Monero

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

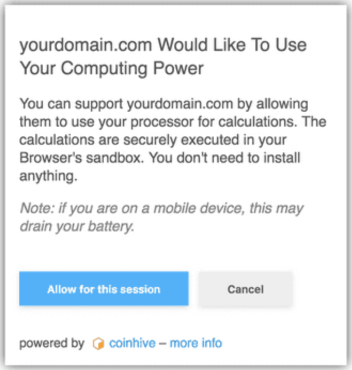
September 9, 2019

Monero

- Privacy-oriented cryptocurrency created in April 2014
- Transaction amounts are hidden
- Transaction inputs and outputs have one-time addresses
- Ring signatures are used to weaken blockchain analysis
- Based on CryptoNote protocol by Nicolas van Saberhagen
    - Initial proposal had amounts in the clear
- Popular for cryptojacking, ransomware, compute-based donations

Cryptojacking

- Hackers use a target's browser to mine Monero
- Coinhive was a cryptocurrency mining service written in JavaScript
  - Hacker embeds the code on website
  - When a user visits the website, her computer starts mining
  - Coinhive gets 30% and hacker gets 70%
- Some websites ask users to allow mining instead of showing ads



Cryptomining Donations

Bitcoin vs Monero

	Bitcoin	**Monero**
Specification	Bitcoin Core client	Monero Core client
Consensus	SHA256 PoW	CryptoNight PoW
Network Hashrate[1]	82 Exahashes/s	345 Megahashes/s
Contract Language	Script	None
Block interval	10 minutes	2 minutes
Block size limit	approx 4 MB	Maximum of 600 KB and twice the median of last 100 blocks
Difficulty adjustment	After 2016 blocks	Every block
Block reward adjustment	After 210,000 blocks	Every block
Current block reward	12.5 BTC per block	3.4 XMR (variable)
Currency units	1 BTC = 10^8 satoshi	1 XMR = 10^{12} piconero

[1] `https://bitinfocharts.com/comparison/monero-hashrate.html`

Transactions using One-Time Addresses

- Each user has two private-public key pairs from an elliptic curve group with base point G and cardinality L
- Let Bob's private keys be (a, b) with public keys (A, B) given by (aG, bG)
- Suppose Alice wants to send a payment to Bob
  1. Alice generates a random $r \in \mathbb{Z}_L^*$ and computes a one-time public key $P = H_s(rA)G + B$
  2. Alice specifies P as destination address and $R = rG$ in transaction output
  3. Bob reads every transaction and computes $P' = H_s(aR)G + B$
  4. If $P' = P$, the Bob knows the private key $x = H_s(aR) + b$ such that $P = xG$
  5. Bob can spend the coins in the one-time address P using x
- The pair (a, B) is called the tracking key
- Tracking key can be safely shared with third parties

Ring Signatures

- Traditional digital signatures prove knowledge of a private key
- Ring signatures prove signer knows 1 out of n private keys
- Consider an elliptic curve group E with cardinality L and base point G
- Let $x_i \in \mathbb{Z}_L^*, i = 0, 1, \ldots, n-1$ be private keys with public keys $P_i = x_i G$
- Suppose a signer knows only x_j and not any of x_i for $i \neq j$
- For a given message m, the signer generates the ring signature as follows:
  1. Signer picks $\alpha, s_i, i \neq j$ randomly from $\mathbb{Z}_L$
  2. Signer computes $L_j = \alpha G$ and $c_{j+1} = H_s(m, L_j)$
  3. Increasing j modulo n, signer computes

$$\begin{aligned} L_{j+1} &= s_{j+1} G + c_{j+1} P_{j+1} \\ c_{j+2} &= H_s(m, L_{j+1}) \\ &\vdots \\ L_{j-1} &= s_{j-1} G + c_{j-1} P_{j-1} \\ c_j &= H_s(m, L_{j-1}) \end{aligned}$$

  4. Signer computes $s_j = \alpha - c_j x_j$ which implies $L_j = s_j G + c_j P_j$
  5. The ring signature is $\sigma = (c_0, s_0, s_1, \ldots, s_{n-1})$
- Verifier computes L_j, remaining c_j's, and checks that $H_s(m, L_{n-1}) = c_0$

Confidential Transactions

- In this context, CT refers to hidden transaction amounts
- But miners need to verify sum of input amounts exceeds sum of output amounts
- Pedersen Commitments
  - Let a denote an amount we want to hide
  - Let G be the base point of an elliptic curve E with cardinality L
  - Let H be a generator of E such that $\log_G H$ is unknown
  - The Pedersen commitment to amount a with blinding factor $x \in \mathbb{Z}_L$ is

$$C(a, x) = xG + aH$$

  - **Hiding:** If x is chosen uniformly from $\mathbb{Z}_L$, then C reveal nothing about a
  - **Binding:** If $\log_G H$ is unknown, C cannot be revealed to be a commitment to some $a' \neq a$
  - **Homomorphic:** $C(a_1, x_1) + C(a_2, x_2) = C(a_1 + a_2, x_1 + x_2)$
- Suppose we have one input and two outputs
  - Let $C(p, x_p)$ be the commitment to input amount p
  - Let $C(q, x_q)$ and $C(r, x_r)$ be commitments to output amounts q and r such that $x_p = x_q + x_r$
  - Let the fees amount be f
  - Miners check that

$$C(p, x_p) = C(q, x_q) + C(r, x_r) + fH$$

Range Proofs

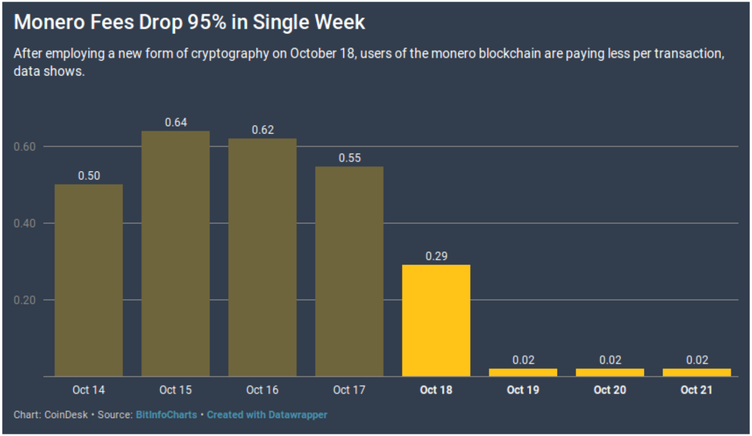
- In an elliptic curve with cardinality L, $C(a, x) = C(a + L, x)$
- Can allow adversary to spend non-existent coins
- L is typically of the order of 2^{256}
- Need proof that committed amount lies in a range, say $\{0, 1, \ldots, 2^{32} - 1\}$
- Range proof using ring signatures
  - Let $a = \sum_{i=0}^{31} a_i 2^i$ where each a_i is either 0 or 1
  - Let $C_i = C(a_i 2^i, x_i) = x_i G + a_i 2^i H$
  - If we consider $\{C_i, C_i - 2^i H\}$ as a pair of public keys, we know exactly one of the corresponding private keys
  - A ring signature for each i proves that either C_i or $C_i - 2^i H$ is a commitment to 0
  - By picking blinding factors such that $x = \sum_{i=0}^{31} x_i$, we have

$$C(a, x) = \sum_{i=0}^{31} C_i = \sum_{i=0}^{31} C(a_i 2^i, x_i)$$

- Range proofs dominated the size of the transaction until Bulletproofs came along

Bulletproofs

- Range proofs with logarithmic scaling based on discrete logarithm assumption
- Proposed in 2017 and implemented in Monero in October 2018



References

- Monero Wikipedia page
  https://en.wikipedia.org/wiki/Monero_(cryptocurrency)
- UNICEF cryptomining donation https://www.thehopepage.org/
- Monero website https://getmonero.org/
- CryptoNote Protocol https://bytecoin.org/old/whitepaper.pdf
- Monero's Building Blocks by Bassam El Khoury Seguias (10 articles)
  https://delfr.com/category/monero/
- A first look at browser-based cryptojacking
  https://arxiv.org/abs/1803.02887
- Monero block explorers https://xmrchain.net/,
  https://moneroblocks.info/
- Github repository https://github.com/monero-project/monero
- CryptoNight Hash Function https://cryptonote.org/cns/cns008.txt
- Confidential transactions writeup, Greg Maxwell
  https://people.xiph.org/~greg/confidential_values.txt
- An investigation into confidential transactions, Adam Gibson
  https://github.com/AdamISZ/ConfidentialTransactionsDoc
- Bulletproofs https://crypto.stanford.edu/bulletproofs/
- Bulletproofs in Monero https://www.coindesk.com/
  monero-fees-fall-to-almost-zero-after-bulletproofs-upgrade