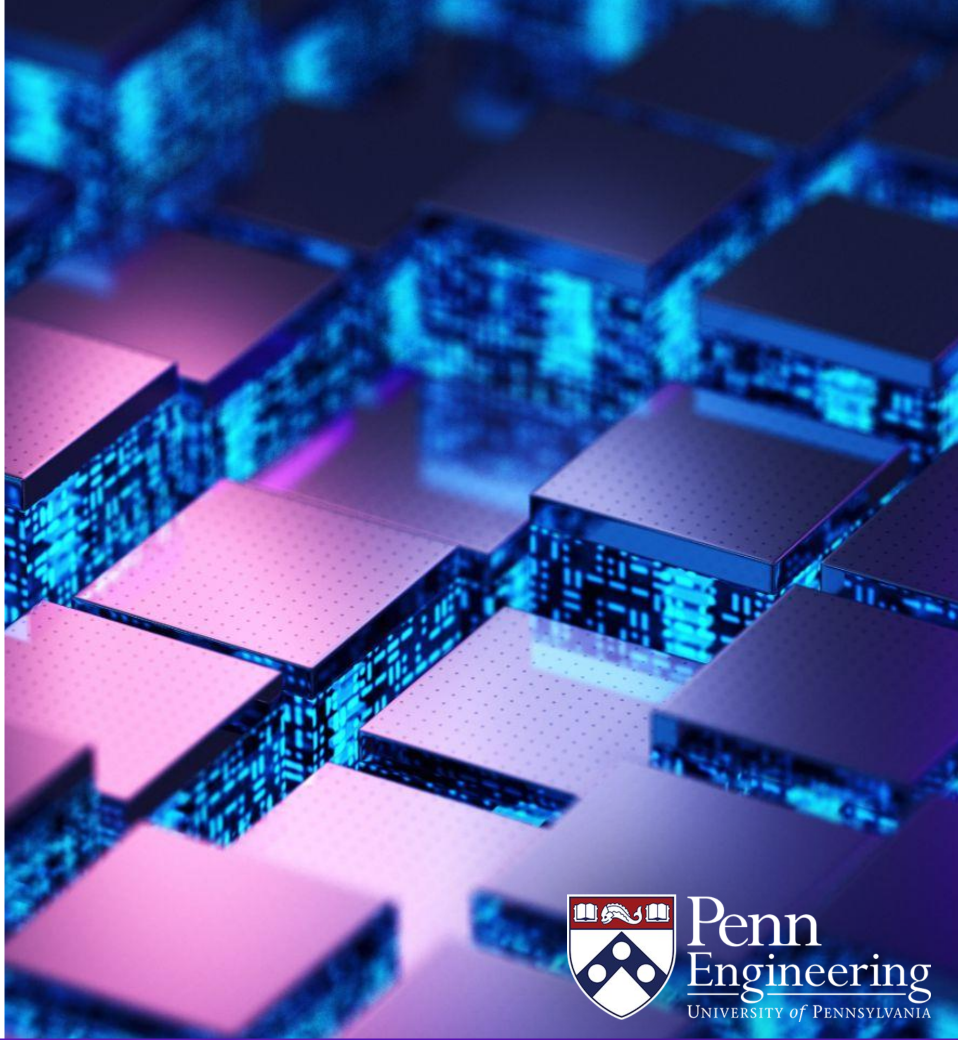
EAS 5830: BLOCKCHAINS

Tracing Bitcoin Transactions

Professor Brett Hemenway Falk



Public ledgers are not private

“The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method…”

-Satoshi Nakamoto

Maintaining Privacy in Bitcoin

“privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.”

(Public keys are pseudonyms)

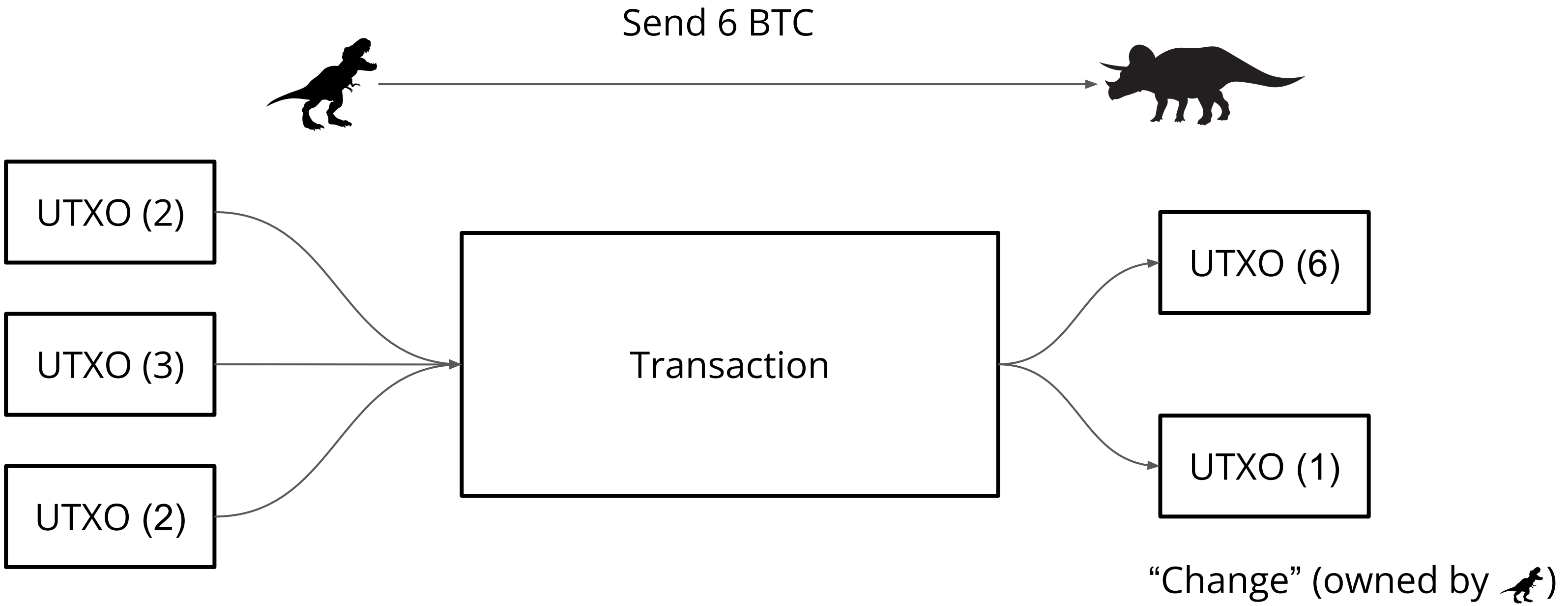
(Recipients are hashes of public keys)

“a new key pair should be used for each transaction to keep them from being linked to a common owner.”

-Satoshi Nakamoto

Making transactions in the UTXO model

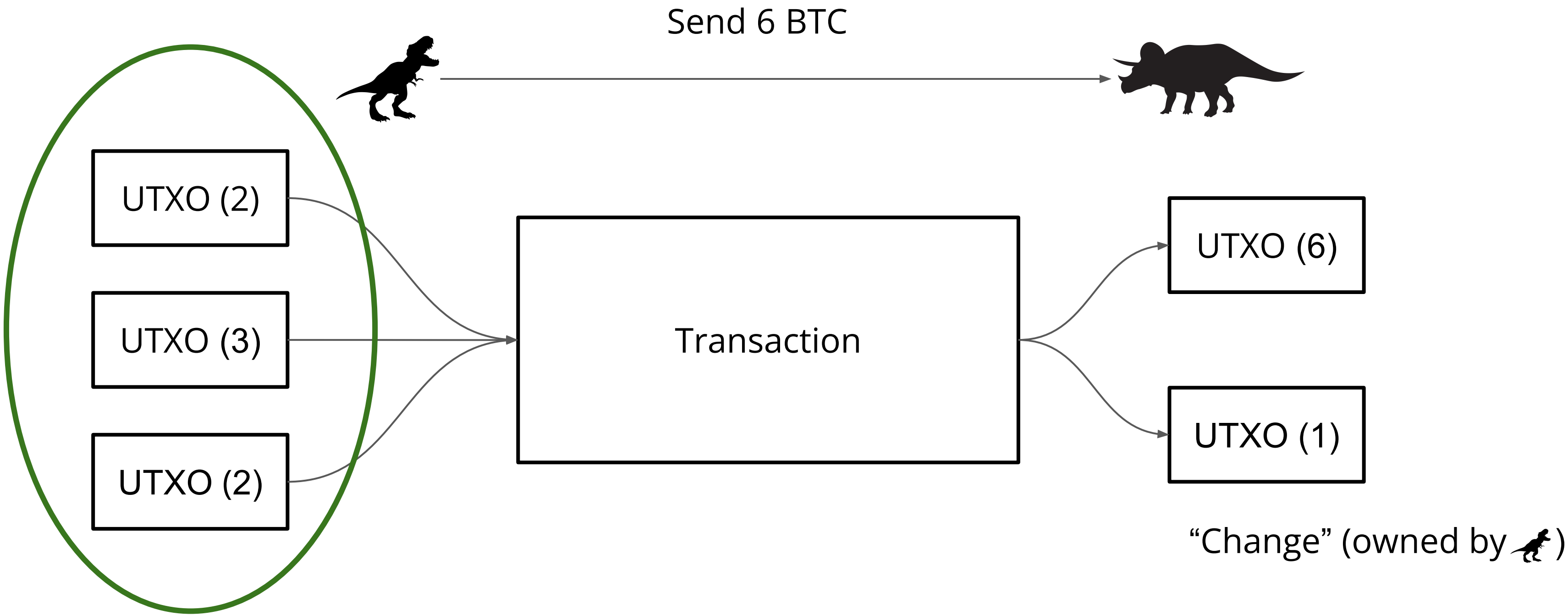
Making transactions in the UTXO model



Heuristics

- Multi-input heuristic
  - If multiple inputs with different keys are used in one transaction, those keys belong to the same owner
- Shadow Address Heuristic
  - If a transaction has multiple outputs, and exactly one of them has never been seen before, that address is a ‘change’ address and belongs to the same owner as the input

Multi-input heuristic



Send 6 BTC

UTXO (2)

UTXO (3)

UTXO (2)

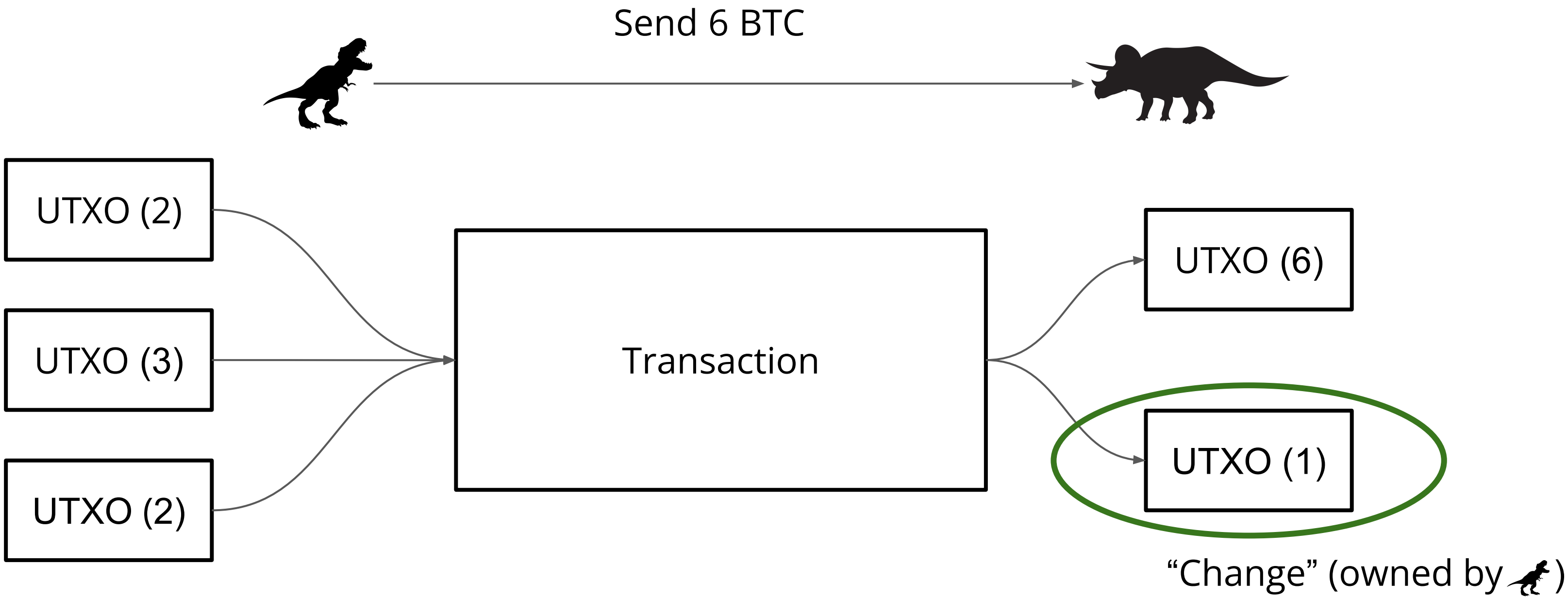
Transaction

UTXO (6)

UTXO (1)

“Change” (owned by 🦖)

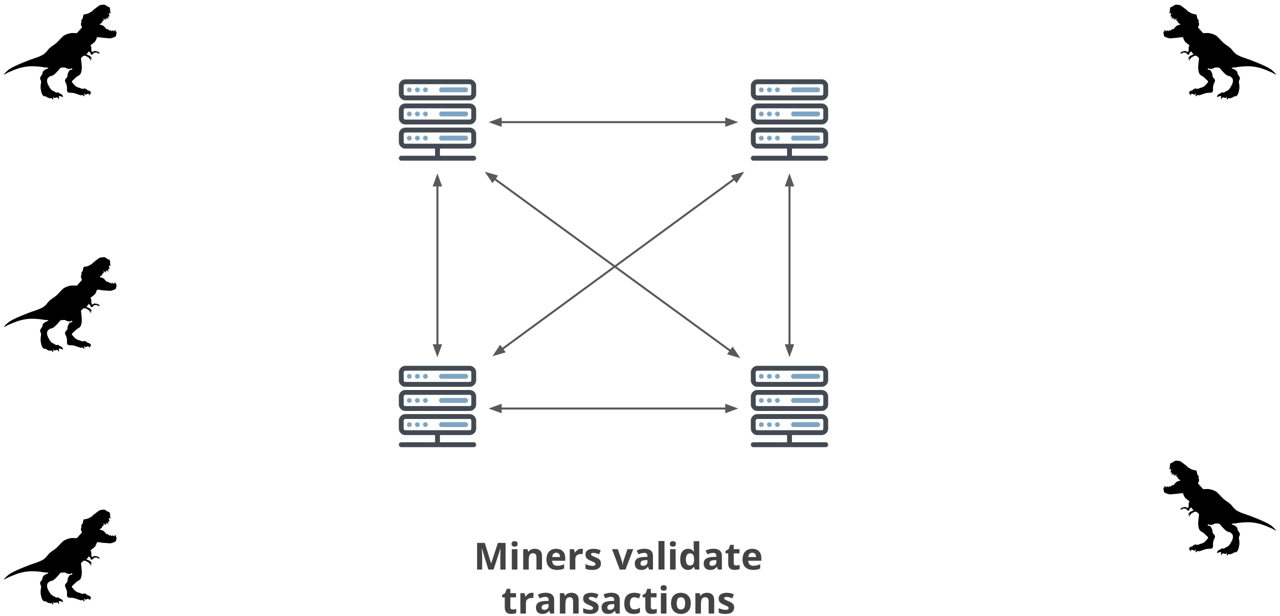
Shadow address heuristic



Heuristics

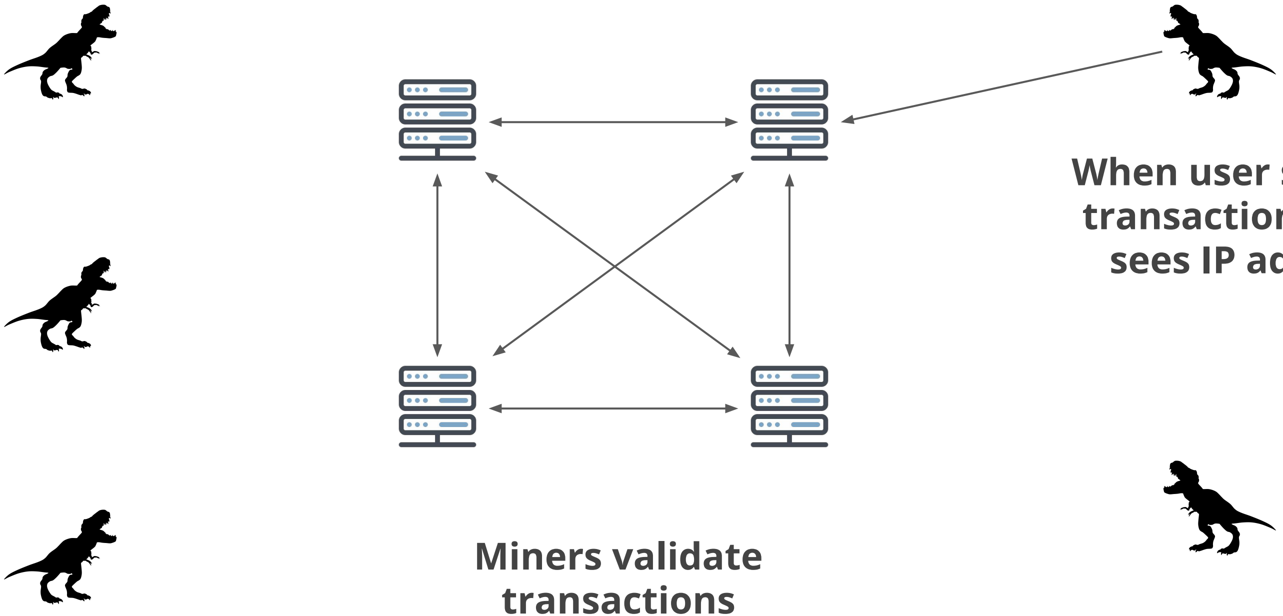
- A Fistful of Bitcoins: Characterizing Payments Among Men with No Names (2013)
- Evaluating User Privacy in Bitcoin (2013)
  - “the profiles of almost 40% of the users can be, to a large extent, recovered even when users adopt privacy measures recommended by Bitcoin”
- Tracking Bitcoin Users Activity Using Community Detection on a Network of Weak Signals (2017)

Miners have extra information



Miners validate transactions

Miners have extra information



When user submits transaction miner sees IP address

Miners validate transactions

Coinseer

- Academics developed a Bitcoin client (CoinSeer)
- Ran a validator for five months (from July 2012 to January 2013)
- CoinSeer kept track of all transactions and *IP address* that relayed the transaction
- Analyzed about 3.9 million transactions
- Able to link between 250 - 1150 Bitcoin accounts to specific IP addresses (depending on their confidence threshold of the link).
    - An Analysis of Anonymity in Bitcoin Using P2P Network Traffic

Chainalysis

- Chainalysis is the primary tracking tool used by the US government
- May have been running 10% of Bitcoin nodes

Tracking via HTML cookies

- When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies (2017)
  - “if the user pays using a cryptocurrency, trackers typically possess enough information about the purchase to uniquely identify the transaction on the blockchain, link it to the user’s cookie, and further to the user’s real identity.”
- Surveyed 130 e-commerce sites that accept Bitcoins
  - 53 of them share purchase information third party trackers.
- Sites place tracking cookies on a user’s machine
- Cookies can be used to track the user’s activity across multiple sites, and much of this information is sent in the clear
- Cookies link Bitcoin address used to make a purchase at one site to the personally identifiable information (e.g. name,address, phone number)
- Can even de-anonymize CoinJoin transactions

Tumblers and Mixers

- An analysis of Bitcoin laundry services
- Analyzed several popular mixing services (“tumblers”) that mix, tumble or launder Bitcoin transactions
- Found that these mixers generally have weak mixing algorithms that do little to prevent tracing “tainted” BTC
- Some mixers actively decrease anonymity by storing client IP addresses

Chipmixer

- Generates “chips”
  - UTXOs in power-of-two increments
  - .001 BTC, .002 BTC, .004 BTC, etc
- User sends money to Chipmixer account
- Chipmixer gives user secret-key to a set of chips
- Chips were created *before* user sent money to Chipmixer
- User must trust Chipmixer
  - No guarantee Chipmixer will send chips
  - Chipmixer still holds sk for chips

“Bitcoin is the opposite of untraceable…other cryptocurrencies too are completely traceable and had served as this kind of trap I began to see for people seeking Financial privacy”

Andy Greenberg