The Zcash Anonymous Cryptocurrency

or zk-SNARKs for the interested layperson

Sven M. Hallberg

29 Dec 2016

33rd Chaos Communication Congress, Hamburg

What is Zcash

- Based on Bitcoin (altcoin)
- Adds a second type of address (tXXXX..., zXXXX...)

→ “Shielded” transactions hide sender, receiver, amount

- Uses recent magic (“zk-SNARKs”: 2010–)

- Evolution of Zerocoin (2013), Zerocash (2014)
- A company, a future (?!) foundation *(I am not affiliated.)*

Miers et al., *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*
Ben-Sasson et al., *Zerocash: Decentralized Anonymous Payments from Bitcoin*

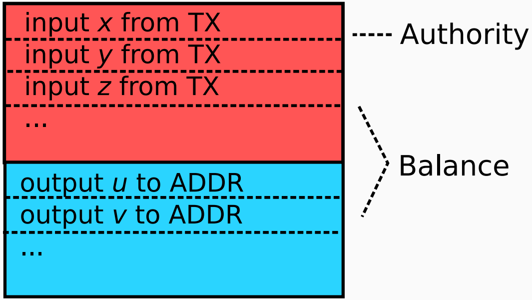
What's in this talk

Focus on Zcash the abstract system

- form of transactions
- what is hidden
- how validity is proved
- where zk-SNARKs come in

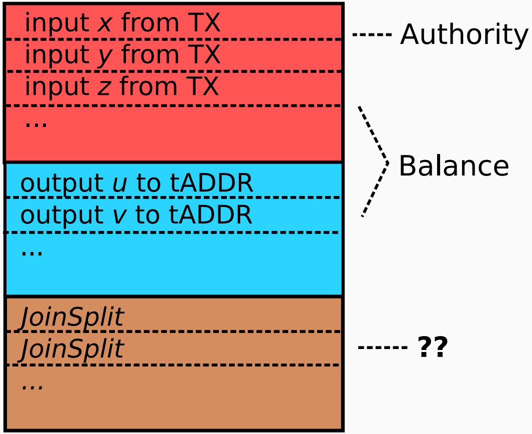
Bitcoin is...

A distributed ledger of consensus-validated transactions.



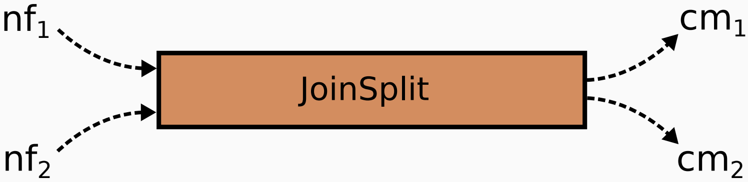
Zcash is...

A distributed ledger of consensus-validated transactions.



JoinSplit

- Zcash is transfered as *notes* (“coins”)
- Note plaintext (owner, value, etc.) is secret
- Each note has a nullifier and a commitment (public)
- JoinSplit consumes (2) and creates (2) notes



JoinSplit description in detail

$$(v_{\text{in}}, v_{\text{out}},\ rt,\ nf_1, nf_2,\ cm_1, cm_2,\ epk, seed, h_1, h_2,\ \pi,\ C_1, C_2,\ )$$

rt commitments in existence

nf_1, nf_2 nullifiers (inputs)

cm_1, cm_2 commitments (outputs)

π proof of validity

JoinSplit description in detail

$$(v_{\text{in}}, v_{\text{out}},\ rt,\ nf_1, nf_2,\ cm_1, cm_2,\ epk, seed, h_1, h_2,\ \pi,\ C_1, C_2,\ )$$

rt commitments in existence

nf_1, nf_2 nullifiers (inputs)

cm_1, cm_2 commitments (outputs)

π proof of validity

→ Prover knows notes such that...

zk-SNARKs (as a black box)

zero-knowledge, succinct, non-interactive arguments of knowledge

"API":

- Setup(*stmt*)
- $\pi \leftarrow$ Prove(*input*)
- Verify(π)

$\rightarrow$ `libsnark`

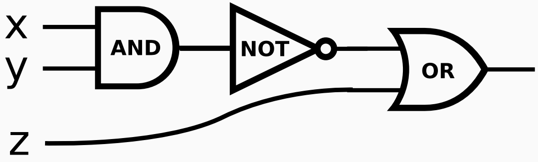
JoinSplit statement

Prover knows notes (a, v, ρ, r) such that...

- Input notes are in rt
- nf_1, nf_2 correspond to input notes
- cm_1, cm_2 correspond to output notes
- Balance
- Spend authority
- Non-malleability
- Uniqueness of ρ

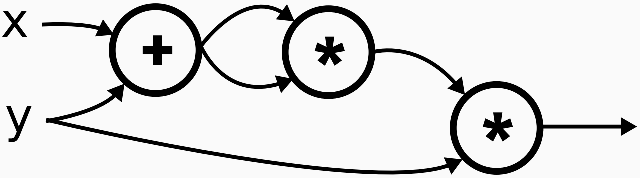
A boolean circuit

$$\neg (x \wedge y) \vee z$$



An arithmetic circuit

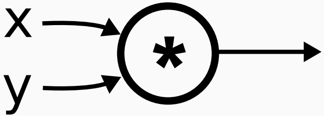
$$(x + y)^2 \cdot y$$



ARITHMETIC AND

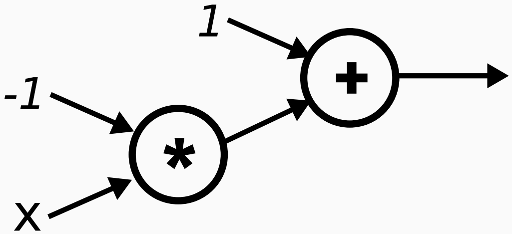
$$x \cdot y$$

$$x, y \in \{0, 1\}$$



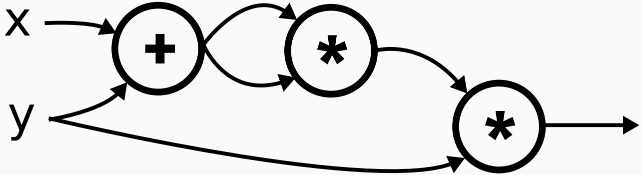
$$1 - x$$

$$x \in \{0, 1\}$$



Assign x, y so that output = 0

$$(x + y)^2 \cdot y$$



$$\begin{aligned} x^2 + y^2 &= z^2 \\ \Leftrightarrow \quad x^2 + y^2 - z^2 &= 0 \end{aligned}$$

Assign x, y, z so that output = 0

Satisfiability of equations

$$
\begin{aligned}
& x^2 + y^2 &= z^2 \\
\Leftrightarrow\quad & x^2 + y^2 - z^2 &= 0
\end{aligned}
$$

Assign x, y, z so that output = 0

zk-SNARKs prove knowledge of x, y, z

Game plan

- Encode JoinSplit statement as arithmetic circuit
- Plug into zk-SNARK
- Prove knowledge of notes such that circuit satisfied

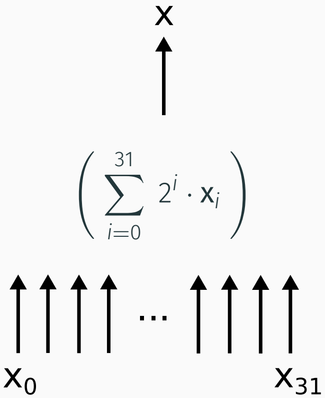
Ingredients of JoinSplit

- Merkle (hash) tree
- Commitment scheme
- Pseudo-random functions
- Arithmetic on $\mathbb{N}$

Ingredients of JoinSplit

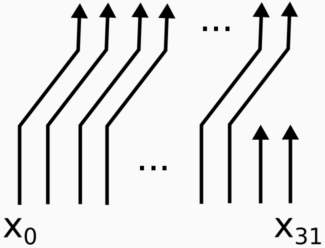
- Merkle (hash) tree (SHA256)
- Commitment scheme (SHA256)
- Pseudo-random functions (SHA256)
- Arithmetic on $\mathbb{N}$

Binary numbers



$$\left(\sum_{i=0}^{31} 2^i \cdot x_i \right)$$

Bit shift



Concrete instantiation (Zerocash)

"Let $\mathcal{H}$ be the SHA256 compression function…"

- $a^{\mathsf{old}}_{\mathsf{pk},i} = \mathcal{H}(a^{\mathsf{old}}_{\mathsf{sk},i} \| 0^{256})$;
- $\mathsf{sn}^{\mathsf{old}}_i = \mathcal{H}(a^{\mathsf{old}}_{\mathsf{sk},i} \| 01 \| [\rho^{\mathsf{old}}_i]_{254})$;
- $\mathsf{cm}^{\mathsf{old}}_i = \mathcal{H}(\mathcal{H}(r^{\mathsf{old}}_i \| [\mathcal{H}(a^{\mathsf{old}}_{\mathsf{pk},i} \| \rho^{\mathsf{old}}_i)]_{128}) \| 0^{192} \| v^{\mathsf{old}}_i)$;
- $\mathsf{cm}^{\mathsf{new}}_i = \mathcal{H}(\mathcal{H}(r^{\mathsf{new}}_i \| [\mathcal{H}(a^{\mathsf{new}}_{\mathsf{pk},i} \| \rho^{\mathsf{new}}_i)]_{128}) \| 0^{192} \| v^{\mathsf{new}}_i)$; and
- $h_i = \mathcal{H}(a^{\mathsf{old}}_{\mathsf{sk},i} \| 10 \| b_i \| [h_{\mathsf{Sig}}]_{253})$ where $b_1 := 0$ and $b_2 := 1$.

$v^{\mathsf{new}}_1 + v^{\mathsf{new}}_2 + v_{\mathsf{pub}} = v^{\mathsf{old}}_1 + v^{\mathsf{old}}_2$, with $v^{\mathsf{old}}_1, v^{\mathsf{old}}_2 \geq 0$ and $v^{\mathsf{old}}_1 + v^{\mathsf{old}}_2 < 2^{64}$

Questions?

zk-SNARKS

Ben-Sasson et al., *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture* (2015)

- arithmetic circuits $\rightarrow$ QAPs
- pairing-pased cryptography
  - $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
- $\mathbb{G}_1, \mathbb{G}_2$ from elliptic curves

More in the literature...

---

https://eprint.iacr.org/2013/879.pdf

State of the currency

- Trusted setup around 22 Oct
- Launch (Genesis Block) on 28 Oct
- CPU and GPU miners available
- Price started overhyped, fluctuated, cur. ∼50 EUR