Análisis de Zcash

Trabajo de final de máster - MISTIC

Alumno: David Llop Vila
Supervisor: Jordi Herrera Joancomartí
Junio 2018

Zcash

Zcash es una moneda digital descentralizada basada en Bitcoin

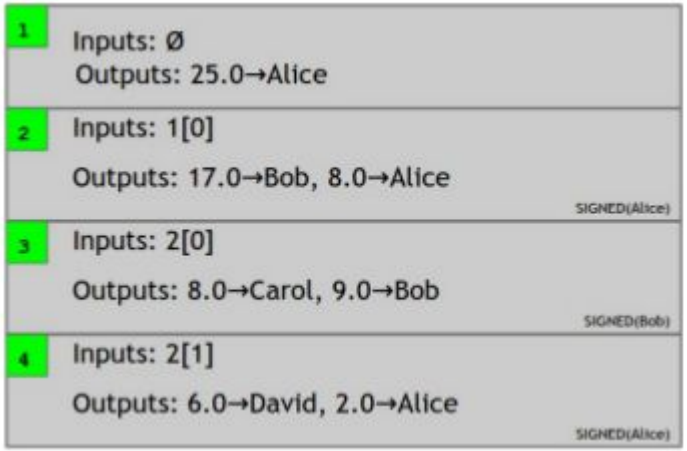
Propuesta de valor: privacidad a través de pruebas de conocimiento nulo

Zerocoin (2013): primera propuesta

Zerocash (2014): propuesta más eficiente y privada

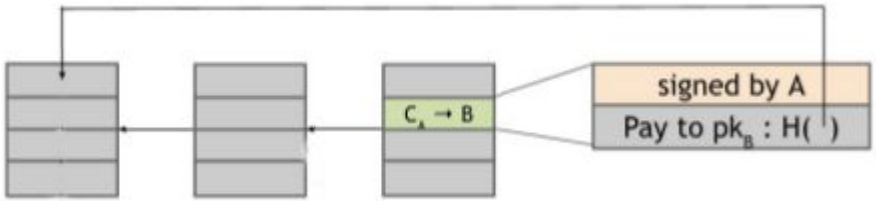
Zcash (2016): primera implementación

Transacciones en Bitcoin



Fuente: Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016

Bloques de la blockchain

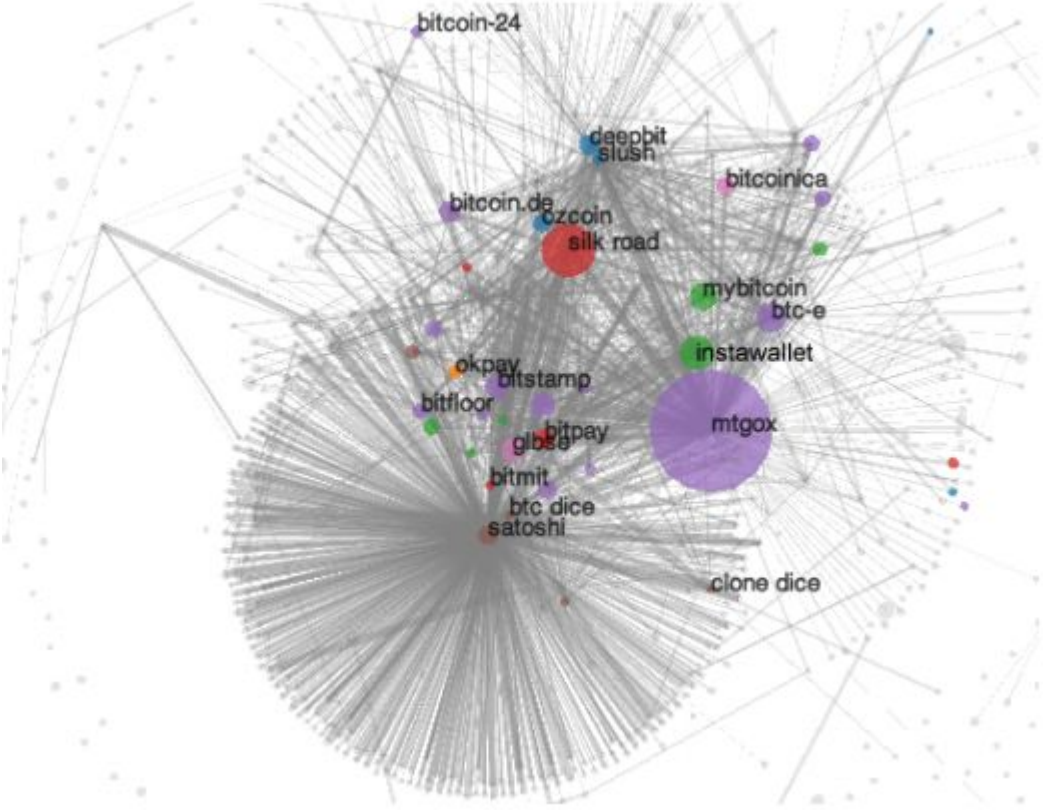


Privacidad en Bitcoin

Las direcciones Bitcoin són pseudónimos.

Las transacciones enlazan entradas y salidas.

Grafos de transacciones desvelan mucha información.



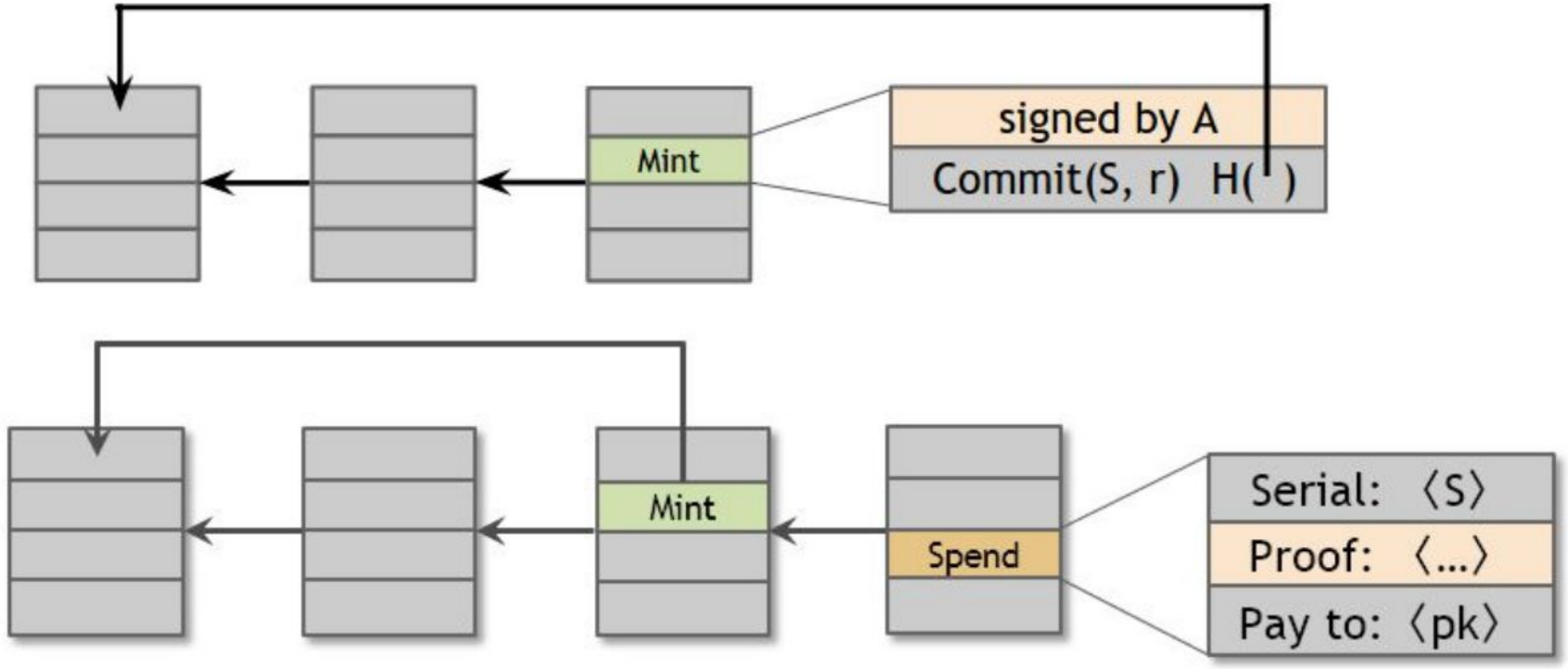
Pruebas de conocimiento nulo

Procedimiento por el cual se puede **probar** que
una **declaración** es cierta,
sin revelar ninguna **información** extra.

Ejemplos:

- Conozco un valor cuyo hash es **d34ca979…**
- Conozco un valor cuyo hash está en el conjunto **{...}**.

Zerocoin



Fuente: Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016

Zerocoin vs. Zerocash/Zcash

	Zerocoin	Zerocash/Zcash
Tamaño de prueba	Crece logarítmicamente	Constante
Valor transferido	Transparente	Blindado
Juntar y separar moneda	Sólo transparente	También blindado
Desplegar en Bitcoin	Se podría (soft-fork)	Necesaria alt-coin

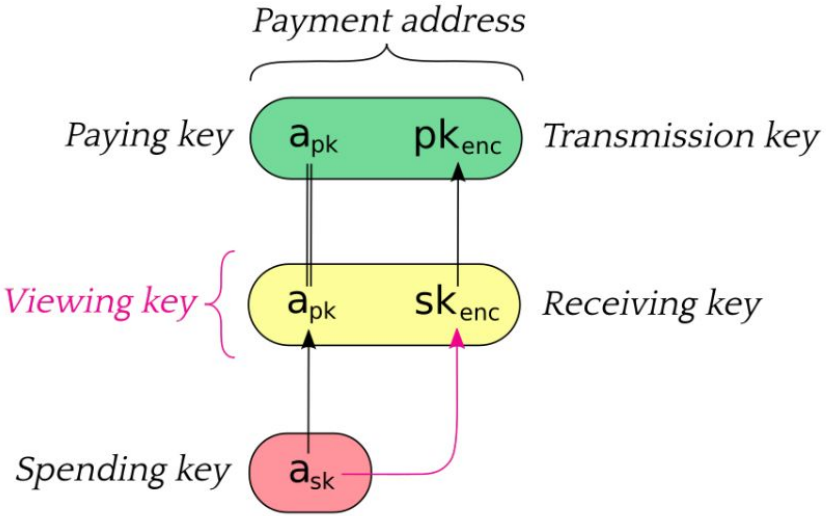
Direcciones de Zcash

Dos tipos de direcciones:

- Transparentes: `t1LhKxV1tjPwfPJM5ym8jmgK2vxvios3Ffa`
- Blindadas: `zcH9dehq4w2WbLUBDHjjzzLD8q9kM5yWCNdjr6oMZqYYUisnMpb9WJBuy8j5RLxpEsEMGFxqCkYjicRCPGZWQjDJWGzyT6e`

Tres tipos de claves:

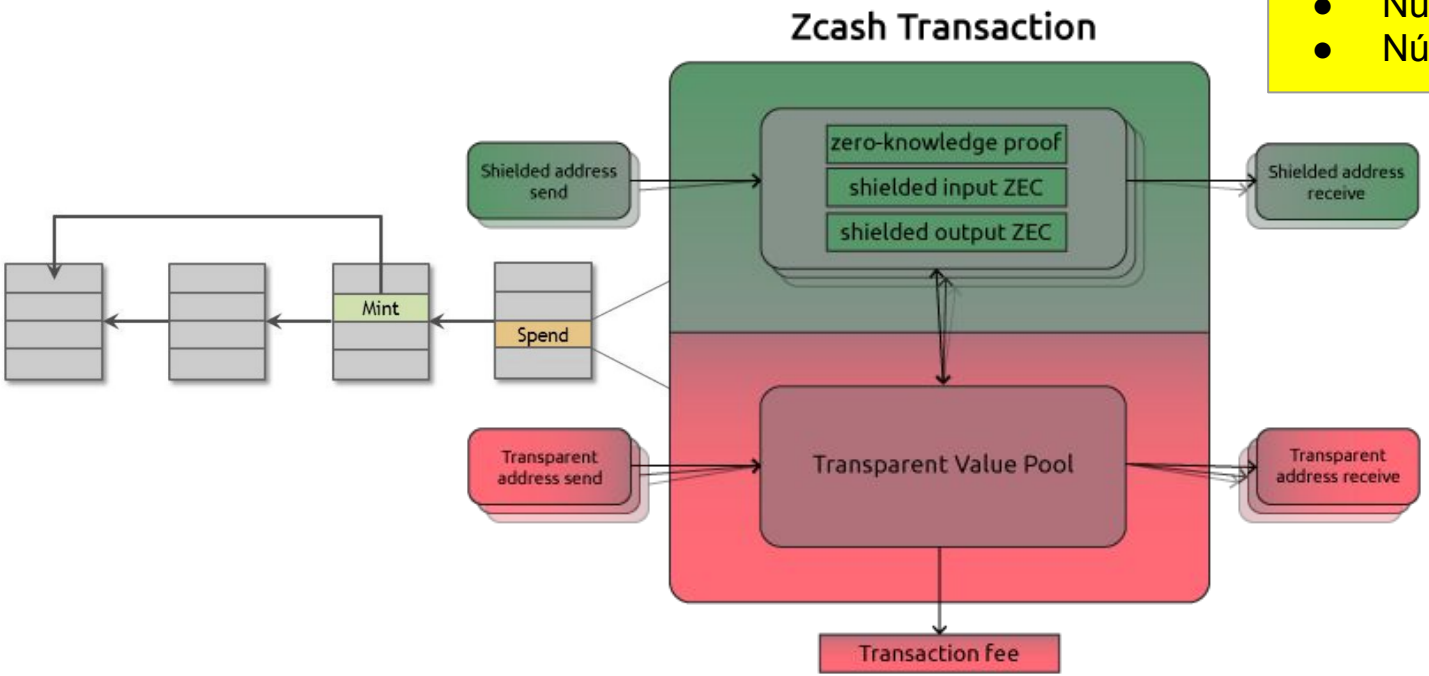
- Pago (pública)
- Visionado (privada)
- Gasto (privada)



Transacciones de Zcash

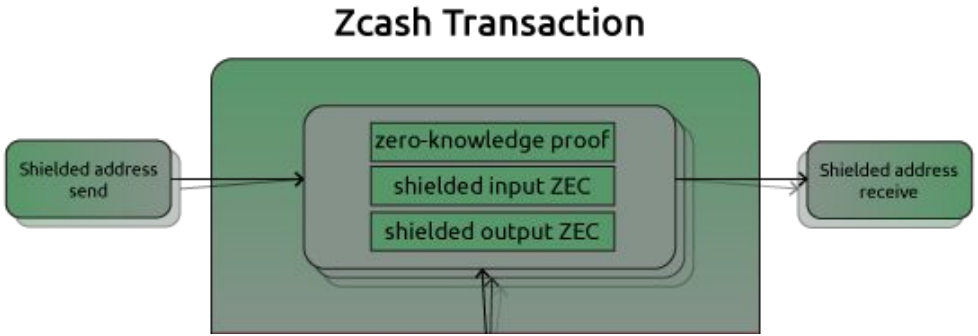
Una “nota” consiste en:

- Clave pública para gastar
- Valor
- Número de serie
- Número aleatorio



Pagos blindados (simplificado)

1. Quema las notas de entrada generando nullifiers
2. Genera notas nuevas (clave pública, valor, número serie, número aleatorio)
3. Cifra el valor, el número de serie y el número aleatorio
4. Genera compromisos para las notas nuevas (hash de los cuatro campos)
5. Genera prueba de conocimiento nulo



zk-SNARKs

zero-**k**nowledge

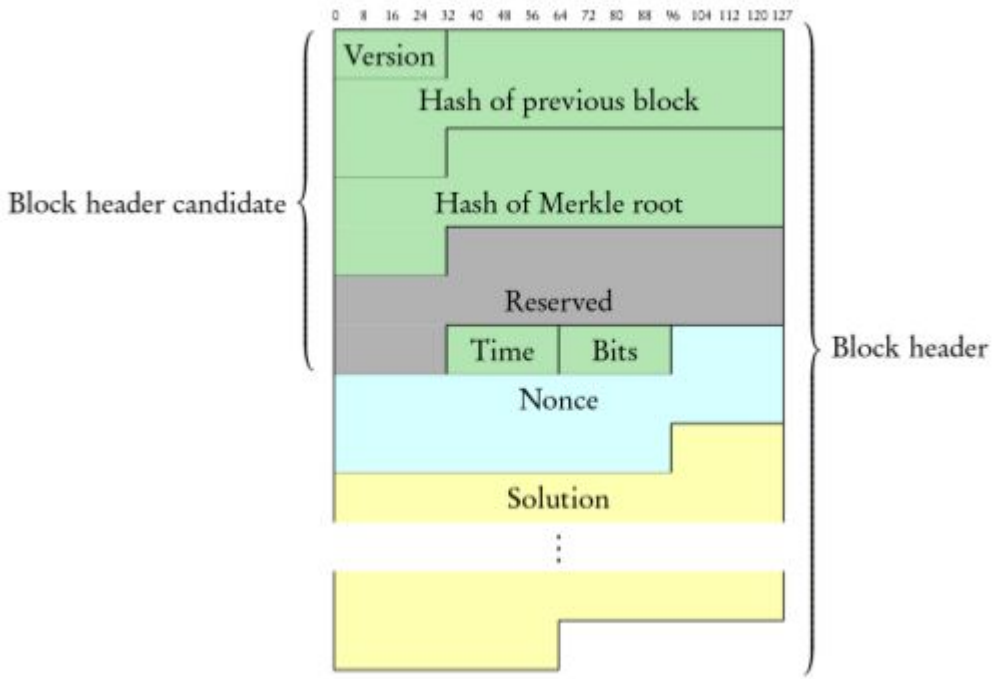
succinct 296 bytes

non-**i**nteractive CRS

argument

of **k**nowledge

Minería en Zcash

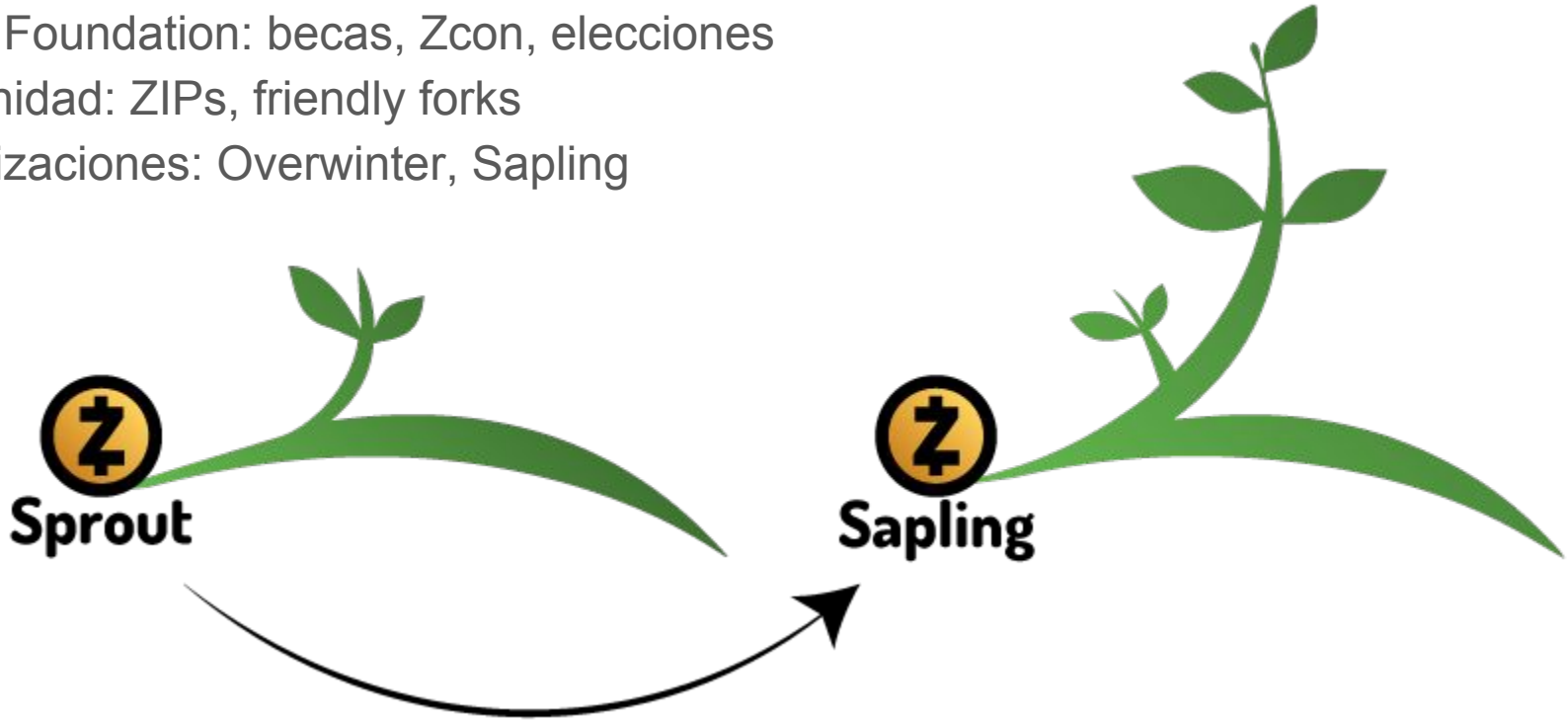


Equihash: bloque válido si:

- Problema cumpleaños generalizado:
  - $H(x1) \oplus H(x2) \oplus H(x3) \oplus ... = 0$
- No armonizaciones
  - Resistencia al Algoritmo de Wagner.
- Filtro de dificultad
  - Mantener el *progress-free*

Comunidad, Consenso, Futuro

- Zcash Company: recompensa de los fundadores
- Zcash Foundation: becas, Zcon, elecciones
- Comunidad: ZIPs, friendly forks
- Actualizaciones: Overwinter, Sapling



Conclusiones

- Zcash soluciona el problema de privacidad en Bitcoin
- La capa de privacidad es opcional
- zk-SNARKs
- Algoritmo de prueba de trabajo
- Futuro prometedor
- Gran interés social y científico

¿Preguntas?