CS 798: Digital Forensics and Incident Response

Lecture 17 - Cryptocurrencies

Diogo Barradas

Winter 2025

University of Waterloo

Financial transactions

- **Physical cash**
  - Untraceable and secure (mostly)
  - Cannot be used for online transactions
- **Credit cards and debit transactions**
  - Banks see transactions
  - Vendors can track and profile customers
  - The dominant online payment methods

Outline

1. Online transactions

2. Bitcoin

   What it is and how it works

   Investigations focused on Bitcoin

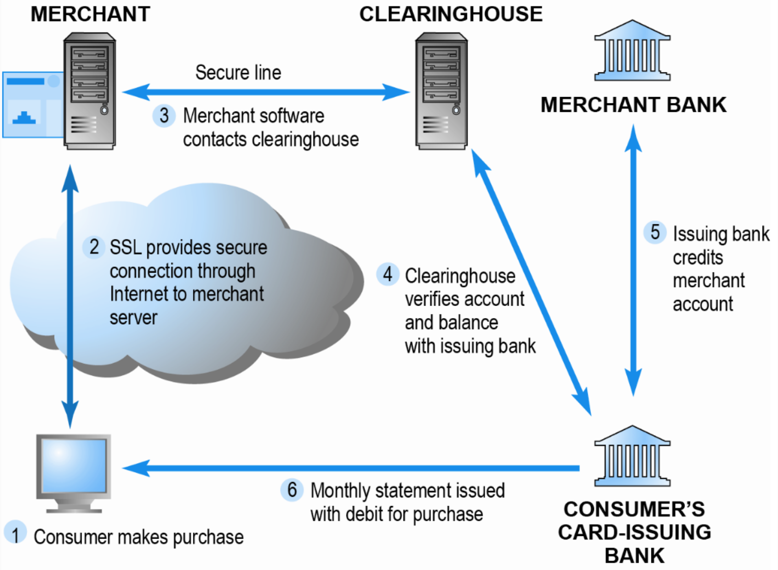
3. Traceless cryptocurrencies

   Zerocoin and Zerocash

   Monero

Online transactions

How does an online credit transaction work?



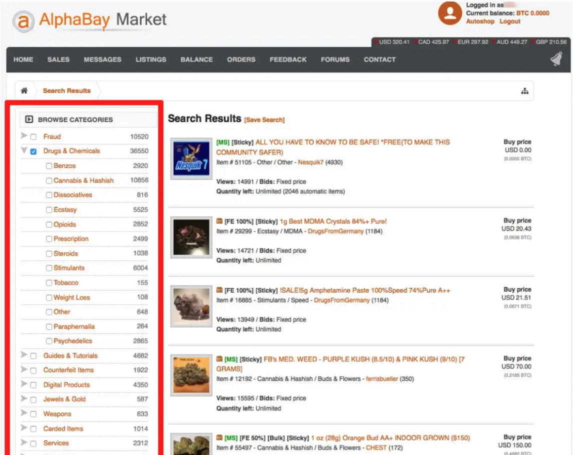
MERCHANT
CLEARINGHOUSE
MERCHANT BANK
Secure line
3 Merchant software contacts clearinghouse
2 SSL provides secure connection through Internet to merchant server
4 Clearinghouse verifies account and balance with issuing bank
5 Issuing bank credits merchant account
6 Monthly statement issued with debit for purchase
1 Consumer makes purchase
CONSUMER'S CARD-ISSUING BANK

Alternative online payment systems

- **Online stored value systems**
  - Based on value stored in a consumer's bank account
  - e.g., PayPal, Amazon Payments
- **Virtual currencies**
  - Circulate within a virtual world
  - e.g., Linden Dollars in Second Life, Facebook Credits
- **E-cash / Cryptocurrencies**
  - Based on algorithms that generate unique tokens that can be used in the "real" world
  - e.g., Bitcoin, Ethereum

Cryptocurrencies and cybercrime

- Cryptocurrencies are the payment method of choice
  - e.g., markets like Silk Road, AlphaBay, Hansa, etc.
  - Often used for exchanges involving drugs, weapons, pornography, hacker hiring...



AlphaBay Market
Logged in as [redacted]
Current balance: BTC 0.0000
Autoshop Logout
USD 320.41 CAD 425.97 EUR 297.92 AUD 449.27 GBP 210.56
HOME SALES MESSAGES LISTINGS BALANCE ORDERS FEEDBACK FORUMS CONTACT
Search Results
BROWSE CATEGORIES

□ Fraud	10520
☑ Drugs & Chemicals	36550
□ Benzos	2920
□ Cannabis & Hashish	10856
□ Dissociatives	816
□ Ecstasy	5525
□ Opioids	2852
□ Prescription	2499
□ Steroids	1038
□ Stimulants	6004
□ Tobacco	155
□ Weight Loss	108
□ Other	648
□ Paraphernalia	264
□ Psychedelics	2865
□ Guides & Tutorials	4682
□ Counterfeit Items	1922
□ Digital Products	4350
□ Jewels & Gold	587
□ Weapons	633
□ Carded Items	1014
□ Services	2312

Search Results [Save Search]

[MS] [Sticky] ALL YOU HAVE TO KNOW TO BE SAFE! *FREE(TO MAKE THIS COMMUNITY SAFER)
Item # 51105 - Other / Other - Nesquik7 (4930)
Views: 14991 / Bids: Fixed price
Quantity left: Unlimited (2046 automatic items)
Buy price USD 0.00 (0.0000 BTC)

[FE 100%] [Sticky] 1g Best MDMA Crystals 84%+ Pure!
Item # 29299 - Ecstasy / MDMA - DrugsFromGermany (1184)
Views: 14721 / Bids: Fixed price
Quantity left: Unlimited
Buy price USD 20.43 (0.0638 BTC)

[FE 100%] [Sticky] !SALE!5g Amphetamine Paste 100%Speed 74%Pure A++
Item # 16885 - Stimulants / Speed - DrugsFromGermany (1184)
Views: 13949 / Bids: Fixed price
Quantity left: Unlimited
Buy price USD 21.51 (0.0671 BTC)

[MS] [Sticky] FB's MED. WEED - PURPLE KUSH (8.5/10) & PINK KUSH (9/10) [7 GRAMS]
Item # 12192 - Cannabis & Hashish / Buds & Flowers - ferrisbueller (350)
Views: 15595 / Bids: Fixed price
Quantity left: Unlimited
Buy price USD 70.00 (0.2185 BTC)

[MS] [FE 50%] [Bulk] [Sticky] 1 oz (28g) Orange Bud AA+ INDOOR GROWN ($150)
Item # 55497 - Cannabis & Hashish / Buds & Flowers - CHEST (172)
Buy price USD 150.00 (0.4682 BTC)

Why are cryptocurrencies used by criminals?

- **Fully decentralized**
  - No need to rely on a bank to mediate the transaction
- **Privacy-preserving**
  - Transactions based on pseudonyms
- **Secure**
  - Single-use
  - Reliable

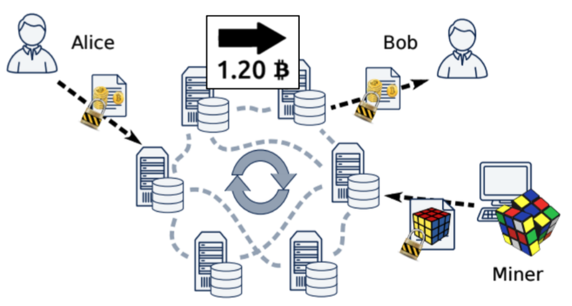
Bitcoin

Bitcoin

What it is and how it works

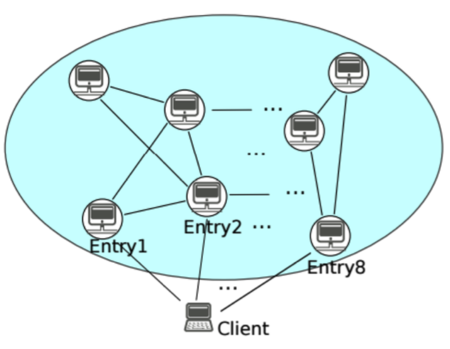
What is Bitcoin?

- A decentralized digital currency (S. Nakamoto, 2008)
  - Effectively a bank run by an ad-hoc network
  - Provides a distributed transaction log
- **Decentralization**
  - Peers of the Bitcoin network re-broadcast valid transactions received from clients
- **Pseudonymity**
  - Clients are identified by public keys of their choice



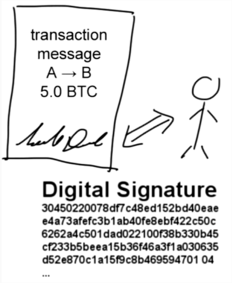
Bitcoin P2P network

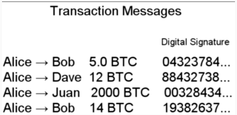
- Peers of the Bitcoin network connect to each other over an unencrypted TCP channel
  - There is no authentication in the network, so each node just keeps a list of IP addresses associated with its connections
  - Bitcoin peers try to maintain 8 outgoing connections



Bitcoin transactions

- Every account address has an associated public key pair for signing transactions
- Public keys also identify the receivers' addresses
    - There is no authentication in the network, so each node keeps a list of IP addresses tied with its connections
    - Bitcoin peers (clients and servers) try to maintain 8 outgoing connections


transaction
message
A → B
5.0 BTC
Digital Signature
30450220078df7c48ed152bd40eae
e4a73afefc3b1ab40fe8ebf422c50c
6262a4c501dad022100f38b330b45
cf233b5beea15b36f46a3f1a030635
d52e870c1a15f9c8b469594701 04
...

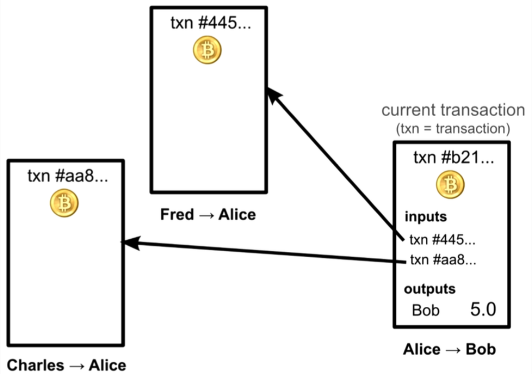


Transaction Messages

		Digital Signature
Alice → Bob	5.0 BTC	04323784...
Alice → Dave	12 BTC	88432738...
Alice → Juan	2000 BTC	00328434...
Alice → Bob	14 BTC	19382637...

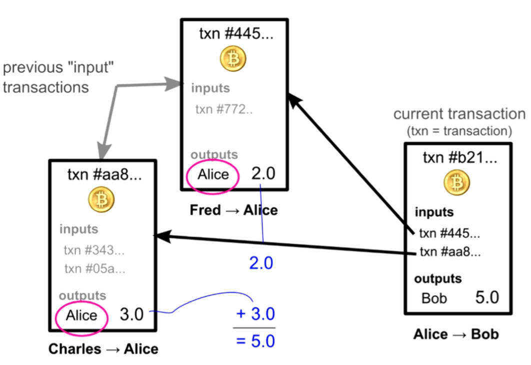
Transaction graph

- Current transactions reference previous txs (called inputs)
  - To send 5.0 BTC to Bob (output), Alice must reference past txs where she received 5 or more BTCs



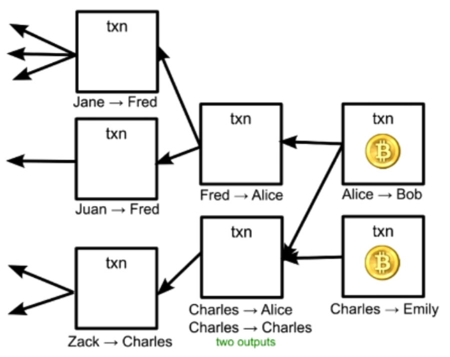
Transaction graph

- Other nodes verifying this transaction will check those inputs
  - Ensure Alice was the recipient, and that the inputs add up to 5+ Bitcoins



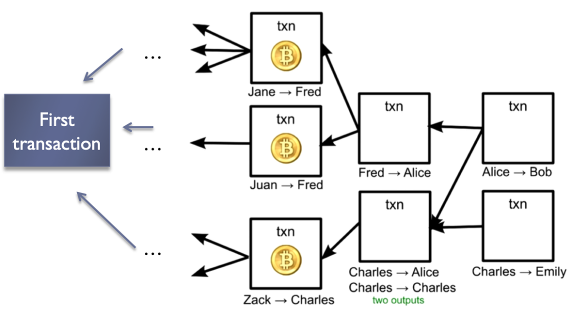
The tx graph keeps the whole tx history

- Ownership of Bitcoins is exchanged via input links
  - Transactions' validity is dependent on previous transactions
- For each tx, added outputs must equal added inputs
  - If you are sending an amount that exceeds your inputs, you must send the remaining amount back to yourself (i.e., get change)



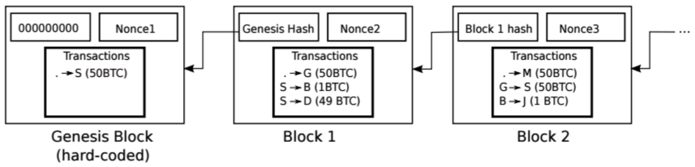
For tx validation, must check until the first tx

- Must check the entire chain to the first tx ever made
  - Wallet software downloads and checks every transaction ever made at install time
  - This can take a considerable amount of time, but needs to be done once



Blockchain to secure the tx graph

- Transaction history is organized as a **blockchain**
- **Miners** are:
  - responsible for generating and appending new blocks to the head of the blockchain
  - rewarded if they succeed at appending a new block into the blockchain

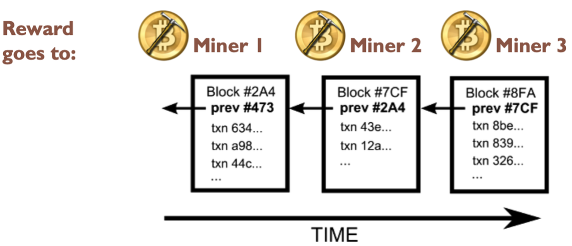


Mining

- **Mining** is the process through which new bitcoin are added to the money supply
  - Mining also serves to secure the bitcoin system against fraudulent transactions or transactions spending the same amount of bitcoin more than once, known as a **double-spend**
- Miners provide processing power to the bitcoin network in exchange for the opportunity to be rewarded bitcoin

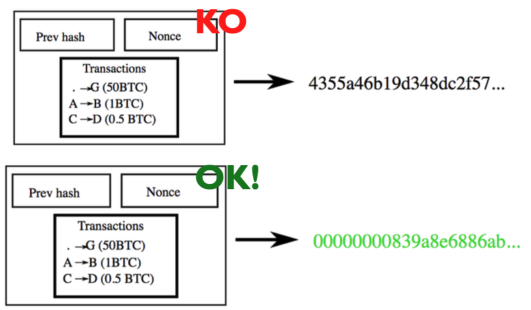
Security through proof-of-work

- Generating a block entails solving a difficult math problem based on a cryptographic hash algorithm
  - Miners compete to solve the problem, and get a reward if they manage to solve it first
  - The solution to the problem (Proof-of-Work) is included in the block and acts as a proof that the miner solved the problem
- Miners provide processing power to the bitcoin network in exchange for the opportunity to be rewarded bitcoin



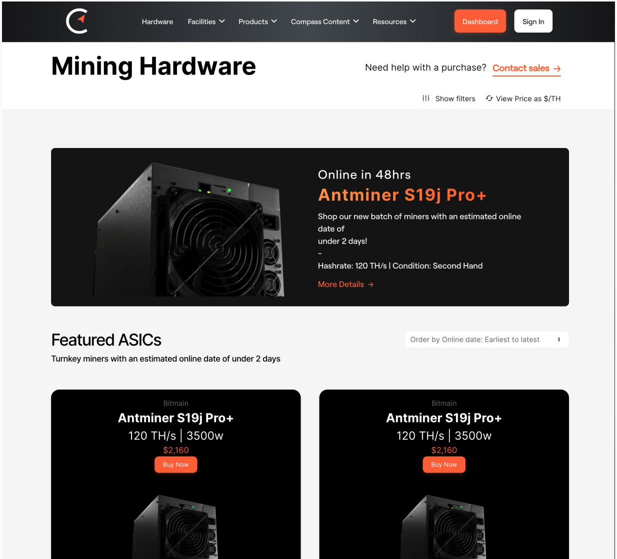
Block generation example

- **Proof-of-work**: Test nonces and compute a hash until you have a given number of leading zero-bits (controls the difficulty)
  - If solution is found, broadcast it to the entire network
  - The longest blockchain is considered the "correct" one
  - Double spending is prevented because only one blockchain is valid



Hardware for bitcoin mining

- Specialized hardware (or GPUs) are required to mine bitcoin



Mining Hardware

Need help with a purchase? Contact sales →

Online in 48hrs

Antminer S19j Pro+

Shop our new batch of miners with an estimated online date of under 2 days!

-

Hashrate: 120 TH/s | Condition: Second Hand

Featured ASICs

Turnkey miners with an estimated online date of under 2 days

Bitmain
Antminer S19j Pro+
120 TH/s | 3500w
$2,160

Bitmain
Antminer S19j Pro+
120 TH/s | 3500w
$2,160

Bitcoin

Investigations focused on Bitcoin

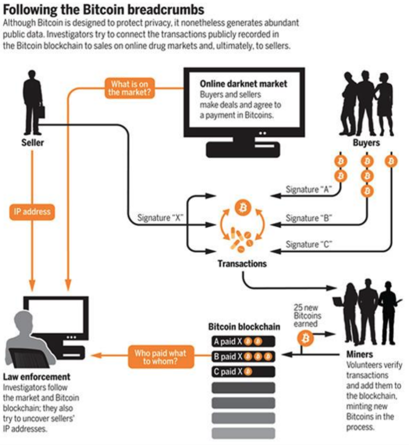
Trail obfuscation techniques in Bitcoin

- Bitcoin address are not mapped to the real user identity
- Bitcoin transactions do not contain personal information
- IP address of a client is not included in new transactions
- User can generate as many Bitcoin addresses as needed

This looks pretty good, right? How can we find criminals?

Is Bitcoin anonymous?

- Names are not associated with transactions
- But the metadata of transactions is recorded and publically accessible to anyone
- Address of both wallets, amount transferred, (and more) are recorded for each transaction in the blockchain



Following the Bitcoin breadcrumbs

Although Bitcoin is designed to protect privacy, it nonetheless generates abundant public data. Investigators try to connect the transactions publicly recorded in the Bitcoin blockchain to sales on online drug markets and, ultimately, to sellers.

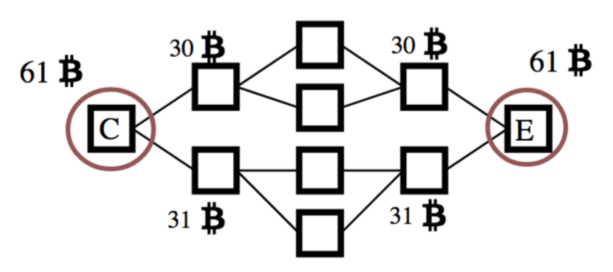
Seller
What is on the market?
Online darknet market
Buyers and sellers make deals and agree to a payment in Bitcoins.
Buyers
IP address
Signature "A"
Signature "X"
Signature "B"
Signature "C"
Transactions
25 new Bitcoins earned
Bitcoin blockchain
A paid X
B paid X
C paid X
Who paid what to whom?
Law enforcement
Investigators follow the market and Bitcoin blockchain; they also try to uncover sellers' IP addresses.
Miners
Volunteers verify transactions and add them to the blockchain, minting new Bitcoins in the process.

Drawbacks of Bitcoin's trail obfuscation

- Authentication mechanisms in Bitcoin exchanges may link user IPs to Bitcoin addresses
- The chain of transactions is transparent and traceable
- Bitcoin address exposed on the Internet reveal all transactions related to its owner
- Gathering some or all inputs when sending Bitcoins to others may expose other addresses of the sender

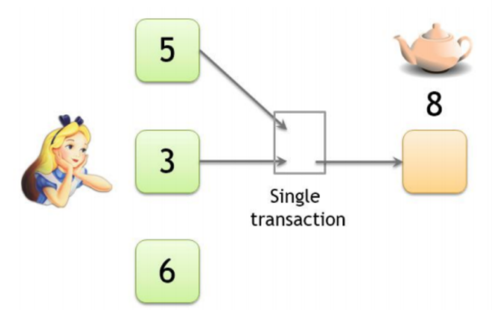
Analysis of the transaction graph

- Some deanonymization techniques are based on analyzing the graphs of transactions in the blockchain
    - Help link different bitcoin addresses
    - Can use several heuristics



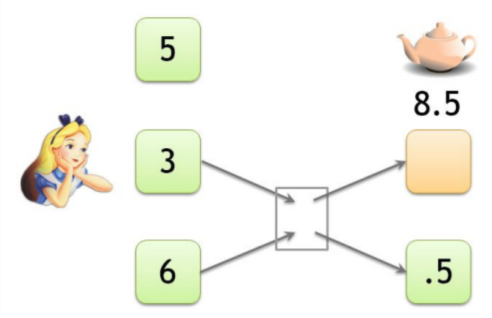
Shared-spending heuristic

- Shared spending is evidence of joint control of the different input addresses
  - Two inputs to the transaction are most likely under the control of the same user
  - This process can be repeated and transitively link an entire cluster of transactions



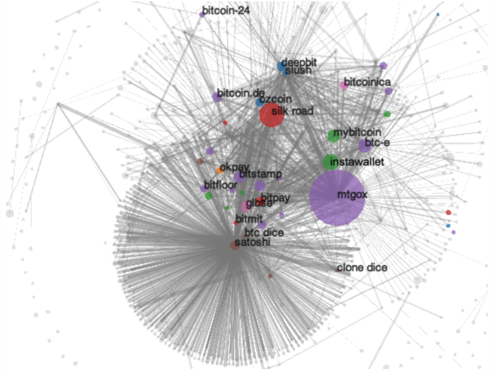
Fresh-change-address heuristic

- Wallet software typically generates a fresh address whenever a "change" address is required
  - Change addresses generally have never before appeared
  - Non-change outputs may have appeared in the blockchain



Clustering of addresses

- In 2013, researchers combined the shared-spending and the fresh-change-address heuristics to cluster Bitcoin addresses



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Meiklejohn et al. IMC'13

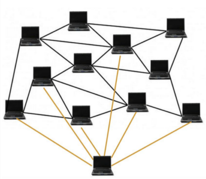
Identifying individuals

- How can we connect little clusters corresponding to individuals to their real-life identities?
- **Direct transacting**
  - Reveals at least at least one address belonging to an individual
- **Bad opsec**
  - People often post their Bitcoin addresses in public forums
- **Evolution of deanonymization algorithms**
  - Usually improve over time when the data is publicly available

Analysis of the Bitcoin protocol and network

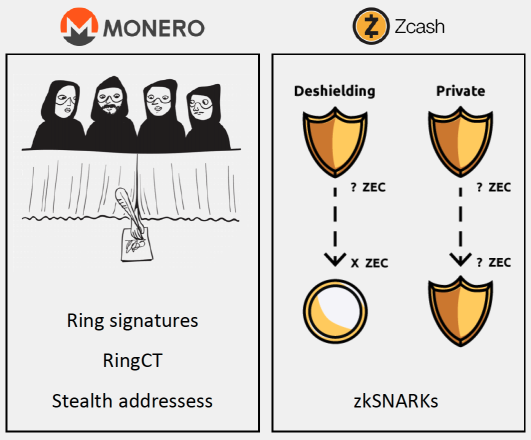
- To post a transaction to the blockchain, one typically broadcasts it to Bitcoin's P2P network. This allows for:
- **Collusion**
  - If sufficient nodes collude with each other, they could figure out the first node to broadcast any transaction

- **Bitcoin protocol sniffing**
  - Since Bitcoin's protocol data is not encrypted, we could obtain the relationship between Bitcoin address - IP address, and get the real identity with the help of the telecom operator's IP records
- **Sybil attack**
  - Fill the network with nodes controlled by the investigator; users would likely connect only to those nodes



Traceless cryptocurrencies

Privacy-preserving cryptocurrencies



Ring signatures

RingCT

Stealth addressess

zkSNARKs

A very brief introduction

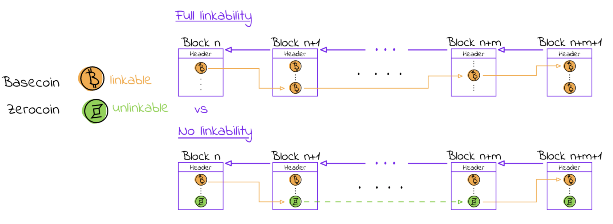
Traceless cryptocurrencies

Zerocoin and Zerocash

What is Zerocoin?

- A distributed approach to private electronic cash
- Extends Bitcoin by adding an anonymous currency on top of it

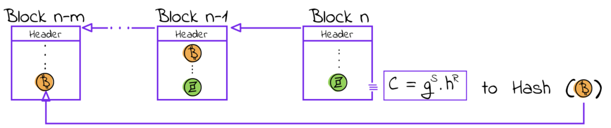
- A **zerocoin** is:
  - A promissory note which is redeemable for a Bitcoin
  - A "closed envelope" containing a serial number



Transaction linkability of a Basecoin(BTC) vs. Zerocoin

Managing Zerocoins

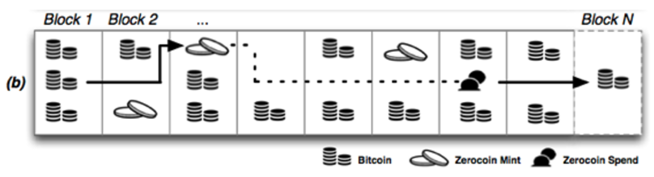
- All starts with a **commitment**:
  - Allow you to commit to and later reveal a value
  - **Binding**: value cannot be tampered with
  - **Blinding**: value cannot be read until revealed
- Choose a serial number and commit to it: $(H(S, r))$
- Mint a zerocoin by placing a mint transaction in the blockchain which "spends" a bitcoin and includes the commitment
- Spending a zerocoin gives the recipient a bitcoin



Zerocoin minting process

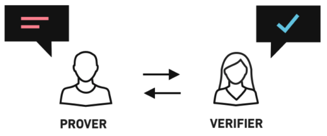
Managing Zerocoins

- To spend a zerocoin
  - You reveal the serial number and place it in the blockchain
  - Prove it is from some zerocoin in the blockchain
    - You have a secret r such that $H(S, r)$ is one of the unspent zerocoins in the blockchain
    - Since r is secret, no one can figure out which zerocoin corresponds to serial number S
    - Folks only know you know how to generate $H(S, r)$ of some unspent zerocoin



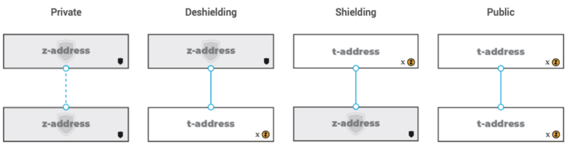
Zero-knowledge proofs

- Specific variant: **zk-SNARKs**
    - Refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier
- Allows us to prove:
    - The serial number of a zerocoin
    - That the coin is in the blockchain



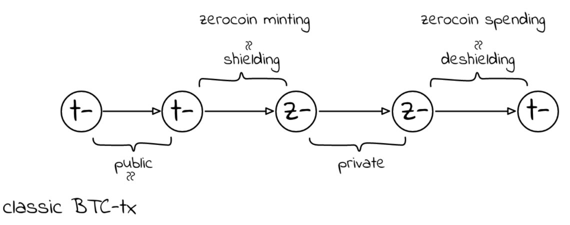
Zerocash: Zerocoin without bitcoin

- Transaction types
  - ZCash allows for 4 different transaction types
  - Used for exchanges between its two different address types
  - Address types can be private or public (z-addresses or t-addresses)



Fully private transactions

- **Idea**: all transactions can be zerocoins
- The transaction value itself is stored within the closed envelope
- The ledger simply stores the existence of transactions (tx details are encrypted)



Zcash transaction types

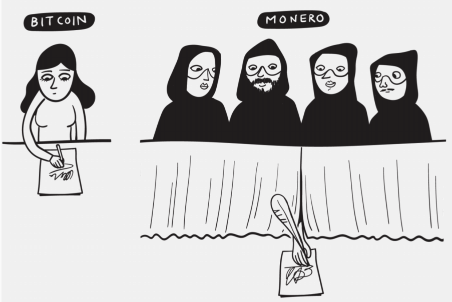
Learn more by reading the original Zerocash paper

Traceless cryptocurrencies

Monero

Privacy notions in Monero

- **Ring signatures** are used in Monero to ensure that:
  - The sender/receiver of a transaction does not let anyone know that they sent/received any Monero
- Ring signatures mix the funds (input) of the sender with other decoy funds from other senders
  - Ring Confidential Transactions (RingCT) guarantee that the transactions are valid without knowing the amounts



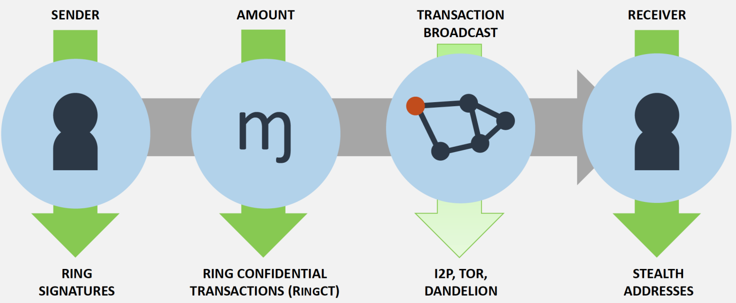
Anatomy of a ring signature

- 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

Stealth addresses

- Funds are not linked to a particular public address
- Senders create one-time addresses on behalf of the recipient (using the recipient's public view and send keys)
- Monero wallets continuously scan the Monero blockchain for any transactions which may be destined to them (using the receiver's private view key)
- The receiver can unlock the funds sent to these one-time addresses by generating a one-time private key

Monero in a nutshell



Learn more at Monero's research lab

Takeaways

- An essential process involved in cybercrime involves how to perform payments online without leaving a trail
- Bitcoin is a virtual currency system that allows for online transactions to be performed securely in a decentralized fashion
- Bitcoin's anonymity guarantees are only relatively good, and recent efforts have been made to create increasingly secure cryptocurrencies

Pointers

- **Other resources:**
  - Bitcoin: A Peer-to-Peer Electronic Cash System
  - A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Meiklejohn et al. IMC'13
- **Acknowledgements:**
  - Adapted and extended from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon
  - Amir Houmansadr - CS660
  - Justin Ehrenhofer
  - Mario Canul and Saxon Knight
  - Aleksandar Hadzhiyski
  - Emmett Steve