Introduction to Monero and how it’s different

Mario Canul & Saxon Knight

University of Hawai’i at Manoa

Some terminology

- Input - An amount of currency being sent
- Output - An amount of currency being received
- Transaction - A set of inputs and outputs
- Block - A set of transactions occurring around the same time
- Blockchain - A historical timeline of blocks linked together (database of transactions)
- Miner - Computer(s) that compete to process a block into the blockchain for a reward
- Fungibility - The ability to interchange two assets with their own individual units (identical worth regardless of origin or history, in this case)

Bitcoin

Basic concepts

Bitcoin

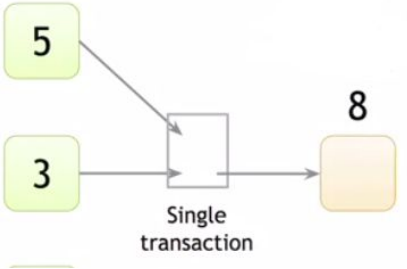
What’s wrong with Bitcoin?

Issue 1: Traceability

Bitcoins can be traced

- All transactions between network participants are public.
- Any transaction can be unambiguously linked to a source and destination.
- Indirect transactions (tumbling) between two parties can still be found through path-finding algorithms.
- Shared spending can be used as evidence for a joint control of source addresses.
- Creating a new address every time will create clusters.

Image credit:
Arvind Narayanan,
Princeton University



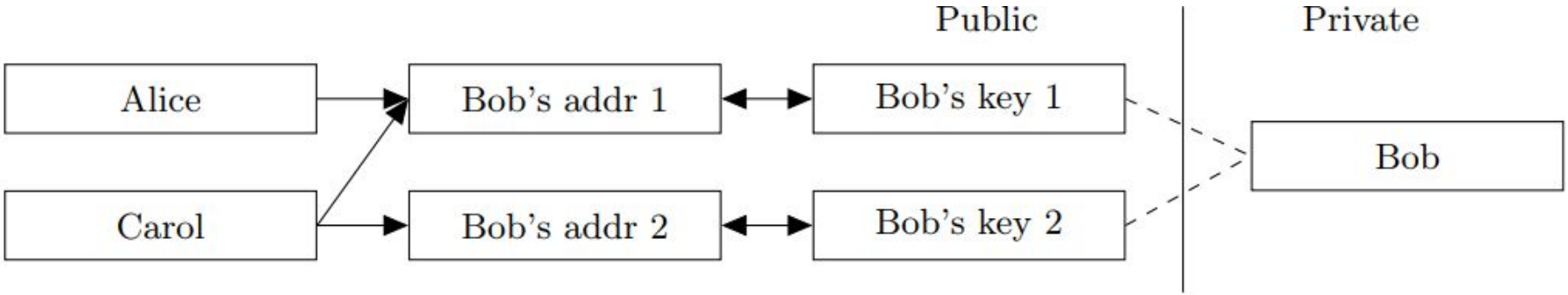


Fig. 2. Traditional Bitcoin keys/transactions model.

Image credit: Nicolas van Saberhagen, CryptoNight v2.0

Implications

- The permanent nature of the blockchain only decreases privacy the more transactions a participant makes.

- Bitcoins may not be fungible
  - All bitcoins initially share the same worth, but...
  - Bitcoins obtained from addresses found to be committing crimes may not be accepted by future buyers, essentially “freezing” them

Issue 2: Linkability

Bitcoins may be linkable

- The property of linkability is that for any two outgoing transactions to different addresses, it may be possible to prove they were sent to the same network participant.
- Although this property has been debated, researchers proposed ways of linking participants on the Bitcoin network through blockchain analysis.
- Blockchain analysis is an open area of research, akin to Open Source Intelligence (OSINT)
- It is suspected that a lot of potentially identifiable information can be found through this type of analysis.

Distributed Online Payment Vulnerability

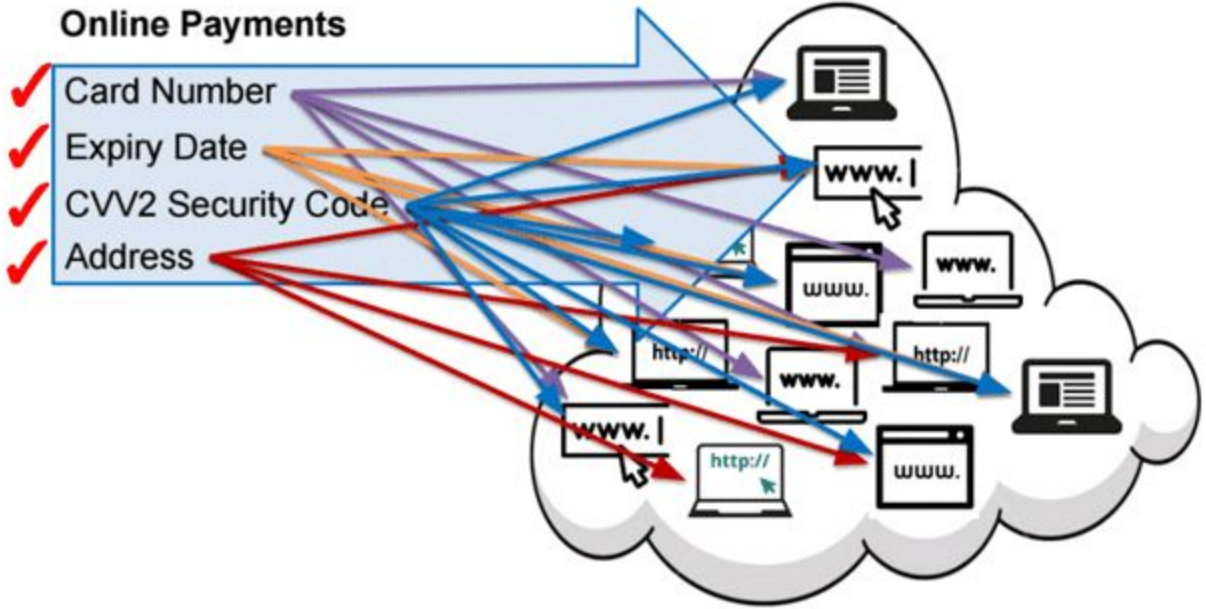


Image credit: Akash Kandpal, http://harrypotter.tech

Implications

- Participants could be linked together, opening privacy issues
- Purchase patterns may be found of a participant if the addresses they send the money to are well known.

Issue 3: Proof-of-Work

Proof-of-work algorithm

- The proof of work algorithm is the underlying cryptographic engine of Bitcoin
- The proof of work algorithm is how Bitcoins are minted through the use of a computer's processing power.
- The proof of work algorithm may be used as a voting system for transactions, new features, or anything that would require network-wide consensus
- The original Bitcoin developer(s) intended to use a "one-CPU-one-vote" scheme
- This creates a discrepancy of voting power as GPUs have vastly more processing power than CPUs
- The discrepancy is a classic example of the Pareto Principle, as 20% of the network controls 80% of the voting power.

Implications

- The CPU-GPU discrepancy in voting power creates a gap in the democratic nature of the network consensus.
- This can enable a small number of participants to control the network consensus and make decisions that may go against the majority of participants.
- A mining majority can freeze arbitrary wallets indefinitely by blacklisting their addresses.

Bulky scripting system

- Bitcoin was created with a scripting system for sophisticated transactions
- Many features are disabled for security purposes or unused
- 164 bytes long just to check that the recipient has their secret key
- This increases the overall size of the blockchain

```
<sig> <pubKey> OP DUP OP HASH160 <pubKeyHash> OP EQUALVERIFY OP CHECKSIG.
```

Issue 4: Emission rate

Emission rate

- Bitcoin’s emission rate is how many Bitcoins are awarded to a miner for a successful block.
- The emission rate is set to halve every 4 years.
- This creates a scenario where the law of diminishing returns forces small miners to stop mining as it becomes less profitable to do so.
- The result is a decrease in the network’s total processing power (known as *hash rate*)

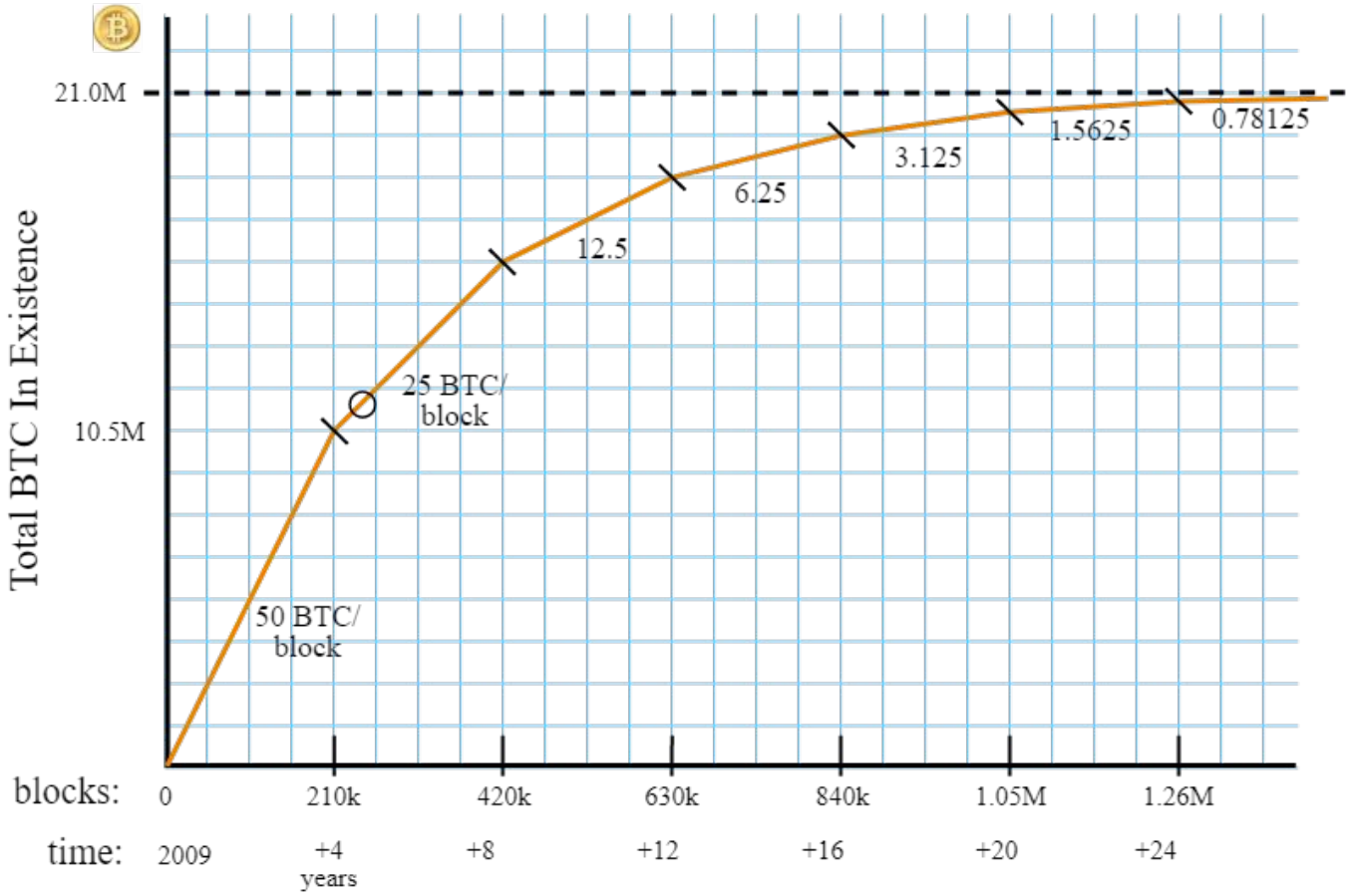


Image Credit: Brian Warner, Mozilla Labs

Implications

- The abrupt change in mining reward may cause sudden negative changes in network processing power.
    - Less miners means transactions fees increase
    - There have been certain documented attacks against the Bitcoin network when there is a sharp decline in network processing power

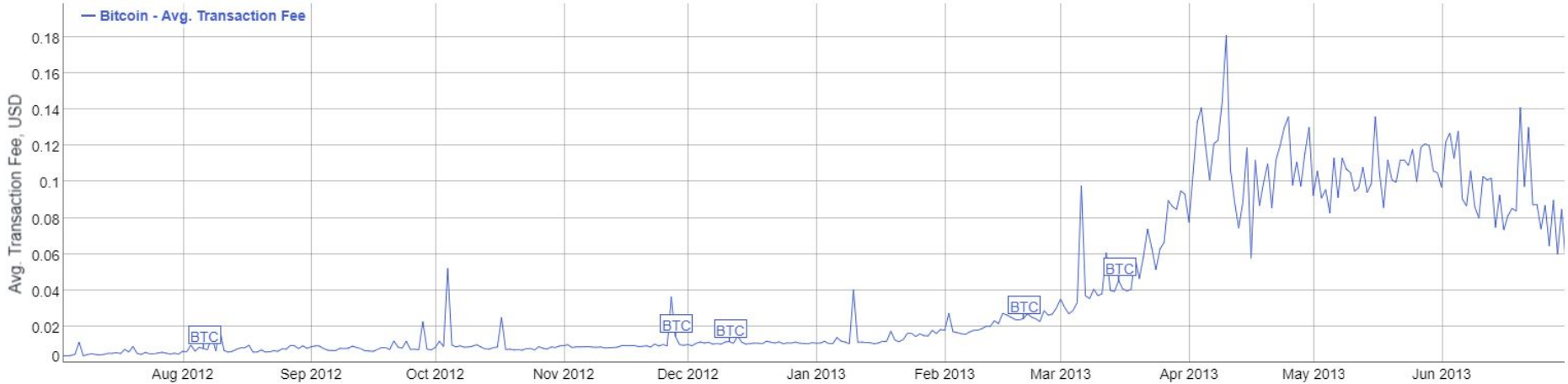
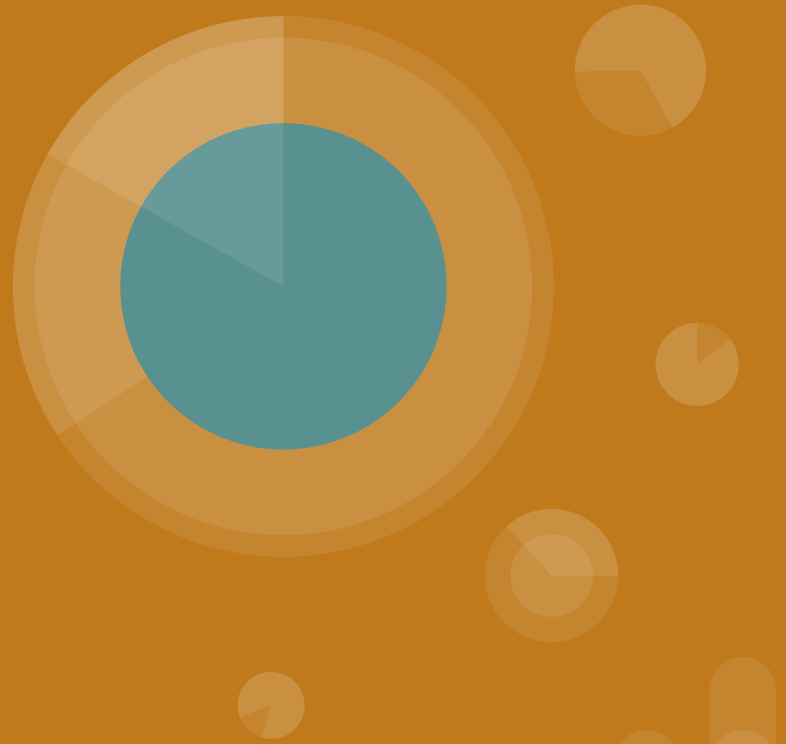


Image credit: https://bitinfocharts.com

Monero

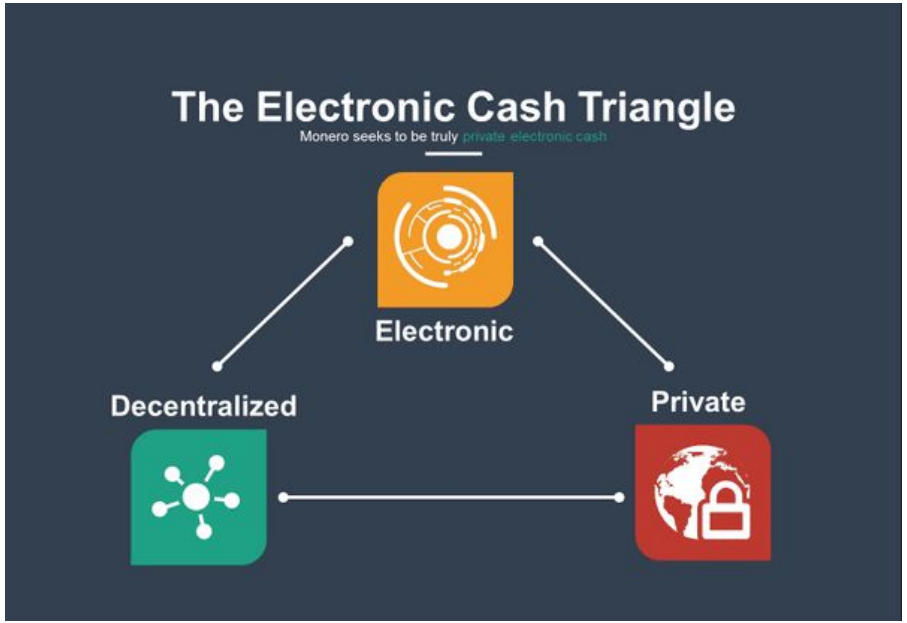
MONERO



The core concepts

Properties of Monero

- Decentralized
- Private
- Electronic



The centerpiece of Monero: Privacy

- Monero keeps the identity of the sender private through ring signatures
- Monero keeps the identity of the receiver private through Confidential Addresses
  - A “stealth” address is created by the use of two keys (public send and public view)
- Monero keeps the privacy of the transaction through Ring Confidential Transactions

Mitigating traceability

Ring signatures

- Ring signatures aim to fix the following problems:
  - The sender of a transaction does not want let anyone know that they sent any Monero.
  - The receiver of a transaction also does not want to let anyone know that they've received Monero.
- Ring signatures mix the funds (input) of the sender with other decoy funds from other senders.
  - Ring Confidential Transactions (RingCT) enable the transaction to mix funds of other senders without knowing the amount of the funds.
  - Ring signatures guarantee that the transactions are valid without knowing the amounts.

Anatomy of Ring signatures

A ring signature is composed of the following pieces:

- Inputs
  - A real input and decoy inputs.
- Key image
  - The blockchain can verify that the ring signature is valid and that it isn't a duplicate transaction
  - One-way reference to the real input, so even the sender can't tell their own transaction apart from the decoys
- Pedersen commitment
  - This tells the network that the sum of inputs is equal to the sum of outputs without revealing the amounts, showing the transaction is legitimate

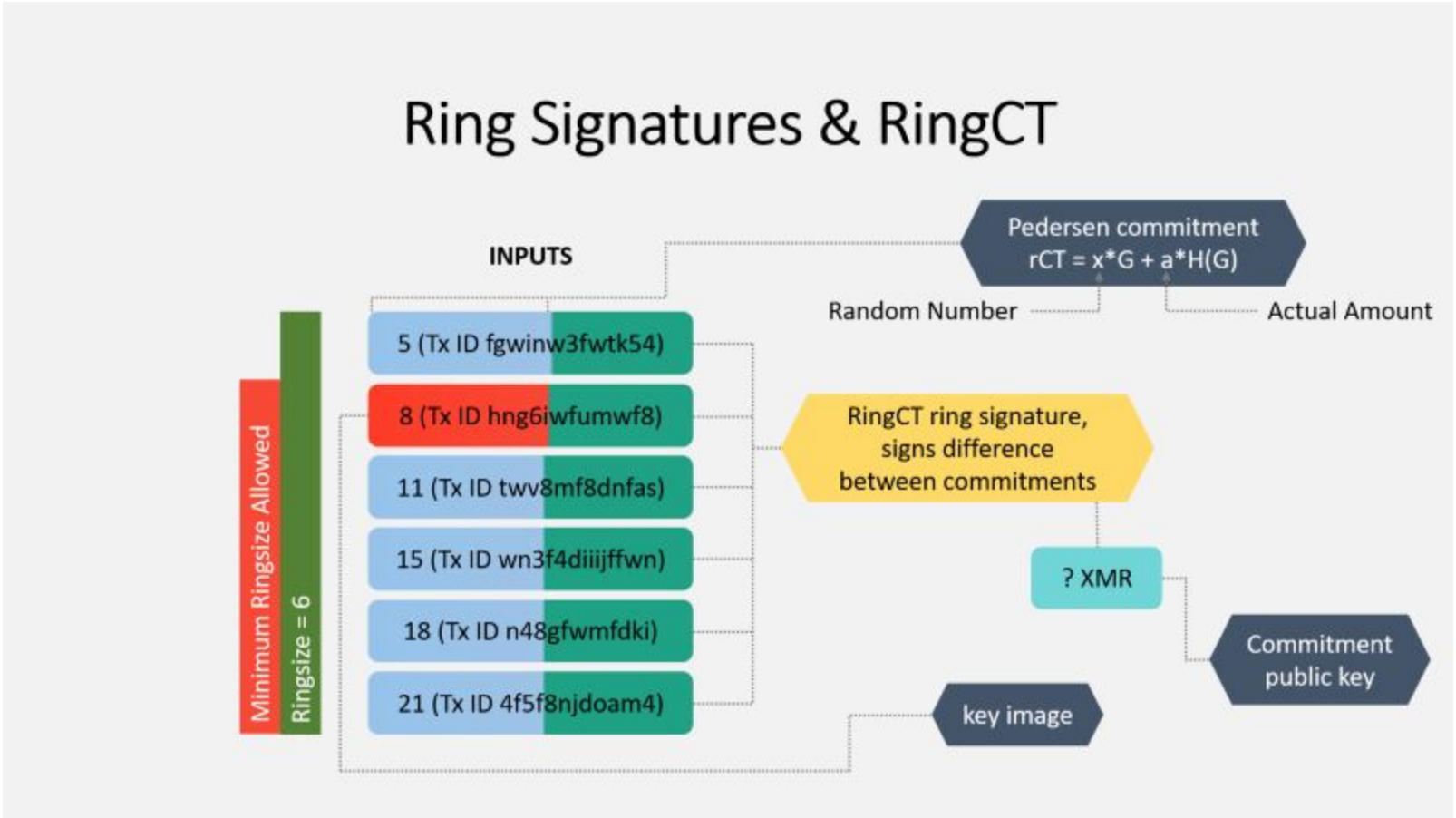


Image credit: Akash Kandpal, http://harrypotter.tech

Accomplishments

- No one in the network can tell who sent or received what.
  - Bitcoin has a public record of the sender’s address, the amount and the recipient's address.

- Monero inputs sent cannot be tracked, and therefore retains full fungibility. The input cannot be denied by other participants based on the input’s spending history.
  - Unlike Bitcoin, where an address can be flagged and funds coming from it may be scrutinized. (e.g. hacker Bitcoin wallets, etc.)

Mitigating linkability

Stealth addresses

- In Monero, the funds are not linked to a particular public address.
- Participants still use public keys, but they are only used by the sender to create one-time addresses.
- The receiver can unlock the funds sent to these one-time addresses using a secret key which only the receiver knows.
- Monero wallets continuously scan the Monero blockchain for any transactions which may be destined to them.

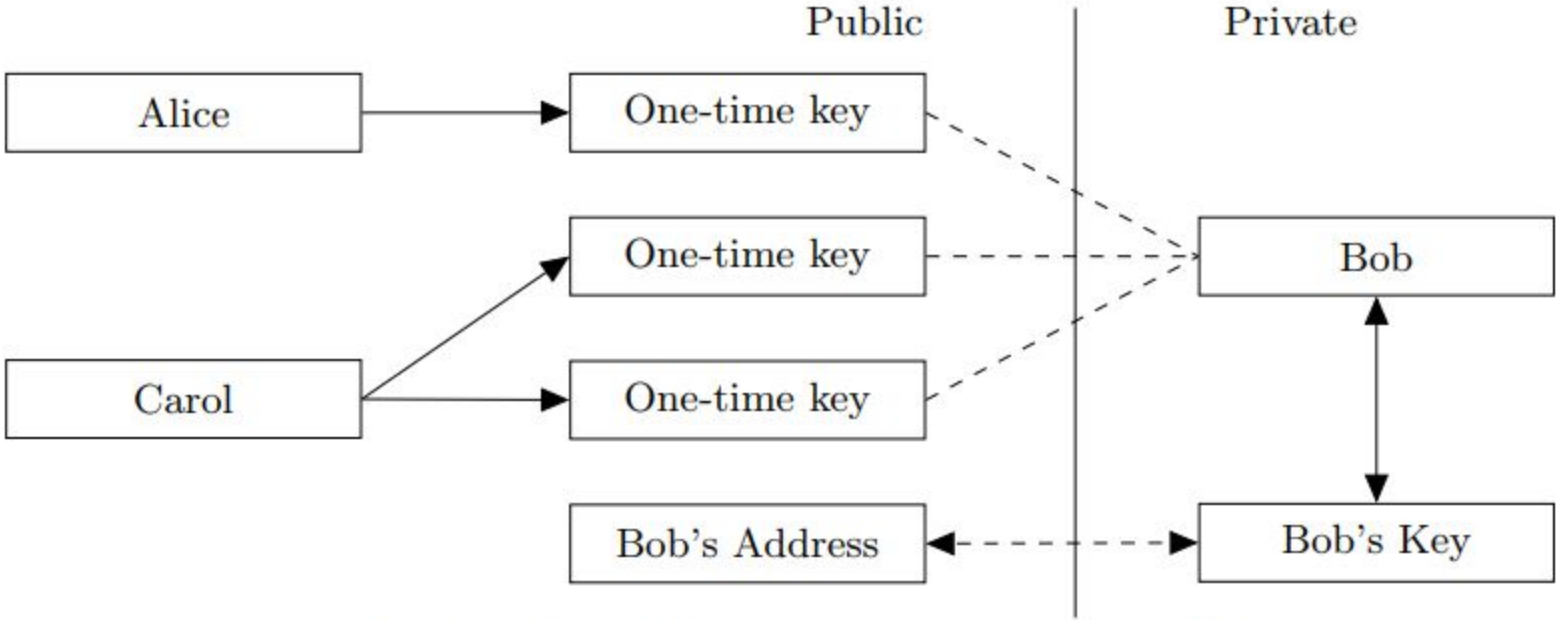


Fig. 3. CryptoNote keys/transactions model.

Image credit: Nicolas van Saberhagen, CryptoNote v2.0

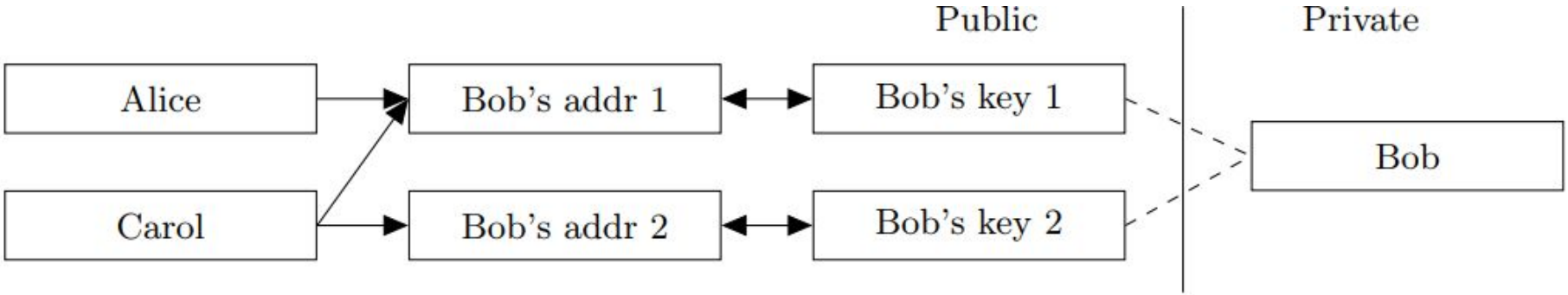


Fig. 2. Traditional Bitcoin keys/transactions model.

Image credit: Nicolas van Saberhagen, CryptoNight v2.0

Accomplishments

- This setup enables the transaction to occur between two wallets without linking them together.
- The sender and receiver are kept anonymous and the amount is kept anonymous.

Monero’s proof-of-work

Egalitarian proof-of-work

- The proof-of-work algorithm used by Monero aims to create a linear relationship between input mined with processing power.

- Miners with low processing power are not forced to stop mining from a sudden loss in profitability, as the difficulty changes slowly.

Bitcoin’s network processing power (all-time)

Image credit: http://blockchain.info

Monero’s network processing power (all time)

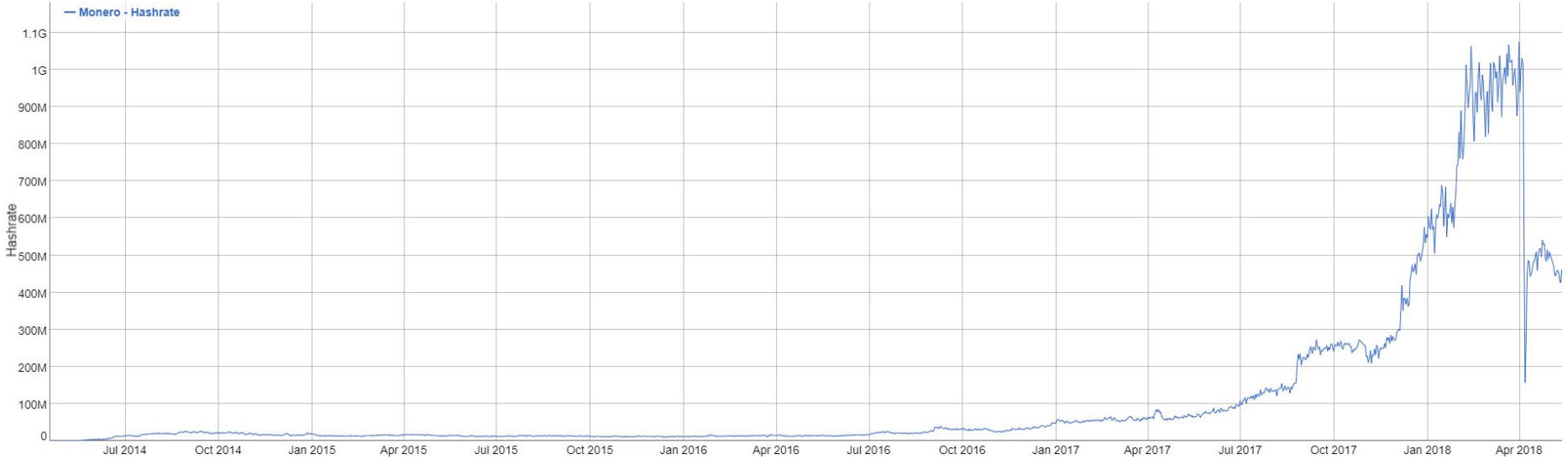


Image credit: https://bitinfocharts.com

Smoothing Emission Rate

Monero’s emission rate

Monero’s emission rate is based on CryptoNote’s design.
From the CryptoNote whitepaper:

6.1 Smooth emission

The upper bound for the overall amount of CryptoNote digital coins is: $\texttt{MSupply} = 2^{64} - 1$ atomic units. This is a natural restriction based only on implementation limits, not on intuition such as “N coins ought to be enough for anybody”.

To ensure the smoothness of the emission process we use the following formula for block rewards:

$$BaseReward = (\texttt{MSupply} - A) \gg 18,$$

where A is amount of previously generated coins.

Creating a transaction

A simple overview of how a transaction works

1. Sender gets a public address from the receiver.
2. Sender sends their input to a one-time randomly generated address.
3. Sender can then create a Ring Confidential Transaction by mixing their input with inputs from other users to form a group of decoy inputs with a real input.
4. If the RingCT created has a valid key image and Pedersen Commitment, miners can then process the transaction.
5. Once processed, the RingCT is now on the Monero blockchain.
6. The receiver scans the Monero blockchain using their private view key and finds the transactions destined for them.

Future improvements

Future improvements: Kovri

- Monero's implementation creates an environment of private transactions, but this does not mean that identity cannot be leaked.
  - An attacker may still be able to find out the source of a transaction with an IP address
- The network source of the transaction can be obfuscated through an anonymizing router called Kovri.
  - Kovri works similarly to Tor in that it uses I2P (Invisible Internet Project) nodes to obfuscate traffic
  - Kovri can be trivially implemented onto Monero and any other cryptocurrency
- Even without Kovri, an attacker who knows the source IP for a ring signature does not know who sent it within the ring.

Questions?

Thank you!