 +2 w*·*2 +2 +1..w*·*2 +2

#### Notes:

* + - * This does not include a difficulty condition, because here we are defining validity of an Equihash solution independent of difficulty.
      * Previous versions of this specification incorrectly specified the range of *r* to be 1 *.. k* 1 for both parts of the algorithm binding condition. The implementation in zcashd was as intended.

*{ − }*

An Equihash solution with *n* = 200 and *k* = 9 is encoded in the solution field of a *block header* as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| I2BSP21 (*i*1 *−* 1) | I2BSP21 (*i*2 *−* 1) | *· · ·* | I2BSP21 (*i*512 *−* 1) |

Recall from [§ 5.2](#_bookmark60) *‘Integers, Bit Sequences, and Endianness’* on p. 24 that bits in the above diagram are ordered from most to least significant in each byte. For example, if the first 3 elements of *i* are [69*,* 42*,* 221], then the corre- sponding bit array is:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I2BSP21 (68) | | | | | | | | | | | | | | | | | | | | | I2BSP21 (41) | | | | | | | | | | | | | | | | | | | | | I2BSP21 (221 *−* 1) | | | | | | | | | | | | | | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 8-bit 0 | | | | | | | | 8-bit 2 | | | | | | | | 8-bit 32 | | | | | | | | 8-bit 0 | | | | | | | | 8-bit 10 | | | | | | | | 8-bit 127 | | | | | | | | 8-bit 255 | | | | | | | | *· · ·* | | | | | | |

and so the first 7 bytes of solution would be [0*,* 2*,* 32*,* 0*,* 10*,* 127*,* 255].

**Note:** I2BSP is big-endian, while integer field encodings in powheader and in the instantiation of EquihashGen are little-endian. The rationale for this is that little-endian serialization of *block headers* is consistent with **Bitcoin**, but using little-endian ordering of bits in the solution encoding would require bit-reversal (as opposed to only shifting).

I2BSP是大端编码，而powheader和EquihashGen的实例化中的整数字段编码是小端的。 其基本原理是块头的小端序列化与比特币一致，但在解码编码中使用小端位排序需要位反转（而不仅仅是移位）。

#### Difficulty filter

Let ToTarget be as defined in [§6.4.4](#_bookmark106) *‘nBits conversion’* on p. 41.

Difficulty is defined in terms of a *target threshold* , which is adjusted for each *block* according to the algorithm defined in [§6.4.3](#_bookmark104) *‘Difficulty adjustment’* on p. 40.

The difficulty filter is unchanged from **Bitcoin**, and is calculated using *SHA-256d* on the whole *block header* (in- cluding solutionSize and solution). The result is interpreted as a 256-bit integer represented in little-endian byte order, which **MUST** be less than or equal to the *target threshold* given by ToTarget(nBits).

#### Difficulty adjustment

**Zcash** uses a difficulty adjustment algorithm based on DigiShield v3/v4 [[DigiByte-PoW],](#_bookmark173) with simplifications and altered parameters, to adjust difficulty to target the desired 2.5-minute block time. Unlike **Bitcoin**, the difficulty adjustment occurs after every block.

Zcash使用基于DigiShield v3 / v4 [DigiByte-PoW]的难度调整算法，通过简化和改变参数来调整难度，以达到所需的2.5分钟块时间。 与比特币不同，难度调整发生在每个块之后。

The constants PoWLimit, PoWAveragingWindow, PoWMaxAdjustDown, PoWMaxAdjustUp, PoWDampingFactor, and

PoWTargetSpacing are instantiated in [§5.3](#_bookmark61) *‘Constants’* on p. 24.

Let ToCompact and ToTarget be as defined in [§6.4.4](#_bookmark106) *‘nBits conversion’* on p. 41.

Let nTime(height) be the value of the nTime field in the *header* of the *block* at *block height* height. Let nBits(height) be the value of the nBits field in the *header* of the *block* at *block height* height. *Block header* fields are specified in [§6.3](#_bookmark97) *‘Block Header’* on p. 37.

Define:

mean

(*S*)

length(S)

:= *S*i /

（  \

i=1

length

(*S*).

median(*S*) := sorted(*S*)ceiling(length(S)/2) clamp upper (*x*) := max(lower*,* min(upper*, x*)))

lower

(*x*) = （

trunc : floor(*x*) *,* if *x ≥* 0

*−*floor(*−x*) *,* otherwise

AveragingWindowTimespan := PoWAveragingWindow *·* PoWTargetSpacing

MinActualTimespan := floor(AveragingWindowTimespan *·* (1 *−* PoWMaxAdjustUp)) MaxActualTimespan := floor(AveragingWindowTimespan *·* (1 + PoWMaxAdjustDown))

MedianTime(height) := median([ nTime(*i*) for *i* from max(0*,* height *−* PoWMedianBlockSpan) up to height *−* 1 ]) ActualTimespan(height) := MedianTime(height) *−* MedianTime(height *−* PoWAveragingWindow) ActualTimespanDamped(height) := AveragingWindowTimespan + trunc ActualTimespan(height) *−* AveragingWindowTimespan

PoWDampingFactor

（ ＼

ActualTimespanClamped(height) := clamp MaxActualTimespan (ActualTimespanDamped(height))

MinActualTimespan



MeanTarget(height

) :=

PoWLimit*,* if height *≤* PoWAveragingWindow

mean([ ToTarget(nBits(*i*)) for *i* from height *−* PoWAveragingWindow up to height *−* 1 ])*,*



The *target threshold* for a given *block height* height is then calculated as:

otherwise

PoWLimit*,*

MeanTarget height

if height = 0

Threshold(height) :=

min(PoWLimit*,* floor（ A ( ) ＼ *·* ActualTimespanClamped(height))*,*

veragingWindowTimespan





ThresholdBits(height) := ToCompact(Threshold(height)).

otherwise

ThresholdBits(height) := ToCompact(Threshold(height)).

**Note:** The convention used for the height parameters to MedianTime, ActualTimespan, ActualTimespanDamped, ActualTimespanClamped, MeanTarget, Threshold, and ThresholdBits is that these functions use only information from *blocks preceding* the given *block height* .

用于高度参数MedianTime，ActualTimespan，ActualTimespanDamped，ActualTimespanClamped，MeanTarget，Threshold和ThresholdBits的公约是这些函数仅使用来自给定块高度之前的块的信息。

#### nBits conversion

Deterministic conversions between a *target threshold* and a “compact" nBits value are not fully defined in the Bitcoin documentation [[Bitc-nB](#_bookmark166)its], and so we define them here:

size(*x*) := ceiling （ bitlength(*x*) ＼

8

mantissa(*x*) := floor（*x ·* 2563*−*size(x) ）

（ *x* + *· x ,* if *x <*

ToCompact

(*x*)

mantissa( ) 224 size( ) mantissa( ) 223

:= floor（ mantissa(*x*) ＼ + 224 *·* (size(*x*) + 1)*,* otherwise

256

=

24

(*x* 笭 (223 *−* 1)) *·* 256floor x/2

ToTarget

(*x*)

: （0*,*

if *x* 笭 223 = 223

（ ）

*−*3*,* otherwise*.*

#### Definition of Work

As explained in [§ 3.3](#_bookmark14) *‘The Block Chain’* on p. 9, a node chooses the “best” *block chain* visible to it by finding the chain of valid *blocks* with the greatest total work.

Let ToTarget be as defined in [§6.4.4](#_bookmark106) *‘nBits conversion’* on p. 41.

The work of a *block* with value nBits for the nBits field in its *block header* is defined as floor（ 2256 ＼.

ToTarget(nBits) + 1

## Calculation of Block Subsidy and Founders’ Reward

[§ 3.8](#_bookmark19) *‘Block Subsidy and Founders’ Reward’* on p. 12 defines the *block subsidy* , *miner subsidy* , and *Founders’ Reward* . Their amounts in *zatoshi* are calculated from the *block height* using the formulae below. The constants SlowStartInterval, HalvingInterval, MaxBlockSubsidy, and FoundersFraction are instantiated in [§5.3](#_bookmark61) *‘Constants’* on p. 24.

SlowStartShift ◦ N := SlowStartInterval

* + - 2

SlowStartRate ◦ N := MaxBlockSubsidy

* + - SlowStartInterval

Halving(height) := floor（ *−* ＼

height SlowStartShift HalvingInterval

 *·*

SlowStartRate height*,* if height *<* SlowStartInterval

2



BlockSubsidy(height) := SlowStartRate *·* (height + 1)*,* if SlowStartInterval *≤* height *<* SlowStartInterval

2

floor（ ＼ *,* otherwise

MaxBlockSubsidy

2Halving(height)

( ) = （

FoundersReward height : BlockSubsidy(height) *·* FoundersFraction*,* if height *<* SlowStartShift + HalvingInterval

0*,* otherwise

MinerSubsidy(height) := BlockSubsidy(height) *−* FoundersReward(height).

## Payment of Founders’ Reward

The *Founders’ Reward* is paid by a *transparent* output in the *coinbase transaction*, to one of NumFounderAddresses

*transparent* addresses, depending on the *block height* .

创始人的奖励由coinbase交易中的透明输出支付给NumFounderAddresses透明地址之一，具体取决于块高度

For the production network, FounderAddressList1..NumFounderAddresses is:

### [ “t3Vz22vK5z2LcKEdg16Yv4FFneEL1zg9ojd", “t3cL9AucCajm3HXDhb5jBnJK2vapVoXsop3", “t3fqvkzrrNaMcamkQMwAyHRjfDdM2xQvDTR", “t3TgZ9ZT2CTSK44AnUPi6qeNaHa2eC7pUyF", “t3SpkcPQPfuRYHsP5vz3Pv86PgKo5m9KVmx", “t3Xt4oQMRPagwbpQqkgAViQgtST4VoSWR6S", “t3ayBkZ4w6kKXynwoHZFUSSgXRKtogTXNgb", “t3adJBQuaa21u7NxbR8YMzp3km3TbSZ4MGB", “t3K4aLYagSSBySdrfAGGeUd5H9z5Qvz88t2", “t3RYnsc5nhEvKiva3ZPhfRSk7eyh1CrA6Rk", “t3Ut4KUq2ZSMTPNE67pBU5LqYCi2q36KpXQ", “t3ZnCNAvgu6CSyHm1vWtrx3aiN98dSAGpnD", “t3fB9cB3eSYim64BS9xfwAHQUKLgQQroBDG", “t3cwZfKNNj2vXMAHBQeewm6pXhKFdhk18kD", “t3YcoujXfspWy7rbNUsGKxFEWZqNstGpeG4", “t3bLvCLigc6rbNrUTS5NwkgyVrZcZumTRa4", “t3VvHWa7r3oy67YtU4LZKGCWa2J6eGHvShi", “t3eF9X6X2dSo7MCvTjfZEzwWrVzquxRLNeY", “t3esCNwwmcyc8i9qQfyTbYhTqmYXZ9AwK3X", “t3M4jN7hYE2e27yLsuQPPjuVek81WV3VbBj", “t3gGWxdC67CYNoBbPjNvrrWLAWxPqZLxrVY", “t3LTWeoxeWPbmdkUD3NWBquk4WkazhFBmvU", “t3P5KKX97gXYFSaSjJPiruQEX84yF5z3Tjq", “t3f3T3nCWsEpzmD35VK62JgQfFig74dV8C9", “t3Rqonuzz7afkF7156ZA4vi4iimRSEn41hj", “t3fJZ5jYsyxDtvNrWBeoMbvJaQCj4JJgbgX", “t3Pnbg7XjP7FGPBUuz75H65aczphHgkpoJW", “t3WeKQDxCijL5X7rwFem1MTL9ZwVJkUFhpF", “t3Y9FNi26J7UtAUC4moaETLbMo8KS1Be6ME", “t3aNRLLsL2y8xcjPheZZwFy3Pcv7CsTwBec", “t3gQDEavk5VzAAHK8TrQu2BWDLxEiF1unBm", “t3Rbykhx1TUFrgXrmBYrAJe2STxRKFL7G9r", “t3aaW4aTdP7a8d1VTE1Bod2yhbeggHgMajR", “t3YEiAa6uEjXwFL2v5ztU1fn3yKgzMQqNyo", “t3g1yUUwt2PbmDvMDevTCPWUcbDatL2iQGP", “t3dPWnep6YqGPuY1CecgbeZrY9iUwH8Yd4z", “t3QRZXHDPh2hwU46iQs2776kRuuWfwFp4dV", “t3enhACRxi1ZD7e8ePomVGKn7wp7N9fFJ3r", “t3PkLgT71TnF112nSwBToXsD77yNbx2gJJY", “t3LQtHUDoe7ZhhvddRv4vnaoNAhCr2f4oFN", “t3fNcdBUbycvbCtsD2n9q3LuxG7jVPvFB8L", “t3dKojUU2EMjs28nHV84TvkVEUDu1M1FaEx", “t3aKH6NiWN1ofGd8c19rZiqgYpkJ3n679ME", “t3MEXDF9Wsi63KwpPuQdD6by32Mw2bNTbEa", “t3WDhPfik343yNmPTqtkZAoQZeqA83K7Y3f", “t3PSn5TbMMAEw7Eu36DYctFezRzpX1hzf3M", “t3R3Y5vnBLrEn8L6wFjPjBLnxSUQsKnmFpv", “t3Pcm737EsVkGTbhsu2NekKtJeG92mvYyoN" ]

For the test network, FounderAddressList1..NumFounderAddresses is:

### [ “t2UNzUUx8mWBCRYPRezvA363EYXyEpHokyi", “t2N9PH9Wk9xjqYg9iin1Ua3aekJqfAtE543", “t2NGQjYMQhFndDHguvUw4wZdNdsssA6K7x2", “t2ENg7hHVqqs9JwU5cgjvSbxnT2a9USNfhy", “t2BkYdVCHzvTJJUTx4yZB8qeegD8QsPx8bo", “t2J8q1xH1EuigJ52MfExyyjYtN3VgvshKDf", “t2Crq9mydTm37kZokC68HzT6yez3t2FBnFj", “t2EaMPUiQ1kthqcP5UEkF42CAFKJqXCkXC9", “t2F9dtQc63JDDyrhnfpzvVYTJcr57MkqA12", “t2LPirmnfYSZc481GgZBa6xUGcoovfytBnC", “t26xfxoSw2UV9Pe5o3C8V4YybQD4SESfxtp", “t2D3k4fNdErd66YxtvXEdft9xuLoKD7CcVo", “t2DWYBkxKNivdmsMiivNJzutaQGqmoRjRnL", “t2C3kFF9iQRxfc4B9zgbWo4dQLLqzqjpuGQ", “t2MnT5tzu9HSKcppRyUNwoTp8MUueuSGNaB", “t2AREsWdoW1F8EQYsScsjkgqobmgrkKeUkK", “t2Vf4wKcJ3ZFtLj4jezUUKkwYR92BLHn5UT", “t2K3fdViH6R5tRuXLphKyoYXyZhyWGghDNY", “t2VEn3KiKyHSGyzd3nDw6ESWtaCQHwuv9WC", “t2F8XouqdNMq6zzEvxQXHV1TjwZRHwRg8gC", “t2BS7Mrbaef3fA4xrmkvDisFVXVrRBnZ6Qj", “t2FuSwoLCdBVPwdZuYoHrEzxAb9qy4qjbnL", “t2SX3U8NtrT6gz5Db1AtQCSGjrpptr8JC6h", “t2V51gZNSoJ5kRL74bf9YTtbZuv8Fcqx2FH", “t2FyTsLjjdm4jeVwir4xzj7FAkUidbr1b4R", “t2EYbGLekmpqHyn8UBF6kqpahrYm7D6N1Le", “t2NQTrStZHtJECNFT3dUBLYA9AErxPCmkka", “t2GSWZZJzoesYxfPTWXkFn5UaxjiYxGBU2a", “t2RpffkzyLRevGM3w9aWdqMX6bd8uuAK3vn", “t2JzjoQqnuXtTGSN7k7yk5keURBGvYofh1d", “t2AEefc72ieTnsXKmgK2bZNckiwvZe3oPNL", “t2NNs3ZGZFsNj2wvmVd8BSwSfvETgiLrD8J", “t2ECCQPVcxUCSSQopdNquguEPE14HsVfcUn", “t2JabDUkG8TaqVKYfqDJ3rqkVdHKp6hwXvG", “t2FGzW5Zdc8Cy98ZKmRygsVGi6oKcmYir9n", “t2DUD8a21FtEFn42oVLp5NGbogY13uyjy9t", “t2UjVSd3zheHPgAkuX8WQW2CiC9xHQ8EvWp", “t2TBUAhELyHUn8i6SXYsXz5Lmy7kDzA1uT5", “t2Tz3uCyhP6eizUWDc3bGH7XUC9GQsEyQNc", “t2NysJSZtLwMLWEJ6MH3BsxRh6h27mNcsSy", “t2KXJVVyyrjVxxSeazbY9ksGyft4qsXUNm9", “t2J9YYtH31cveiLZzjaE4AcuwVho6qjTNzp", “t2QgvW4sP9zaGpPMH1GRzy7cpydmuRfB4AZ", “t2NDTJP9MosKpyFPHJmfjc5pGCvAU58XGa4", “t29pHDBWq7qN4EjwSEHg8wEqYe9pkmVrtRP", “t2Ez9KM8VJLuArcxuEkNRAkhNvidKkzXcjJ", “t2D5y7J5fpXajLbGrMBQkFg2mFN8fo3n8cX", “t2UV2wr1PTaUiybpkV3FdSdGxUJeZdZztyt" ]

**Note:** For the test network only, the addresses from index 4 onward have been changed from what was imple- mented at launch. This reflects a hard fork on the test network, starting from *block height* 53127. [[ZcashIssue-2113]](#_bookmark194)

Each address representation in FounderAddressList denotes a *transparent* P2SH multisig address. Let SlowStartShift be defined as in the previous section.

Define:

FounderAddressChangeInterval := ceiling （ SlowStartShift + HalvingInterval＼

NumFounderAddresses

FounderAddressIndex(height) := 1 + floor（ FounderA

height ＼.

ddressChangeInterval

Let RedeemScriptHash(height) be the standard redeem script hash, as defined in [[Bitc-Multisig],](#_bookmark165) for the P2SH multisig address with Base58Check representation given by FounderAddressList FounderAddressIndex(height) .

让RedeemScriptHash（height）成为标准的救赎脚本哈希，如[Bitc-Multisig]中定义的，用于通过FounderAddressList FounderAddressIndex（height）给出Base58Check表示的P2SH多重地址地址。

**Consensus rule:** A *coinbase transaction* for *block height* height 1 *..* SlowStartShift + HalvingInterval 1 **MUST** include at least one output that pays exactly FoundersReward(height) *zatoshi* with a standard P2SH script of the form OP\_HASH160 RedeemScriptHash(height) OP\_EQUAL as its scriptPubKey.

*∈ { − }*

块高度高度为1到SlowStartShift + HalvingInterval 1的coinbase交易必须至少包含一个输出，该输出支付与标准P2SH脚本完全相同的FoundersReward（height）zatoshi，形式为OP\_HASH160 RedeemScriptHash（height）OP\_EQUAL作为其scriptPubKey。

#### Notes:

* No *Founders’ Reward* is required to be paid for height SlowStartShift + HalvingInterval (i.e. after the first halving), or for height = 0 (i.e. the *genesis block* ).

*≥*

* The *Founders’ Reward* addresses are not treated specially in any other way, and there can be other outputs to them, in *coinbase transactions* or otherwise. In particular, it is valid for a *coinbase transaction* with height 1 *..* SlowStartShift + HalvingInterval 1 to have other outputs, possibly to the same address, that do not meet the criterion in the above consensus rule, as long as at least one output meets it.

*{ − }*

*∈*

•创始人的奖励地址不会以任何其他方式专门处理，并且可以有其他输出给他们，在coinbase交易或其他方式。 特别是，它对于高度为1的coinbase事务有效。SlowStartShift + HalvingInterval 1只要至少有一个输出满足上述共识规则中的其他输出，可能为同一地址，但不符合上述共识规则中的条件 它。

## Changes to the Script System

The OP\_CODESEPARATOR opcode has been disabled. This opcode also no longer affects the calculation of signature hashes.

## Bitcoin Improvement Proposals

In general, Bitcoin Improvement Proposals (BIPs) do not apply to **Zcash** unless otherwise specified in this section.

All of the BIPs referenced below should be interpreted by replacing “BTC”, or “bitcoin” used as a currency unit, with “ZEC”; and “satoshi” with “zatoshi”.

The following BIPs apply, otherwise unchanged, to **Zcash**: [[BIP-](#_bookmark146)11], [[BIP-](#_bookmark148)14], [[BIP-31],](#_bookmark151) [[BIP-35],](#_bookmark154) [[BIP-37],](#_bookmark155) [[BIP-61].](#_bookmark156) The following BIPs apply starting from the **Zcash** *genesis block* , i.e. any activation rules or exceptions for particular

*blocks* in the **Bitcoin** *block chain* are to be ignored: [[BIP-](#_bookmark149)16], [[BIP-30],](#_bookmark150) [[BIP-65],](#_bookmark158) [[BIP-66].](#_bookmark159)

[[BIP-34]](#_bookmark153) applies to all blocks other than the **Zcash** *genesis block* (for which the “height in coinbase” was inadver- tently omitted).

[[BIP-13]](#_bookmark147) applies with the changes to address version bytes described in [§ 5.6.1](#_bookmark85) *‘Transparent Payment Addresses’*

on p. 31.

# Differences from the Zerocash paper

## Transaction Structure

**Zerocash** introduces two new operations, which are described in the paper as new transaction types, in addition to the original transaction type of the cryptocurrency on which it is based (e.g. **Bitcoin**).

除了它所基于的加密货币的原始交易类型（例如比特币）之外，Zerocash还引入了两个新的操作，这些操作在本文中被描述为新的交易类型。

In **Zcash**, there is only the original **Bitcoin** transaction type, which is extended to contain a sequence of zero or more **Zcash**-specific operations.

在Zcash中，只有原始的比特币交易类型，它被扩展为包含一系列零个或多个Zcash特定的操作。

This allows for the possibility of chaining transfers of *shielded* value in a single **Zcash** *transaction*, e.g. to spend a *shielded note* that has just been created. (In **Zcash**, we refer to value stored in UTXOs as *transparent* , and value stored in *JoinSplit transfer* output *notes* as *shielded* .) This was not possible in the **Zerocash** design without using multiple transactions. It also allows *transparent* and *shielded* transfers to happen atomically — possibly under the control of nontrivial script conditions, at some cost in distinguishability.

这允许在单个Zcash交易中链接屏蔽值的传输，例如， 花费刚刚创建的屏蔽票据。 （在Zcash中，我们将存储在UTXOs中的值称为透明值，并将存储在JoinSplit传输输出注释中的值作为屏蔽值。）在不使用多个交易的情况下，这在Zerocash设计中是不可能的。 它也允许透明值和屏蔽值转移的原子性 - 可能在非平凡脚本条件的控制下，以可分辨性为代价。

TODO: Describe changes to signing.

## Memo Fields

**Zcash** adds a *memo field* sent from the creator of a *JoinSplit description* to the recipient of each output *note*. This feature is described in more detail in [§5.5](#_bookmark82) *‘Note Plaintexts and Memo Fields’* on p. 30.

Zcash将JoinSplit描述的创建者发送的备注字段添加到每个输出票据的接收者。

## Unification of Mints and Pours

In the original **Zerocash** protocol, there were two kinds of transaction relating to *shielded notes*:

* + - a “Mint” transaction takes value from *transparent* UTXOs as input and produces a new *shielded note* as output.
    - “Mint”交易将透明UTXO的价值作为输入，并产生新的屏蔽票据作为输出。
    - a “Pour” transaction takes up to Nold *shielded notes* as input, and produces up to Nnew *shielded notes* and a

*transparent* UTXO as output.

•“倒入”交易以N\_old屏蔽音符作为输入，并产生多达N\_new屏蔽音符和一个透明UTXO作为输出。

Only “Pour” transactions included a *zk-SNARK* proof.

In **Zcash**, the sequence of operations added to a *transaction* (see [§ 7.1](#_bookmark115) *‘Transaction Structure’* on p. 44) consists only of *JoinSplit transfers*. A *JoinSplit transfer* is a Pour operation generalized to take a *transparent* UTXO as input, allowing *JoinSplit transfers* to subsume the functionality of Mints. An advantage of this is that a **Zcash** *transaction* that takes input from an UTXO can produce up to Nnew output *notes*, improving the indistinguishability properties of the protocol. A related change conceals the input arity of the *JoinSplit transfer* : an unused (zero-value) input is indistinguishable from an input that takes value from a *note*.

在Zcash中，添加到事务中的操作序列（参见第44页第7.1节“事务结构”）只包含JoinSplit传输。 JoinSplit传输是一种Pour操作，通常将透明的UTXO作为输入，允许JoinSplit输出的类型包含Mints。 这样做的一个好处是，从UTXO获取输入的Zcash交易可以产生多达Nnew个输出票据，从而改进协议的不可区分性。 相关的变化隐藏了JoinSplit传输的输入数据：未使用的（零值）输入与从票据获取的价值输入无法区分。

This unification also simplifies the fix to the Faerie Gold attack described below, since no special case is needed for Mints.

## Faerie Gold attack and fix

When a *shielded note* is created in **Zerocash**, the creator is supposed to choose a new ρ value at random. The *nullifier* of the *note* is derived from its *spending key* (ask) and ρ. The *note commitment* is derived from the recip- ient address component apk, the value v, and the commitment trapdoor r, as well as ρ. However nothing prevents creating multiple *notes* with different v and r (hence different *note commitments*) but the same ρ.

在Zerocash中创建屏蔽票据时，创作者应该随机选择一个新的ρ值。 票据的无效因子来自支出关键字（ask）和ρ。 票据承诺来自收件人地址组件apk，值v，承诺陷门r以及ρ。 然而，没有什么能够阻止用不同的v和r（因此不同的票据承诺）创建多个票据，但是相同的ρ。

An adversary can use this to mislead a *note* recipient, by sending two *notes* both of which are verified as valid by

Receive (as defined in [[BCG+2014,](#_bookmark137) Figure 2]), but only one of which can be spent.

敌手可以通过发送两张通过接收验证为有效的记录（如[BCG + 2014，图2]中所定义）来误导记录收件人，但只能使用其中的一个。

We call this a “Faerie Gold” attack — referring to various Celtic legends in which faeries pay mortals in what appears to be gold, but which soon after reveals itself to be leaves, gorse blossoms, gingerbread cakes, or other less valuable things [[LG2004].](#_bookmark180)

我们称之为“精灵黄金”攻击 - 指的是各种凯尔特传说，其中的仙人似乎是金子，但不久之后就显现为叶子，金雀花，姜饼蛋糕或其他不太有价值的东西[LG2004]。

This attack does not violate the security definitions given in [[BCG+2014].](#_bookmark137) The issue could be framed as a problem either with the definition of Completeness, or the definition of Balance:

此攻击不违反[BCG + 2014]中给出的安全定义。 这个问题可以被定义为完整性的定义或平衡的定义：

* + - The Completeness property asserts that a validly received *note* can be spent provided that its *nullifier* does not appear on the ledger. This does not take into account the possibility that distinct *notes*, which are validly received, could have the same *nullifier* . That is, the security definition depends on a protocol de- tail –*nullifiers*– that is not part of the intended abstract security property, and that could be implemented incorrectly.
    - 完整性属性声明可以使用收到的有效票据，只要其否定器没有显示在账本上。 这没有考虑到收到的有效不同票据可能具有相同的否定器。 也就是说，安全性定义依赖于协议的详细说明-nullifiers-不属于预期的抽象安全属性的一部分，并且可能会被错误地实现。
    - The Balance property only asserts that an adversary cannot obtain *more* funds than they have minted or received via payments. It does not prevent an adversary from causing others’ funds to decrease. In a Faerie Gold attack, an adversary can cause spending of a *note* to reduce (to zero) the effective value of another *note* for which the attacker does not know the *spending key* , which violates an intuitive conception of global balance.
    - •平衡财产只声称对手无法获得比他们通过付款铸造或收到更多资金。 这并不妨碍对手造成他人资金减少。 在精灵黄金攻击中，攻击者可以通过花费票据来减少（至零）攻击者不知道支出密钥的另一个票据的有效价值，这违反了对全局平衡的直观概念。

These problems with the security definitions need to be repaired, but doing so is outside the scope of this speci- fication. Here we only describe how **Zcash** addresses the immediate attack.

It would be possible to address the attack by requiring that a recipient remember all of the ρ values for all *notes* they have ever received, and reject duplicates (as proposed in [[GGM2016]).](#_bookmark175) However, this requirement would interfere with the intended **Zcash** feature that a holder of a *spending key* can recover access to (and be sure that they are able to spend) all of their funds, even if they have forgotten everything but the *spending key* .

可以通过要求收件人记住他们收到的所有票据的所有ρ值并拒绝重复（如[GGM2016]中提出的）来解决攻击。 但是，这个要求会干扰Zcash的预期功能，即开支密钥的持有者可以恢复访问（并确保他们能够支出）所有资金，即使他们已经忘记了开支密钥以外的所有内容。

Instead, **Zcash** enforces that an adversary must choose distinct values for each ρ, by making use of the fact that all of the *nullifiers* in *JoinSplit descriptions* that appear in a valid *block chain* must be distinct. This is true regardless of whether the *nullifiers* corresponded to real or dummy notes (see [§4.4.1](#_bookmark40) *‘Dummy Notes’* on p. 19). The *nullifiers* are used as input to hSigCRH to derive a public value hSig which uniquely identifies the transaction, as described in [§4.3](#_bookmark38) *‘JoinSplit Descriptions’* on p. 17. (hSig was already used in **Zerocash** in a way that requires it to be unique in order to maintain indistinguishability of *JoinSplit descriptions*; adding the *nullifiers* to the input of the hash used to calculate it has the effect of making this uniqueness property robust even if the *transaction* creator is an adversary.)

相反，Zcash强制敌手必须为每个ρ选择不同的值，方法是利用JoinSplit描述中出现在有效块链中的所有否定器必须不同。 无论是真实票据还是虚拟票据，情况都是如此（参见第19页§4.4.1“虚拟注释”）。 否定器被用作hSigCRH的输入来派生一个唯一标识该交易的公共值hSig，如§4.3节“JoinSplit描述”中所述。 17.（hSig已经在Zerocash中被使用，要求它是唯一的以便保持JoinSplit描述的不可区分性;将散列函数添加到用于计算它的散列的输入中具有使得这个唯一性属性稳健的效果 即使交易创建者是敌手。）

The ρ value for each output *note* is then derived from a random private seed ϕ and h using PRFρ . The correct

new

Sig ϕ

construction of ρ for each output *note* is enforced by [§ 4.9.1](#_bookmark53) *‘Uniqueness of* ρi *’* on p. 22 in the *JoinSplit state- ment* .

Now even if the creator of a *JoinSplit description* does not choose ϕ randomly, uniqueness of *nullifiers* and col- lision resistance of both hSigCRH and PRFρ will ensure that the derived ρ values are unique, at least for any two *JoinSplit descriptions* that get into a valid *block chain*. This is sufficient to prevent the Faerie Gold attack.

A variation on the attack attempts to cause the *nullifier* of a sent *note* to be repeated, without repeating ρ. However, since the *nullifier* is computed as PRFnf (ρ), this is only possible if the adversary finds a collision (across both

inputs) on PRFnf

ask

, which is assumed to be infeasible — see [§4.1.2](#_bookmark24) *‘Pseudo Random Functions’* on p. 12.

Critically, “*nullifier* integrity” [(§4.9.1](#_bookmark50) *‘Nullifier integrity’* on p. 22) is enforced whether or not the enforceMerklePathi flag is set for an input *note*. If this were not the case then an adversary could perform the attack by creating a zero- valued *note* with a repeated *nullifier* , since the *nullifier* does not depend on the value.

必须保证的是，无论是否为输入备注设置了enforceMerklePathi标志，都会强制执行“无效器完整性”（§4.9.1“无效化器完整性”，见第22页）。 如果情况并非如此，那么攻击者可以通过用重复的否定器创建零值票据来执行攻击，因为否定器不依赖于该值。

## Internal hash collision attack and fix

The **Zerocash** security proof requires that the composition of COMMr and COMMs is a computationally binding commitment to its inputs apk, v, and ρ. However, the instantiation of COMMr and COMMs in section 5.1 of the paper did not meet the definition of a binding commitment at a 128-bit security level. Specifically, the internal hash of apk and ρ is truncated to 128 bits (motivated by providing statistical hiding security). This allows an attacker, with a

work factor on the order of 264, to find distinct pairs (apk*,* ρ) and (apk*t,* ρ*t* ) with colliding outputs of the truncated

hash, and therefore the same *note commitment* . This would have allowed such an attacker to break the Balance property by double-spending *notes*, potentially creating arbitrary amounts of currency for themself [[HW2016].](#_bookmark177)

Zerocash安全证明要求COMMr和COMMs的组合对其输入apk，v和ρ具有计算上的约束力。 然而，本文第5.1节中的COMMr和COMMs的实例化不符合128位安全级别的绑定承诺的定义。 具体来说，apk和ρ的内部散列被截断为128位（通过提供统计隐藏安全性）。 这允许工作因子为2^64的攻击者通过截短散列的冲突输出找到不同的对（apk，ρ）和（apkt，ρt），因此也是相同的音符承诺。 这将允许这样的攻击者通过双重支出笔记打破平衡财产，可能为自己创造任意数量的货币[HW2016]。

**Zcash** uses a simpler construction with a single SHA-256 evaluation for the commitment. The motivation for the nested construction in **Zerocash** was to allow Mint transactions to be publically verified without requiring a *zero- knowledge proof* (as described under step 3 in [[BCG+2014,](#_bookmark137) section 1.3]). Since **Zcash** combines “Mint” and “Pour” transactions into a generalized *JoinSplit transfer* which always uses a *zero-knowledge proof* , it does not require the nesting. A side benefit is that this reduces the number of SHA256Compress evaluations needed to compute each *note commitment* from three to two, saving a total of four SHA256Compress evaluations in the *JoinSplit statement* .

Zcash使用更简单的构造和单个SHA-256评估来完成承诺。 Zerocash中嵌套建设的动机是允许Mint交易在不需要零知识证明的情况下进行公开验证（如[BCG + 2014，第1.3节]中的步骤3所述）。 由于Zcash将“Mint”和“Pour”交易合并为一个通常使用零知识证明的广义JoinSplit传输，因此它不需要嵌套。 一个好处是，这减少了计算每个票据承诺所需的SHA256Compress分析次数（从3到2），从而在JoinSplit语句中总共节省了4次SHA256Compress分析。

**Note: Zcash** *note commitments* are not statistically hiding, so **Zcash** does not support the “everlasting anonymity” property described in [[BCG+2014,](#_bookmark137) section 8.1], even when used as described in that section. While it is possible to define a statistically hiding, computationally binding commitment scheme for this use at a 128-bit security level, the overhead of doing so within the *JoinSplit statement* was not considered to justify the benefits.

Zcash票据承诺没有统计隐藏性，因此Zcash不支持[BCG + 2014，第8.1节]中描述的“永久匿名”财产，即使按照该部分所述使用。 虽然可以在128位安全级别上定义统计隐藏的计算绑定承诺方案，但在JoinSplit语句中这样做的开销并不被认为是有利的。

## Changes to PRF inputs and truncation

The format of inputs to the PRFs instantiated in [§5.4.2](#_bookmark69) *‘Pseudo Random Functions’* on p. 26 has changed relative to **Zerocash**. There is also a requirement for another PRF, PRFρ, which must be domain-separated from the others.

In the **Zerocash** protocol, ρold is truncated from 256 to 254 bits in the input to PRFsn (which corresponds to PRFnf

i

in **Zcash**). Also, hSig is truncated from 256 to 253 bits in the input to PRFpk. These truncations are not taken into account in the security proofs.

第5.4.2节“伪随机函数”中实例化的PRF的输入格式。 26相对于Zerocash已经发生了变化。 另外还需要另一个PRF，即PRFρ，它必须与其他域分开。 在Zerocash协议中，ρold在PRFsn（对应于Zcash中的PRFnf）的输入中从256到254位截断。 而且，hSig在PRFpk的输入中从256到253位被截断。 这些截断在安全性证明中未被考虑。

Both truncations affect the validity of the proof sketch for Lemma D.2 in the proof of Ledger Indistinguishability in [[BCG+2014,](#_bookmark137) Appendix D].

In more detail:

* + - In the argument relating **H** and O2, it is stated that in O2, “for each *i ∈ {*1*,* 2*},* sni := PRFsn (ρ) for a random

(and not previously used) ρ”. It is also argued that “the calls to PRFsn are each by

ask

. The latter

ask

definition unique”

assertion depends on the fact that ρ is “not previously used”. However, the argument is incorrect because the

truncated input to PRFsn , i.e. [ρ] , may repeat even if ρ does not.

ask

254

* In the same argument, it is stated that “with overwhelming probability, hSig is unique”. In fact what is required to be unique is the truncated input to PRFpk, i.e. [hSig]253 = [CRH(pksig )]253. In practice this value will be unique under a plausible assumption on CRH provided that pksig is chosen randomly, but no formal argument for this is presented.

Note that ρ is truncated in the input to PRFsn but not in the input to COMMr, which further complicates the analysis.

As further evidence that it is essential for the proofs to explicitly take any such truncations into account, consider a slightly modified protocol in which ρ is truncated in the input to COMMr but not in the input to PRFsn. In that case, it would be possible to violate balance by creating two *notes* for which ρ differs only in the truncated bits. These *notes* would have the same *note commitment* but different *nullifiers*, so it would be possible to spend the same value twice.

请注意，ρ在PRFsn的输入中被截断，而在COMMr的输入中截断，这进一步使分析变得复杂。

作为进一步的证据，证明明确地考虑任何这样的截断是必要的，考虑略微修改的协议，其中ρ在输入到COMMr中截断，但不在PRFsn的输入中截断。 在这种情况下，通过创建两个音符来抵消平衡是可能的，因为ρ仅在截断位中不同。 这些票据将具有相同的票据承诺但具有不同的否定器，因此可能花费两次相同的值。

For resistance to Faerie Gold attacks as described in [§7.4](#_bookmark119) *‘Faerie Gold attack and fix’* on p. 45, **Zcash** depends on collision resistance of hSigCRH (instantiated using BLAKE2b-256) and PRFρ (instantiated using SHA256Compress). Collision resistance of a truncated hash does not follow from collision resistance of the original hash, even if the truncation is only by one bit. This motivated avoiding truncation along any path from the inputs to the computation of hSig to the uses of ρ.

截断散列的冲突阻力并不依据原始散列的冲突阻力，即使截断只有一位。 这种动机避免了从输入到计算hSig到使用ρ的任何路径的截断。

Since the PRFs are instantiated using SHA256Compress which has an input block size of 512 bits (of which 256 bits are used for the PRF input and 4 bits are used for domain separation), it was necessary to reduce the size of the PRF key to 252 bits. The key is set to ask in the case of PRFaddr, PRFnf , and PRFpk, and to ϕ (which does not exist in

**Zerocash**) for PRFρ, and so those values have been reduced to 252 bits. This is preferable to requiring reasoning

about truncation, and 252 bits is quite sufficient for security of these cryptovalues.

由于PRF是使用SHA256Compress实例化的，其输入块大小为512位（其中256位用于PRF输入，4位用于域分离），因此有必要将PRF密钥的大小减小到252位。 在PRFaddr，PRFnf和PRFpk的情况下，将关键字设置为询问，并且针对φ（其不存在于Zerocash）用于PRFρ，所以这些值已经减少到252位。 这比推理要好

关于截断，252位对于这些密码值的安全性来说是足够的。

## In-band secret distribution

**Zerocash** specified ECIES (referencing Certicom’s SEC 1 standard) as the encryption scheme used for the in-band secret distribution. This has been changed to a scheme based on Curve25519 key agreement, and the authenti- cated encryption algorithm AEAD\_CHACHA20\_POLY1305. This scheme is still loosely based on ECIES, and on the crypto\_box\_seal scheme defined in libsodium [[libsodium-Seal].](#_bookmark182)

The motivations for this change were as follows:

* + - The **Zerocash** paper did not specify the curve to be used. We believe that Curve25519 has significant side- channel resistance, performance, implementation complexity, and robustness advantages over most other available curve choices, as explained in [[Bern2006].](#_bookmark144)
    - Zerocash论文中没有指定要使用的曲线。 正如[Bern2006]中所解释的，我们相信Curve25519与其他大多数可用曲线选择相比，具有明显的旁路通道阻抗，性能，实现复杂性和鲁棒性优势。
    - ECIES permits many options, which were not specified. There are at least –counting conservatively– 576 possible combinations of options and algorithms over the four standards (ANSI X9.63, IEEE Std 1363a-2004, ISO/IEC 18033-2, and SEC 1) that define ECIES variants [[MAEA2010].](#_bookmark183)
    - •ECIES允许许多选项，但未指定。 在定义ECIES变体[MAEA2010]的四个标准（ANSI X9.63，IEEE标准1363a-2004，ISO / IEC 18033-2和SEC 1）中，至少有一些可能的选项和算法的组合。
    - Although the **Zerocash** paper states that ECIES satisfies key privacy (as defined in [[BBDP2001]),](#_bookmark136) it is not clear that this holds for all curve parameters and key distributions. For example, if a group of non-prime order is used, the distribution of ciphertexts could be distinguishable depending on the order of the points rep- resenting the ephemeral and recipient public keys. Public key validity is also a concern. Curve25519 key agreement is defined in a way that avoids these concerns due to the curve structure and the “clamping” of private keys.
    - 尽管Zerocash论文指出ECIES满足关键隐私（如[BBDP2001]中所定义），但对于所有曲线参数和关键分布情况，这并不清楚。 例如，如果使用一组非主要次序，则密文的分布可以根据表示短暂和接收者公钥的点的顺序来区分。 公钥有效性也是一个问题。 Curve25519密钥协议的定义方式避免了由于曲线结构和私钥“夹紧”而引起的这些问题
    - Unlike the DHAES/DHIES proposal on which it is based [[ABR1999],](#_bookmark134) ECIES does not require a representation of the sender’s ephemeral public key to be included in the input to the KDF, which may impair the security properties of the scheme. (The Std 1363a-2004 version of ECIES [[IEEE2004]](#_bookmark179) has a “DHAES mode” that allows this, but the representation of the key input is underspecified, leading to incompatible implementations.) The scheme we use has both the ephemeral and recipient public key encodings –which are unambiguous for Curve25519– and also hSig and a nonce as described below, as input to the KDF. Note that because pkenc is included in the KDF input, being able to break the Elliptic Curve Diffie-Hellman Problem on Curve25519 (without breaking AEAD\_CHACHA20\_POLY1305 as an authenticated encryption scheme or BLAKE2b-256 as a KDF) would not help to decrypt the *transmitted notes ciphertext* unless pkenc is known or guessed.

•与其所依据的DHAES / DHIES提案[ABR1999]不同，ECIES不要求发件人的临时公钥被包含在KDF的输入中，这可能会损害该计划的安全属性。 （ECIES [IEEE2004]的Std 1363a-2004版本有一个“DHAES模式”，允许这样做，但是键输入的表示没有详细说明，导致不兼容的实现。）我们使用的方案既有短暂接收者公钥 编码 - 这对于Curve25519来说是明确的 - 并且还有hSig和随机数，如下所述，作为KDF的输入。 请注意，因为pkenc包含在KDF输入中，所以能够在Curve25519上打破椭圆曲线Diffie-Hellman问题（不需要将AEAD\_CHACHA20\_POLY1305作为已认证的加密方案，或将BLAKE2b-256作为KDF进行破解）将无助于解密传输的票据密文 除非pkenc是已知的或猜测的。

* + - The KDF also takes a public seed hSig as input. This can be modeled as using a different “randomness extrac- tor” for each *JoinSplit transfer* , which limits degradation of security with the number of *JoinSplit transfers*. This facilitates security analysis as explained in [[DGKM2011]](#_bookmark172) — see section 7 of that paper for a security proof that can be applied to this construction under the assumption that single-block BLAKE2b-256 is a “weak

PRF”. Note that hSig is authenticated, by the ZK proof, as having been chosen with knowledge of aold old , so

sk,1..N

an adversary cannot modify it in a ciphertext from someone else’s transaction for use in a chosen-ciphertext attack without detection.

•KDF还将公共种子hSig作为输入。 这可以模拟为每个JoinSplit传输使用不同的“随机抽取器”，这可以通过JoinSplit传输的数量来限制安全性的降低。 这有助于进行安全分析，如[DGKM2011]中所述 - 请参阅该文章的第7部分，以便在单块BLAKE2b-256是“弱PRF”的假设下应用于此构造的安全证明。 请注意，通过ZK证明，hSig被认证为具有aold old的知识，因此攻击者无法在其他人的交易中以密文对其进行修改，以用于未经检测的选择密文攻击。

* + - The scheme used by **Zcash** includes an optimization that reuses the same ephemeral key (with different nonces) for the two ciphertexts encrypted in each *JoinSplit description*.
    - •Zcash使用的方案包含一个优化，该方法重复使用每个JoinSplit描述中加密的两个密文相同的临时密钥（具有不同的随机数）。

The security proofs of [[ABR1999]](#_bookmark134) can be adapted straightforwardly to the resulting scheme. Although DHAES as defined in that paper does not pass the recipient public key or a public seed to the hash function *H*, this does not impair the proof because we can consider *H* to be the specialization of our KDF to a given recipient key and seed. It is necessary to adapt the “HDH independence” assumptions and the proof slightly to take into account that the ephemeral key is reused for two encryptions.

[ABR1999]的安全证明可以直接适用于最终的方案。 尽管该论文定义的DHAES没有将接收者公钥或公共种子传递给散列函数H，但这并不影响证据，因为我们可以认为H是我们KDF对给定接收者密钥和种子的专门化。 有必要稍微调整“HDH独立性”假设和证明以考虑到短暂密钥被重复用于两种加密。

Note that the 256-bit key for AEAD\_CHACHA20\_POLY1305 maintains a high concrete security level even under at- tacks using parallel hardware [[Bern2005]](#_bookmark143) in the multi-user setting [[Zave2012].](#_bookmark193) This is especially necessary because the privacy of **Zcash** transactions may need to be maintained far into the future, and upgrading the encryption algorithm would not prevent a future adversary from attempting to decrypt ciphertexts encrypted before the up- grade. Other cryptovalues that could be attacked to break the privacy of transactions are also sufficiently long to resist parallel brute force in the multi-user setting: ask is 252 bits, and skenc is no shorter than ask.

请注意，即使在多用户设置[Zave2012]中使用并行硬件[Bern2005]的情况下，AEAD\_CHACHA20\_POLY1305的256位密钥也能保持较高的具体安全级别。 这是特别必要的，因为Zcash事务的隐私可能需要在未来维持很久，并且升级加密算法不会阻止未来的攻击者试图解密在高级之前加密的密文。 其他可以攻击以破坏交易隐私的加密值也足够长，以抵制多用户设置中的并行蛮力：ask为252位，并且skenc不低于ask。

## Omission in Zerocash security proof

The abstract **Zerocash** protocol requires PRFaddr only to be a PRF; it is not specified to be collision-resistant. This reveals a flaw in the proof of the Balance property.

Suppose that an adversary finds a collision on PRFaddr such that a1 and a2 are distinct *spending keys* for the same

sk

sk

apk. Because the *note commitment* is to apk, but the *nullifier* is computed from ask (and ρ), the adversary is able to double-spend the note, once with each ask. This is not detected because each spend reveals a different *nullifier* . The *JoinSplit statements* are still valid because they can only check that the ask in the witness is *some* preimage of the apk used in the *note commitment* .

The error is in the proof of Balance in [[BCG+2014,](#_bookmark137) Appendix D.3]. For the “ violates Condition I” case, the proof says:

*A*

“(i) If cmold = cmold, then the fact that snold \* snold implies that the witness *a* contains two distinct openings of

1 2 1 2

cmold (the first opening contains (aold *,* ρold ), while the second opening contains (aold *,* ρold )). This violates the

1 sk,1 1 sk,2 2

binding property of the commitment scheme COMM."

In fact the openings do not contain aold ; they contain aold . (In **Zcash** cmold opens directly to (aold *,* vold*,* ρold ), and in

sk,i

**Zerocash** it opens to (vold*,* COMMs (aold *,* ρold ).)

**pk**,i i

**pk**,i i i

i **pk**,i i

A similar error occurs in the argument for the “*A* violates Condition II” case.

The flaw is not exploitable for the actual instantiations of PRFaddr in **Zerocash** and **Zcash**, which *are* collision- resistant assuming that SHA256Compress is.

The proof can be straightforwardly repaired. The intuition is that we can rely on collision resistance of PRFaddr

(on both its arguments) to argue that distinctness of aold and aold , together with constraint 1(b) of the *JoinSplit*

sk,1

sk,2

and a

*statement* (see [§4.9.1](#_bookmark51) *‘Spend authority’* on p. 22), implies distinctness of aold

pk,1

old pk,2

, therefore distinct openings

of the *note commitment* when Condition I or II is violated.

## Miscellaneous

* + - The paper defines a *note* as ((apk*,* pkenc )*,* v*,* ρ*,* r*,* s*,* cm), whereas this specification defines it as (apk*,* v*,* ρ*,* r). The instantiation of COMMs in section 5.1 of the paper did not actually use s, and neither does the new instan- tiation of COMM in **Zcash**. pkenc is also not needed as part of a *note*: it is not an input to COMM nor is it constrained by the **Zerocash** POUR *statement* or the **Zcash** *JoinSplit statement* . cm can be computed from the other fields.
    - The length of proof encodings given in the paper is 288 bytes. This differs from the 296 bytes specified in [§ 5.4.9.1](#_bookmark80) *‘PHGR13’* on p. 29, because both the *x*-coordinate and compressed *y*-coordinate of each point need to be represented. Although it is possible to encode a proof in 288 bytes by making use of the fact that elements of Fq can be represented in 254 bits, we prefer to use the standard formats for points defined in [[IEEE2004].](#_bookmark179) The fork of *libsnark* used by **Zcash** uses this standard encoding rather than the less efficient (uncompressed) one used by upstream *libsnark* .
    - The range of monetary values differs. In **Zcash**, this range is 0 *..* MAX\_MONEY ; in **Zerocash** it is 0 *..* 264 1 . (The *JoinSplit statement* still only directly enforces that the sum of amounts in a given *JoinSplit transfer* is in the latter range; this enforcement is technically redundant given that the Balance property holds.)

*{ } { − }*

# Acknowledgements

The inventors of **Zerocash** are Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza.

The authors would like to thank everyone with whom they have discussed the **Zerocash** protocol design; in addi- tion to the inventors, this includes Mike Perry, Isis Lovecruft, Leif Ryge, Andrew Miller, Zooko Wilcox, Samantha Hulsey, Jack Grigg, Simon Liu, Ariel Gabizon, jl777, Ben Blaxill, Alex Balducci, Jake Tarren, Solar Designer, Ling Ren, Alison Stevenson, John Tromp, Paige Peterson, Maureen Walsh, Jay Graber, Jack Gavigan, Filippo Valsorda, Zaki Manian, and no doubt others.

**Zcash** has benefited from security audits performed by NCC Group and Coinspect.

The Faerie Gold attack was found by Zooko Wilcox; subsequent analysis of variations on the attack was performed by Daira Hopwood and Sean Bowe. The internal hash collision attack was found by Taylor Hornby. The error in the **Zerocash** proof of Balance relating to collision-resistance of PRFaddr was found by Daira Hopwood. The errors in the proof of Ledger Indistinguishability mentioned in [§ 7.6](#_bookmark122) *‘Changes to PRF inputs and truncation’* on p. 46 were also found by Daira Hopwood.

# Change history

#### 2017.0-beta-2.9

* Refer to skenc as a *receiving key* rather than as a viewing key.
* Updates for *incoming viewing key* support.

#### 2017.0-beta-2.8

* Correct the non-normative note describing how to check the order of *π*B .

#### 2017.0-beta-2.7

* Fix an off-by-one error in the specification of the Equihash algorithm binding condition. (The implementa- tion in zcashd was as intended.)
* Correct the types and consensus rules for *transaction version numbers* and *block version numbers*. (Again, the implementation in zcashd was as intended.)
* Clarify the computation of hi in a *JoinSplit statement* .

#### 2017.0-beta-2.6

* Be more precise when talking about curve points and pairing groups.

#### 2017.0-beta-2.5

* Clarify the consensus rule preventing double-spends.
* Clarify what a *note commitment* opens to in [§7.8](#_bookmark126) *‘Omission in* ***Zerocash*** *security proof’* on p. 48.
* Correct the order of arguments to COMM in [§5.4.7](#_bookmark75) *‘Commitment’* on p. 28.
* Correct a statement about indistinguishability of *JoinSplit descriptions*.
* Change the *Founders’ Reward* addresses, for the test network only, to reflect the hard fork described in [[ZcashIssue-2113].](#_bookmark194)

#### 2017.0-beta-2.4

* Explain a variation on the Faerie Gold attack and why it is prevented.
* Generalize the description of the InternalH attack to include finding collisions on (apk*,* ρ) rather than just on

ρ.

* Rename enforcei to enforceMerklePathi.

#### 2017.0-beta-2.3

* Specify the security requirements on the *SHA-256 compression* function in order for the scheme in [§ 5.4.7](#_bookmark75)

*‘Commitment’* on p. 28 to be a secure commitment.

* Specify G2 more precisely.
* Explain the use of interstitial *treestates* in chained *JoinSplit transfers*.

#### 2017.0-beta-2.2

* Give definitions of computational binding and computational hiding for commitment schemes.
* Give a definition of statistical zero knowledge.
* Reference the white paper on MPC parameter generation [[BGG2016].](#_bookmark145)

#### 2017.0-beta-2.1

* Merkle is a bit length, not a byte length.
* Specify the maximum *block* size.

#### 2017.0-beta-2

* Add abstract and keywords.
* Fix a typo in the definition of *nullifier* integrity.
* Make the description of *block chains* more consistent with upstream **Bitcoin** documentation (referring to “best“ chains rather than using the concept of a *block chain view* ).
* Define how nodes select a best chain.

#### 2016.0-beta-1.13

* Specify the difficulty adjustment algorithm.
* Clarify some definitions of fields in a *block header* .
* Define PRFaddr in [§4.2](#_bookmark37) *‘Key Components’* on p. 17.

#### 2016.0-beta-1.12

* Update the hashes of proving and verifying keys for the final Sprout parameters.
* Add cross references from *payment address* and *spending key* encoding sections to where the key compo- nents are specified.
* Add acknowledgements for Filippo Valsorda and Zaki Manian.

#### 2016.0-beta-1.11

* Specify a check on the order of *π*B in a *zero-knowledge proof* .
* Note that due to an oversight, the **Zcash** *genesis block* does not follow [[BIP-34].](#_bookmark153)

#### 2016.0-beta-1.10

* Update reference to the Equihash paper [[BK2016].](#_bookmark170) (The newer version has no algorithmic changes, but the section discussing potential ASIC implementations is substantially expanded.)
* Clarify the discussion of proof size in “Differences from the **Zerocash** paper”.

#### 2016.0-beta-1.9

* Add *Founders’ Reward* addresses for the production network.
* Change “*protected* ” terminology to “*shielded* ”.

#### 2016.0-beta-1.8

* Revise the lead bytes for *transparent* P2SH and P2PKH addresses, and reencode the testnet *Founders’ Reward*

addresses.

* Add a section on which BIPs apply to **Zcash**.
* Specify that OP\_CODESEPARATOR has been disabled, and no longer affects signature hashes.
* Change the representation type of vpub\_old and vpub\_new to uint64\_t. (This is not a consensus change

because the type of vold and vnew was already specified to be *{*0 *..* MAX\_MONEY*}*; it just better reflects the

pub

pub

implementation.)

* Correct the representation type of the *block* nVersion field to uint32\_t.

#### 2016.0-beta-1.7

* Clarify the consensus rule for payment of the *Founders’ Reward* , in response to an issue raised by the NCC audit.

#### 2016.0-beta-1.6

* Fix an error in the definition of the sortedness condition for Equihash: it is the sequences of indices that are sorted, not the sequences of hashes.
* Correct the number of bytes in the encoding of solutionSize.
* Update the section on encoding of *transparent* addresses. (The precise prefixes are not decided yet.)
* Clarify why BLAKE2b- is different from truncated BLAKE2b-512.
* Clarify a note about SU-CMA security for signatures.
* Add a note about PRFnf corresponding to PRFsn in **Zerocash**.
* Add a paragraph about key length in [§7.7](#_bookmark124) *‘In-band secret distribution’* on p. 47.
* Add acknowledgements for John Tromp, Paige Peterson, Maureen Walsh, Jay Graber, and Jack Gavigan.

#### 2016.0-beta-1.5

* Update the *Founders’ Reward* address list.
* Add some clarifications based on Eli Ben-Sasson’s review.

#### 2016.0-beta-1.4

* Specify the *block subsidy* , *miner subsidy* , and the *Founders’ Reward* .
* Specify *coinbase transaction* outputs to *Founders’ Reward* addresses.
* Improve notation (for example “*·*” for multiplication and “*T* [亿]” for sequence types) to avoid ambiguity.

#### 2016.0-beta-1.3

* Correct the omission of solutionSize from the *block header* format.
* Document that compactSize uint encodings must be canonical.
* Add a note about conformance language in the introduction.
* Add acknowledgements for Solar Designer, Ling Ren and Alison Stevenson, and for the NCC Group and Coinspect security audits.

#### 2016.0-beta-1.2

* Remove GeneralCRH in favour of specifying hSigCRH and EquihashGen directly in terms of BLAKE2b.
* Correct the security requirement for EquihashGen.

#### 2016.0-beta-1.1

* Add a specification of abstract signatures.
* Clarify what is signed in the “Sending Notes” section.
* Specify ZK parameter generation as a randomized algorithm, rather than as a distribution of parameters.

#### 2016.0-beta-1

* Major reorganisation to separate the abstract cryptographic protocol from the algorithm instantiations.
* Add type declarations.
* Add a “High-level Overview” section.
* Add a section specifying the *zero-knowledge proving system* and the encoding of proofs. Change the en- coding of points in proofs to follow IEEE Std 1363[a].
* Add a section on consensus changes from **Bitcoin**, and the specification of Equihash.
* Complete the “Differences from the **Zerocash** paper” section.
* Correct the Merkle tree depth to 29.
* Change the length of *memo fields* to 512 bytes.
* Switch the *JoinSplit signature* scheme to Ed25519, with consequent changes to the computation of hSig.
* Fix the lead bytes in *payment address* and *spending key* encodings to match the implemented protocol.
* Add a consensus rule about the ranges of vold and vnew.

pub

pub

* Clarify cryptographic security requirements and added definitions relating to the in-band secret distribution.
* Add various citations: the “Fixing Vulnerabilities in the Zcash Protocol” and “Why Equihash?” blog posts, sev- eral crypto papers for security definitions, the **Bitcoin** whitepaper, the **CryptoNote** whitepaper, and several references to **Bitcoin** documentation.
* Reference the extended version of the **Zerocash** paper rather than the Oakland proceedings version.
* Add *JoinSplit transfers* to the Concepts section.
* Add a section on Coinbase Transactions.
* Add acknowledgements for Jack Grigg, Simon Liu, Ariel Gabizon, jl777, Ben Blaxill, Alex Balducci, and Jake Tarren.
* Fix a Makefile compatibility problem with the escaping behaviour of echo.
* Switch to biber for the bibliography generation, and add backreferences.
* Make the date format in references more consistent.
* Add visited dates to all URLs in references.
* Terminology changes.

#### 2016.0-alpha-3.1

* Change main font to Quattrocento.

#### 2016.0-alpha-3

* Change version numbering convention (no other changes).

#### 2.0-alpha-3

* Allow anchoring to any previous output *treestate* in the same *transaction*, rather than just the immediately preceding output *treestate*.
* Add change history.

#### 2.0-alpha-2

* Change from truncated BLAKE2b-512 to BLAKE2b-256.
* Clarify endianness, and that uses of BLAKE2b are unkeyed.
* Minor correction to what *SIGHASH types* cover.
* Add “as intended for the **Zcash** release of summer 2016" to title page.
* Require PRFaddr to be collision-resistant (see [§7.8](#_bookmark126) *‘Omission in* ***Zerocash*** *security proof’* on p. 48).
* Add specification of path computation for the *incremental Merkle tree*.
* Add a note in [§ 4.9.1](#_bookmark49) *‘Merkle path validity’* on p. 21 about how this condition corresponds to conditions in the **Zerocash** paper.
* Changes to terminology around keys.

#### 2.0-alpha-1

* First version intended for public review.

# References

[ABR1999] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. *DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem*. Cryptology ePrint Archive: Report 1999/007. Received March 17, 1999. September 1998. URL: [https : / / eprint . iacr . org / 1999 / 007](https://eprint.iacr.org/1999/007) (visited on 2016-08-21)

(*↑* p[13,](#_bookmark25) [47,](#_bookmark123) [48).](#_bookmark125)

[ANWW2013] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O’Hearn, and Christian Winnerlein.

*BLAKE2: simpler, smaller, fast as MD5*. January 29, 2013. URL: <https://blake2.net/#sp>(visited on 2016-08-14) (*↑* p[25,](#_bookmark63) [26,](#_bookmark68) [27).](#_bookmark71)

[BBDP2001] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. *Key-Privacy in Public- Key Encryption*. September 2001. URL: [https://cseweb.ucsd.edu/~mihir/papers/anonenc.](https://cseweb.ucsd.edu/%7Emihir/papers/anonenc.html)

[html](https://cseweb.ucsd.edu/%7Emihir/papers/anonenc.html) (visited on 2016-08-14). Full version. (*↑* p[14,](#_bookmark29) [47).](#_bookmark123)

[BCG+2014] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. *Zerocash: Decentralized Anonymous Payments from Bitcoin (extended ver- sion)*. URL: <http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf> (visited on 2016-08-06). A condensed version appeared in *Proceedings of the IEEE Sympo- sium on Security and Privacy (Oakland) 2014*, pages 459–474; IEEE, 2014. ( p[5,](#_bookmark2) [7,](#_bookmark9) [13,](#_bookmark25) [20,](#_bookmark42) [21,](#_bookmark46) [23,](#_bookmark56)

*↑*

[45,](#_bookmark118) [46,](#_bookmark120) [48).](#_bookmark125)

[BCGTV2013] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. *SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge*. Cryptology ePrint Archive: Report 2013/507. Last revised October 7, 2013. URL: [https : / / eprint . iacr . org / 2013 / 507](https://eprint.iacr.org/2013/507)

(visited on 2016-08-31). An earlier version appeared in *Proceedings of the 33rd Annual Inter- national Cryptology Conference, CRYPTO ’13*, pages 90–108; IACR, 2013. (*↑* p[29).](#_bookmark78)

[BCTV2014] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. “Scalable Zero Knowledge via Cycles of Elliptic Curves (extended version)”. In: *Advances in Cryptology - CRYPTO 2014*. Vol. 8617. Lecture Notes in Computer Science. Springer, 2014, pages 276–294. URL: [https://](https://www.cs.tau.ac.il/%7Etromer/papers/scalablezk-20140803.pdf) [www . cs . tau . ac . il / ~tromer / papers / scalablezk - 20140803 . pdf](https://www.cs.tau.ac.il/%7Etromer/papers/scalablezk-20140803.pdf) (visited on 2016-09-01)

(*↑* p[17).](#_bookmark36)

[BCTV2015] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture*. Cryptology ePrint Archive: Report 2013/879. Last revised May 19, 2015. URL: <https://eprint.iacr.org/2013/879>(visited on 2016-08-21)

(*↑* p[29,](#_bookmark78) [30).](#_bookmark81)

[BDEHR2011] Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Hülsing, and Markus Rückert. *On the Security of the Winternitz One-Time Signature Scheme (full version)*. Cryptology ePrint Archive: Report 2011/191. Received April 13, 2011. URL: <https://eprint.iacr.org/2011/191>

(visited on 2016-09-05) (*↑* p[15).](#_bookmark31)

[BDL+2012] Daniel Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. “High-speed high- security signatures”. In: *Journal of Cryptographic Engineering* 2 (September 26, 2011), pages 77–

89. URL: [http : / / cr . yp . to / papers . html # ed25519](http://cr.yp.to/papers.html#ed25519) (visited on 2016-08-14). Document ID: a1a62a2f76d23f65d622484ddd09caf8. (*↑* p[27).](#_bookmark71)

[Bern2005] Daniel Bernstein. “Understanding brute force”. In: *ECRYPT STVL Workshop on Symmetric Key Encryption, eSTREAM report 2005/036*. April 25, 2005. URL: [https : / / cr . yp . to / papers .](https://cr.yp.to/papers.html#bruteforce)

[html#bruteforce](https://cr.yp.to/papers.html#bruteforce) (visited on 2016-09-24). Document ID: 73e92f5b71793b498288efe81fe55dee. (*↑* p[48).](#_bookmark125)

[Bern2006] Daniel Bernstein. “Curve25519: new Diffie-Hellman speed records”. In: *Public Key Cryptogra- phy - 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, February 9, 2006.

URL: [http : / / cr . yp . to / papers . html # curve25519](http://cr.yp.to/papers.html#curve25519) (visited on 2016-08-14). Document ID: 4230efdfa673480fc079449d90f322c0. (*↑* p[13,](#_bookmark25) [27,](#_bookmark71) [32,](#_bookmark88) [47).](#_bookmark123)

[BGG2016] Sean Bowe, Ariel Gabizon, and Matthew Green. *A multi-party protocol for constructing the public parameters of the Pinocchio zk-SNARK*. November 24, 2016. URL: [https :/ / github .](https://github.com/zcash/mpc/blob/master/whitepaper.pdf)

[com/zcash/mpc/blob/master/whitepaper.pdf](https://github.com/zcash/mpc/blob/master/whitepaper.pdf) (visited on 2017-02-11) (*↑* p[33,](#_bookmark91) [50).](#_bookmark131)

[BIP-11] Gavin Andresen. *M-of-N Standard Transactions*. Bitcoin Improvement Proposal 11. Created Oc- tober 18, 2011. URL: <https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki>

(visited on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-13] Gavin Andresen. *Address Format for pay-to-script-hash*. Bitcoin Improvement Proposal 13. Created October 18, 2011. URL: [https : / / github . com / bitcoin / bips / blob / master / bip -](https://github.com/bitcoin/bips/blob/master/bip-0013.mediawiki)

[0013.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0013.mediawiki) (visited on 2016-09-24) (*↑* p[31,](#_bookmark84) [44).](#_bookmark112)

[BIP-14] Amir Taaki and Patrick Strateman. *Protocol Version and User Agent*. Bitcoin Improvement Pro- posal 14. Created November 10, 2011. URL: [https://github.com/bitcoin/bips/blob/master/](https://github.com/bitcoin/bips/blob/master/bip-0014.mediawiki)

[bip-0014.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0014.mediawiki) (visited on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-16] Gavin Andresen. *Pay to Script Hash*. Bitcoin Improvement Proposal 16. Created January 3, 2012.

URL: [https://github.com/bitcoin/bips/blob/master/bip- 0016.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki) (visited on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-30] Pieter Wuille. *Duplicate transactions*. Bitcoin Improvement Proposal 30. Created February 22, 2012. URL: <https://github.com/bitcoin/bips/blob/master/bip-0030.mediawiki>(visited

on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-31] Mike Hearn. *Pong message*. Bitcoin Improvement Proposal 31. Created April 11, 2012. URL:

[https : / / github . com / bitcoin / bips / blob / master / bip - 0031 . mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0031.mediawiki) (visited on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-32] Pieter Wuille. *Hierarchical Deterministic Wallets*. Bitcoin Improvement Proposal 32. Created

February 11, 2012. Last updated January 15, 2014. URL: [https://github.com/bitcoin/bips/](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki) [blob/master/bip-0032.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki) (visited on 2016-09-24) (*↑* p[31).](#_bookmark84)

[BIP-34] Gavin Andresen. *Block v2, Height in Coinbase*. Bitcoin Improvement Proposal 34. Created July 6, 2012. URL: <https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki>(visited

on 2016-10-02) (*↑* p[44,](#_bookmark112) [51).](#_bookmark132)

[BIP-35] Jeff Garzik. *mempool message*. Bitcoin Improvement Proposal 35. Created August 16, 2012. URL: [https://github.com /bitcoin/bips/blob/master/bip- 0035.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0035.mediawiki) (visited on

2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-37] Mike Hearn and Matt Corallo. *Connection Bloom filtering*. Bitcoin Improvement Proposal 37. Created October 24, 2012. URL: [https : / / github . com / bitcoin / bips / blob / master / bip -](https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki)

[0037.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki) (visited on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-61] Gavin Andresen. *Reject P2P message*. Bitcoin Improvement Proposal 61. Created June 18, 2014. URL: [https://github.com/bitcoin/bips/blob/master/bip- 0061.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0061.mediawiki) (visited on

2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-62] Pieter Wuille. *Dealing with malleability*. Bitcoin Improvement Proposal 62. Withdrawn Nov- ember 17, 2015. URL: <https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki>

(visited on 2016-09-05) (*↑* p[15).](#_bookmark31)

[BIP-65] Peter Todd. *OP\_CHECKLOCKTIMEVERIFY*. Bitcoin Improvement Proposal 65. Created October 10, 2014. URL: <https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki>(visited

on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-66] Pieter Wuille. *Strict DER signatures*. Bitcoin Improvement Proposal 66. Created January 10,

2015. URL: [https://github .com /bitcoin/bips/blob /master /bip - 0066 .mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0066.mediawiki) (vis- ited on 2016-10-02) (*↑* p[44).](#_bookmark112)

[BIP-68] Mark Friedenbach, BtcDrak, Nicolas Dorier, and kinoshitajona. *Relative lock-time using con- sensus-enforced sequence numbers*. Bitcoin Improvement Proposal 68. Last revised Novem- ber 21, 2015. URL: [https://github.com/bitcoin/bips/blob/master/bip- 0068.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0068.mediawiki)

(visited on 2016-09-02) (*↑* p[35).](#_bookmark95)

[Bitc-Base58] *Base58Check encoding — Bitcoin Wiki*. URL: [https://en.bitcoin.it/wiki/Base58Check\_](https://en.bitcoin.it/wiki/Base58Check_encoding) [encoding](https://en.bitcoin.it/wiki/Base58Check_encoding) (visited on 2016-01-26) (*↑* p[31).](#_bookmark84)

[Bitc-Block] *Block Headers — Bitcoin Developer Reference*. URL: [https://bitcoin.org/en/developer-](https://bitcoin.org/en/developer-reference#block-headers) [reference#block-headers](https://bitcoin.org/en/developer-reference#block-headers) (visited on 2017-04-25) (*↑* p[38).](#_bookmark99)

[Bitc-CoinJoin] *CoinJoin — Bitcoin Wiki*. URL: <https://en.bitcoin.it/wiki/CoinJoin>(visited on 2016-08-17) (*↑* p[6).](#_bookmark6)

[Bitc-Format] *Raw Transaction Format — Bitcoin Developer Reference*. URL: [https : / / bitcoin . org / en /](https://bitcoin.org/en/developer-reference#raw-transaction-format) [developer-reference#raw-transaction-format](https://bitcoin.org/en/developer-reference#raw-transaction-format) (visited on 2016-03-15) (*↑* p[35).](#_bookmark95)

[Bitc-Multisig] *P2SH multisig (definition) — Bitcoin Developer Reference*. URL: [https://bitcoin.org/en /](https://bitcoin.org/en/developer-guide#term-p2sh-multisig) [developer-guide#term-p2sh-multisig](https://bitcoin.org/en/developer-guide#term-p2sh-multisig) (visited on 2016-08-19) (*↑* p[43).](#_bookmark110)

[Bitc-nBits] *Target nBits — Bitcoin Developer Reference*. URL: [https : / / bitcoin . org / en / developer -](https://bitcoin.org/en/developer-reference#target-nbits) [reference#target-nbits](https://bitcoin.org/en/developer-reference#target-nbits) (visited on 2016-08-13) (*↑* p[37,](#_bookmark98) [41).](#_bookmark105)

[Bitc-P2PKH] *P2PKH (definition) – Bitcoin Developer Reference*. URL: [https://bitcoin.org/en/developer-](https://bitcoin.org/en/developer-guide#term-p2pkh) [guide#term-p2pkh](https://bitcoin.org/en/developer-guide#term-p2pkh) (visited on 2016-08-24) (*↑* p[31).](#_bookmark84)

[Bitc-P2SH] *P2SH (definition) — Bitcoin Developer Reference*. URL: [https://bitcoin.org/en/developer-](https://bitcoin.org/en/developer-guide#term-p2sh) [guide#term-p2sh](https://bitcoin.org/en/developer-guide#term-p2sh) (visited on 2016-08-24) (*↑* p[31).](#_bookmark84)

[Bitc-Protocol] *Protocol documentation — Bitcoin Wiki*. URL: [https : / / en . bitcoin . it / wiki / Protocol \_](https://en.bitcoin.it/wiki/Protocol_documentation) [documentation](https://en.bitcoin.it/wiki/Protocol_documentation) (visited on 2016-10-02) (*↑* p[6).](#_bookmark6)

[BK2016] Alex Biryukov and Dmitry Khovratovich. *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem (full version)*. Cryptology ePrint Archive: Report 2015/946. Last revised October 27, 2016. URL: <https://eprint.iacr.org/2015/946>(visited on 2016-10-30)

(*↑* p[7,](#_bookmark9) [38,](#_bookmark99) [51).](#_bookmark132)

[BN2007] Mihir Bellare and Chanathip Namprempre. *Authenticated Encryption: Relations among no- tions and analysis of the generic composition paradigm*. Cryptology ePrint Archive: Report

2000/025. Last revised July 14, 2007. URL: [https : / / eprint . iacr . org / 2000 / 025](https://eprint.iacr.org/2000/025) (visited on 2016-09-02) (*↑* p[13).](#_bookmark25)

[DGKM2011] Dana Dachman-Soled, Rosario Gennaro, Hugo Krawczyk, and Tal Malkin. *Computational Ex- tractors and Pseudorandomness*. Cryptology ePrint Archive: Report 2011/708. December 28,

2011. URL: <https://eprint.iacr.org/2011/708>(visited on 2016-09-02) (*↑* p[48).](#_bookmark125)

[DigiByte-PoW] DigiByte Core Developers. *DigiSpeed 4.0.0 source code, functions GetNextWorkRequiredV3/4 in src/main.cpp as of commit 178e134*. URL: [https://github.com/digibyte/digibyte/blob/](https://github.com/digibyte/digibyte/blob/178e1348a67d9624db328062397fde0de03fe388/src/main.cpp#L1587) [178e1348a67d9624db328062397fde0de03fe388/src/main.cpp#L1587](https://github.com/digibyte/digibyte/blob/178e1348a67d9624db328062397fde0de03fe388/src/main.cpp#L1587) (visited on 2017-01-20)

(*↑* p[40).](#_bookmark102)

[EWD-831] Edsger W. Dijkstra. *Why numbering should start at zero*. Manuscript. August 11, 1982. URL:

<https://www.cs.utexas.edu/users/EWD/transcriptions/EWD08xx/EWD831.html>(visited on 2016-08-09) (*↑* p[7).](#_bookmark9)

[GGM2016] Christina Garman, Matthew Green, and Ian Miers. *Accountable Privacy for Decentralized Anonymous Payments*. Cryptology ePrint Archive: Report 2016/061. Last revised January 24,

2016. URL: <https://eprint.iacr.org/2016/061>(visited on 2016-09-02) (*↑* p[45).](#_bookmark118)

[GitHub-mpc] Sean Bowe, Ariel Gabizon, and Matthew Green. *GitHub repository ‘ zcash/mpc’ : zk-SNARK parameter multi-party computation protocol*. URL: <https://github.com/zcash/mpc>(visited

on 2017-01-06) (*↑* p[33).](#_bookmark91)

[HW2016] Taylor Hornby and Zooko Wilcox. *Fixing Vulnerabilities in the Zcash Protocol*. Zcash blog. April 25, 2016. URL: <https://z.cash/blog/fixing-zcash-vulns.html>(visited on 2016-06-22)

(*↑* p[46).](#_bookmark120)

[IEEE2000] IEEE Computer Society. *IEEE Std 1363-2000: Standard Specifications for Public-Key Cryptog-*

*raphy*. IEEE, August 29, 2000. DOI: [10.1109/IEEESTD.2000.92292](http://dx.doi.org/10.1109/IEEESTD.2000.92292). URL: [http://ieeexplore.](http://ieeexplore.ieee.org/servlet/opac?punumber=7168) [ieee.org/servlet/opac?punumber=7168](http://ieeexplore.ieee.org/servlet/opac?punumber=7168) (visited on 2016-08-03) (*↑* p[29).](#_bookmark78)

[IEEE2004] IEEE Computer Society. *IEEE Std 1363a-2004: Standard Specifications for Public-Key Cryp- tography – Amendment 1: Additional Techniques*. IEEE, September 2, 2004. DOI: [10 . 1109 /](http://dx.doi.org/10.1109/IEEESTD.2004.94612) [IEEESTD.2004.94612](http://dx.doi.org/10.1109/IEEESTD.2004.94612). URL: <http://ieeexplore.ieee.org/servlet/opac?punumber=9276>

(visited on 2016-08-03) (*↑* p[29,](#_bookmark78) [47,](#_bookmark123) [49).](#_bookmark128)

[LG2004] Eddie Lenihan and Carolyn Eve Green. *Meeting the Other Crowd: The Fairy Stories of Hidden Ireland*. TarcherPerigee, February 2004, pages 109–110. ISBN: 1-58542-206-1 (*↑* p[45).](#_bookmark118)

[libsnark-fork] *libsnark: C++ library for zkSNARK proofs (Zcash fork)*. URL: [https : / / github . com / zcash /](https://github.com/zcash/libsnark) [libsnark](https://github.com/zcash/libsnark) (visited on 2016-08-14) (*↑* p[29).](#_bookmark78)

[libsodium-Seal] *Sealed boxes — libsodium*. URL: [https : / / download . libsodium . org / doc / public - key \_](https://download.libsodium.org/doc/public-key_cryptography/sealed_boxes.html) [cryptography/sealed\_boxes.html](https://download.libsodium.org/doc/public-key_cryptography/sealed_boxes.html) (visited on 2016-02-01) (*↑* p[47).](#_bookmark123)

[MAEA2010] V. Gayoso Martínez, F. Hernández Alvarez, L. Hernández Encinas, and C. Sánchez Ávila. “A Com- parison of the Standardized Versions of ECIES”. In: *Proceedings of Sixth International Con- ference on Information Assurance and Security, 23–25 August 2010, Atlanta, GA, USA. ISBN: 978-1-4244-7407-3*. IEEE, 2010, pages 1–4. DOI: [10.1109/ISIAS.2010.5604194](http://dx.doi.org/10.1109/ISIAS.2010.5604194). URL: [https:](https://digital.csic.es/bitstream/10261/32674/1/Gayoso_A%20Comparison%20of%20the%20Standardized%20Versions%20of%20ECIES.pdf)

[//digital.csic.es/bitstream/10261 /32674 /1 /Gayoso \_ A % 20Comparison % 20of% 20the%](https://digital.csic.es/bitstream/10261/32674/1/Gayoso_A%20Comparison%20of%20the%20Standardized%20Versions%20of%20ECIES.pdf) [20Standardized%20Versions%20of%20ECIES.pdf](https://digital.csic.es/bitstream/10261/32674/1/Gayoso_A%20Comparison%20of%20the%20Standardized%20Versions%20of%20ECIES.pdf) (visited on 2016-08-14) (*↑* p[47).](#_bookmark123)

[Naka2008] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. October 31, 2008. URL:

<https://bitcoin.org/en/bitcoin-paper>(visited on 2016-08-14) (*↑* p[5).](#_bookmark2)

[NIST2015] NIST. *FIPS 180-4: Secure Hash Standard (SHS)*. August 2015. DOI: [10.6028/NIST.FIPS.180-4](http://dx.doi.org/10.6028/NIST.FIPS.180-4).

URL: <http://csrc.nist.gov/publications/PubsFIPS.html#180-4>(visited on 2016-08-14) (*↑* p[25,](#_bookmark63) [31).](#_bookmark84)

[PGHR2013] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova. *Pinocchio: Nearly Practical Verifi- able Computation*. Cryptology ePrint Archive: Report 2013/279. Last revised May 13, 2013. URL:

<https://eprint.iacr.org/2013/279>(visited on 2016-08-31) (*↑* p[29).](#_bookmark78)

[RFC-2119] Scott Bradner. *Request for Comments 7693: Key words for use in RFCs to Indicate Requirement*

*Levels*. Internet Engineering Task Force (IETF). March 1997. URL: [https://tools.ietf.org/](https://tools.ietf.org/html/rfc2119) [html/rfc2119](https://tools.ietf.org/html/rfc2119) (visited on 2016-09-14) (*↑* p[5).](#_bookmark2)

[RFC-7539] Yoav Nir and Adam Langley. *Request for Comments 7539: ChaCha20 and Poly1305 for IETF Protocols*. Internet Research Task Force (IRTF). May 2015. URL: [https : / / tools . ietf . org /](https://tools.ietf.org/html/rfc7539) [html/rfc7539](https://tools.ietf.org/html/rfc7539) (visited on 2016-09-02). As modified by verified errata at [https://www.rfc-](https://www.rfc-editor.org/errata_search.php?rfc=7539)

[editor.org/errata\_search.php?rfc=7539](https://www.rfc-editor.org/errata_search.php?rfc=7539) (visited on 2016-09-02). (*↑* p[26,](#_bookmark68) [27).](#_bookmark71)

[RIPEMD160] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. *RIPEMD-160, a strengthened version of RIPEMD*. URL: [http : // homes . esat . kuleuven . be / ~bosselae / ripemd160 . html](http://homes.esat.kuleuven.be/%7Ebosselae/ripemd160.html) (visited on

2016-09-24) (*↑* p[31).](#_bookmark84)

[Unicode] The Unicode Consortium. *The Unicode Standard*. The Unicode Consortium, 2016. URL: [http:](http://www.unicode.org/versions/latest/)

[//www.unicode.org/versions/latest/](http://www.unicode.org/versions/latest/) (visited on 2016-08-31) (*↑* p[30).](#_bookmark81)

[vanS2014] Nicolas van Saberhagen. *CryptoNote v 2.0*. Date disputed. URL: [https :// cryptonote . org /](https://cryptonote.org/whitepaper.pdf) [whitepaper.pdf](https://cryptonote.org/whitepaper.pdf) (visited on 2016-08-17) (*↑* p[6).](#_bookmark6)

[WG2016] Zooko Wilcox and Jack Grigg. *Why Equihash?* Zcash blog. April 15, 2016. URL: [https : / / z .](https://z.cash/blog/why-equihash.html) [cash/blog/why-equihash.html](https://z.cash/blog/why-equihash.html) (visited on 2016-08-05) (*↑* p[38).](#_bookmark99)

[Zave2012] Gregory M. Zaverucha. *Hybrid Encryption in the Multi-User Setting*. Cryptology ePrint Archive:

Report 2012/159. Received March 20, 2012. URL: <https://eprint.iacr.org/2012/159>(visited on 2016-09-24) (*↑* p[48).](#_bookmark125)

[ZcashIssue-2113] Simon Liu. *GitHub repository ‘ zcash/zcash’ : Issue 2113*. URL: [https://github .com /zcash /](https://github.com/zcash/zcash/issues/2113) [zcash/issues/2113](https://github.com/zcash/zcash/issues/2113) (visited on 2017-02-20) (*↑* p[43,](#_bookmark110) [50).](#_bookmark131)