# A Forensic Look of Cryptocurrency: Challenges and Possible Solutions

Yong Guan

Department of Electrical and Computer Engineering
Associate Director for Research, Information Assurance Center
Iowa State University

August 5, 2016

## Recent BitCoin Cases

- Mt. Gox, Feb/March 2014, A coin theft case
- Silk Road: Online Black Market
  - Ran as a Tor hidden service
  - Launched in Feb 2011, Shutdown in 2013
  - Ross William Ulbricht arrested, and a jury trial began (Jan 13, 2015) in U.S.A. v. Ulbricht in Federal Court in Manhattan
- Kidnapping case in Hong Kong, Nov. 2015
- Silk Road 2.0:
  - "Pandora", "Blue Sky", "Hydra" and "Cloud Nine"
  - "Executive Outcomes" (exotic firearms trafficking)
  - "Fake Real Plastic" (counterfeit credit cards)
  - "Fake ID" (fake passports)
  - "Fast Cash!" and "Super Notes Counter" (offered to sell counterfeit Euros and US dollars in exchange for Bitcoin)
- Not surprisingly, the investigation remains ongoing, Silk Road 3.0, ...

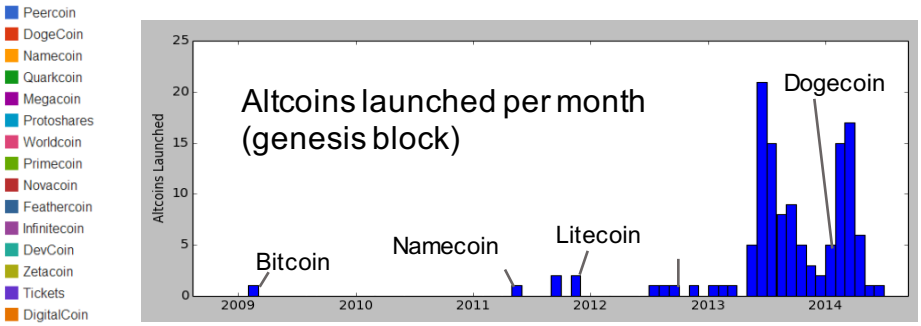
# BitCoin, AltCoins, and the Cryptocurrency Ecosystems

Forensic Aspects: Challenges and Possible solutions

IOWA STATE UNIVERSITY

## A Short History of Cryptocurrency

- David Chaum, 1982, Anonymous e-cash via Blind Signature
- Bitcoin, started in 2009, gain quick popularity.
- Since then, between 150-500 altcoins launched.



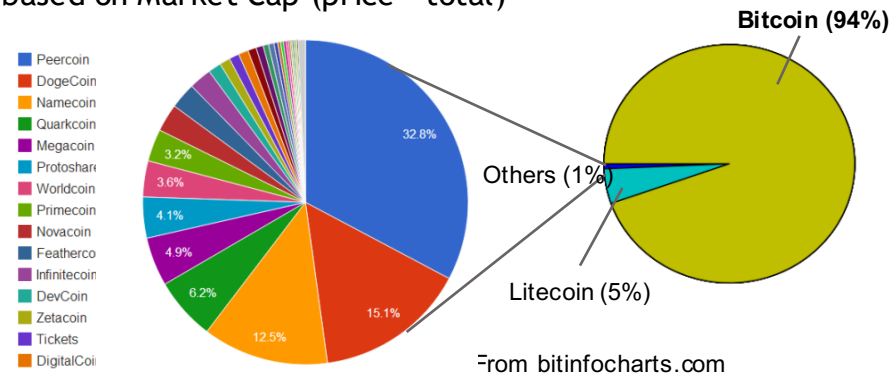

From bitinfocharts.com

IOWA STATE UNIVERSITY

# Bitcoin, Altcoins, and the Cryptocurrency Ecosystem

**Bitcoin and Litecoin are 99% of total**

based on Market Cap (price * total)




From bitinfocharts.com

Bitcoin and hundreds of Altcoins coexist

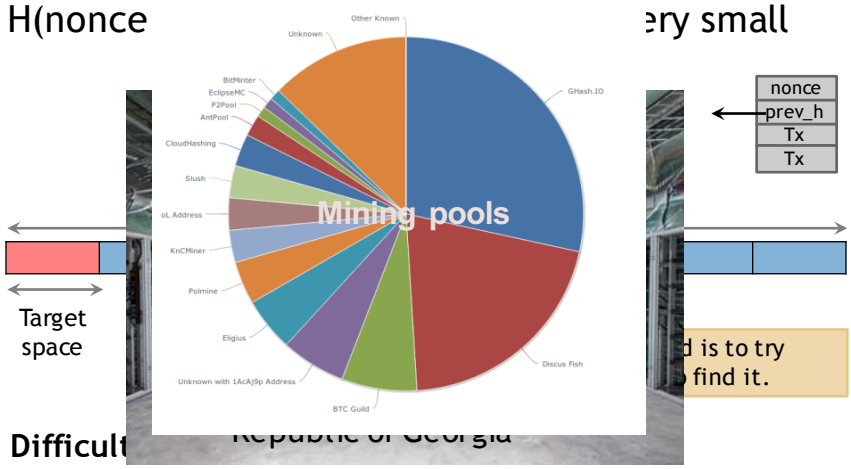
- Compete and interact supportively or destructively

IOWA STATE UNIVERSITY

# Bitcoin Mining

To create block, find nonce s.t.

H(nonce ... ery small





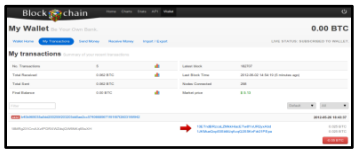


Difficult

IOWA STATE UNIVERSITY

## Online Wallets and Exchanges

- Online wallet
  Like local wallet, but in the cloud
  but security worries




- Bitcoin Exchanges
  Like **Bank**
  Accept deposits of Bitcoins and real-world currency ($, €, …)
  promise to pay back on demand
  Lets customers:
  make and receive Bitcoin payments
  buy/sell Bitcoins for real-world currency
  typically, match up BTC buyer with BTC seller

IOWA STATE UNIVERSITY

## Banks and Exchanges

Charles Ponzi

IOWA STATE UNIVERSITY

WIRED.CO.UK

FOLLOW

NEWS Topics / TECHNOLOGY BITCOIN MT GOX CRYPTOCURRENCIES

6 issues for £9 + FREE iPad & iPhone editions SUBSCRIBE

## Study: 45 percent of Bitcoin exchanges end up closing

TECHNOLOGY / 26 APRIL 13 / by IAN STEADMAN

Tweet Like 14 g+1

A study of the Bitcoin exchange industry has found that 45 percent of exchanges fail, taking their users' money with them. Those that survive are the ones that handle the most traffic -- but they are also the exchanges that suffer the greatest number of cyber attacks.

Computer scientists Tyler Moore (from the Southern Methodist University, Dallas) and Nicolas Christin (of Carnegie Mellon University) found 40 exchanges on the web which offered a service of changing bitcoins into other fiat currencies or back again. Of those 40, 18 have gone out of business -- 13 closing without warning, and five closing after suffering security breaches that forced them to close. Four other exchanges have


Almost half of all exchanges close *Shutterstock*

IOWA STATE UNIVERSITY

# Objectives of This Work

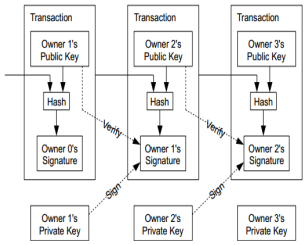
- Why Forensics on Bitcoin?
  - Bitcoin currency is freely circulated, not subject to central management
  - Bitcoin are decently anonymized and difficult to be ID related
  - Transactions involve various goods and services
    - Black drug and weapon markets
    - Selling theft identities
  - Bitcoin theft is hardly recoverable
    - No insurance on lost money
  - Detecting Bitcoin activities are difficult
- Objectives of this work (to answer these forensic questions)
  - Is it possible to know which Bitcoin addresses belong to the same person/group?
  - Is it possible to discover some pattern on where money (Bitcoin) flows between Bitcoin users/groups?
  - Is it possible (and where) to collect forensic evidence on certain Bitcoin transactions?

- Joint work with Chen Zhao, IFIP 11.9 Digital Forensics Conference 2015

IOWA STATE UNIVERSITY

# How Bitcoin Works

- Signature Based Transaction
  - Every transaction involves a list of payers (inputs) and a list of payees (outputs)
  - A payer/payee is uniquely identified by a public address
  - An address is a script generated from an ECDSA private/public key pair
  - Spend payments (Bitcoin) from others to pay
  - Unable to send payments without the private key

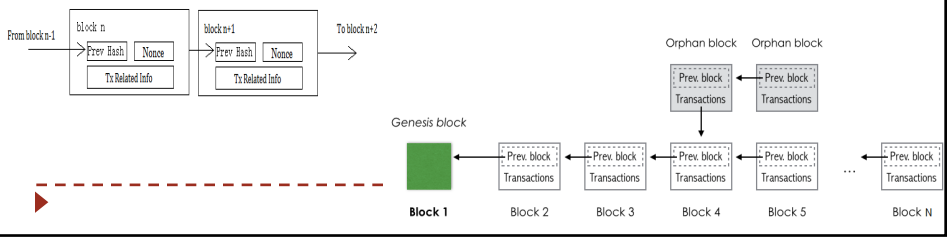



- Transactions are broadcast to the Internet (eventually in Block Chain, if confirmed)
  - Once issued a transaction cannot be cancelled
  - Others can spend your money if key is disclosed
  - A person can have multiple addresses
    - E.g. generate a new key pair for every single Transaction

IOWA STATE UNIVERSITY

# Block Chain

- A Database to Store Global Bitcoin Transactions
- A Chained Structure by One Block Hashed to the Next
  - Each block contains Bitcoin transactions
  - The block chain is publicly open for global mining
  - Mining is difficult as each block has to be hashed under some threshold
  - Mining reward is saved in the newly mined block (as payment to addresses)
- Transaction confirmation
  - Transactions are received and confirmed by Bitcoin miners around the world
  - Not confirmed until seen in a block
  - Unconfirmed transactions are invalid before actually confirmed



IOWA STATE UNIVERSITY

# What Transactions Look Like


```
{
"inputs":
[
{"value": 2.5, "address": "13vjvKHDeFhtwRGseVkLFIeXA7ZrJA2Uo9"},
{"value": 0.5092427, "address":
"1EyH7htSWjSyuXgofuE9gKX5Sr4yEyDcD2"}
],
"blocktime": 1389490523,
"outputs":
[
{"value": 2.8, "address": "1Q5ztGyLj7KxL2rs7bmVcKYDfTYmpQs5bo"},
{"value": 0.2090427, "address":
"1G7HKqqTUCrTpMDEYV5SdzcarFPhKKHb12"}
]
}
```


**A Single Transaction**


```
{
"inputs":
[{"address": "coinbase"}],
"blocktime": 1354133545,
"blockhash": "0000000000000498e426effa08fc54070cd7ca70e8020 6f8763e7ceaaab734bc",
"outputs": [{"value": 25.051 2, "address":" 18 11 f7UUQAkAejj1 1dU5cVtKUSTfoSVzdm"}]
}
```


**A Coinbase Transaction**

- Every transaction has an input list and an output list
- A coinbase transaction is a mining reward with no valid input address
- Outputs and inputs can have multiple addresses and different values
- Sum of outputs have to be equal to or lower than sum of inputs
  - Because one can not spend more money than he has
  - Difference between input and output are paid to whoever confirmed the Tx.

IOWA STATE UNIVERSITY

# A 3-Step Approach

- Step 1 – Address clustering
  - Mark all addresses that possibly belong to the same entity
  - Map an address to the correct entity set
  - Query which set an address belongs to in O(1)
- Step 2 – Generate address graph
  - Inherit database from Step 1
  - Clearly show the transaction pattern between any 2 entities of interest
- Step 3 – Observation and graph search
  - Investigate suspicious coins (transactions)
  - Traverse and search for the trace of money

IOWA STATE UNIVERSITY

# Address clustering


```
{
"inputs":
[
{"value": 2.5, "address": "13vjvKHDeFhtwRGseVkLF1eXA7ZrJA2Uo9"},
{"value": 0.5092427, "address": "1EyH7htSWjSyuXgofuE9gKX5Sr4yEyDcD2"}
],
"blocktime": 1389490523,
"outputs":
[
{"value": 2.8, "address": "1Q5ztGyLj7KxL2rs7bmVcKYDfTYmpQs5bo"},
{"value": 0.2090427, "address": "1G7HKqqTUCrTpMDEYV5SdzcarFPhKKHbl2"}
]
}
```

```
{
"inputs":
[{"address": "coinbase"}],
"blocktime": 1354133545,
"blockhash":
"0000000000000498e426effa08fc54070cd7ca70e80206f8763e7ceaaab734bc",
"outputs":[{"value": 25.0512,
"address":"1811f7UUQAkAejj11dU5cVtKUSTfoSVzdm"}]
}
```


- Addresses are mapped to the same set given:
  - Inputs to the same transaction
  - Outputs of the same coinbase transaction
  - A one-time change address generated for that single transaction
    - Not the only address in the output
    - Not in the input
    - All the other transactions in the output are used as output for more than once
      - Not sure which address is the change

IOWA STATE UNIVERSITY

# Some Useful Heuristics

- A transaction input list contains addresses from the same person
  - One cannot spend them in on transaction unless truly own the inputs
- Coinbases reflect mining behaviors
  - The output addresses share the mining reward due to collaboration
- Some output addresses are used as payees only once
  - Can be one-time change addresses for the sole purpose of change
  - No way to tell all of them for sure, but there are some characteristics
    - Make sure it only appears once as output
    - We ignore possible existence of multiple one-time change addresses in the same transaction
    - To avoid false positive
  - One-time change addresses are clustered into the transaction input own addresses
    - Because change is paid to the payer

IOWA STATE UNIVERSITY

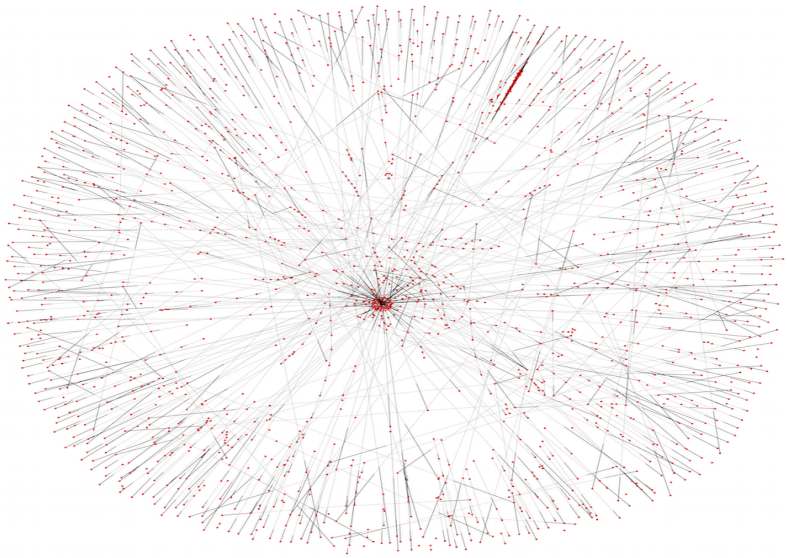
# Set Union Operations

- Out Data Set
  - All 34,839,029 transactions from block 210,000 to 314,700
  - A total 35,770,360 addresses are involved
- What we want
  - For every single address we know which set it is in (set ID)
  - Addresses that are clustered to the same set have the same set ID
- We used a small key-value-mapping database to represent the sets
  - Set clustering should be transitive, e.g. one element is joined all that set is
  - Use the key-value mapping to save runtime complexity

IOWA STATE UNIVERSITY

# Address Graph

Address Graph – Tx Data From Block #284000 to #284600



IOWA STATE UNIVERSITY

# Coin Flow Analysis

- Problem definition
  - Given specific coins suspicious of theft or other crimes, track possible trace of money within a specific time period
  - Give answers to how much money goes to where
- Approach Description
  - Use address graphs parsed from relevant blocks
  - BFS search the graph and save coin amount spent on each level
    - Coin amount is the net output value
    - Net output=sum(out edges)-sum(in edges from unvisited vertices)

IOWA STATE UNIVERSITY

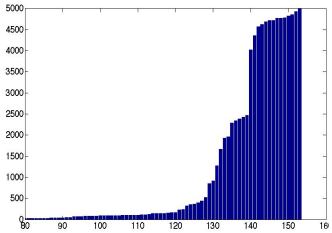
# Mt. Gox Incident

- Largest Bitcoin Loss Case in History
  - Press release time February 7, 2014
  - Led to bankruptcy of Mt. Box, a Japan based Bitcoin exchange provider
  - Claimed loss up to 850,000 BTC (0.5$ Billion by market value at time)
  - Still undergoing investigation
- Two Major Possible Causes
  - Attack against the systems that made double withdrawals possible
    - E.g. cash withdrawal at 2 BTC for 1 BTC
  - Internal break-in and theft
    - Could steal huge amounts of customer assets

IOWA STATE UNIVERSITY

# Case Study – Mt. Gox

- Search for suspicious transaction outputs
  - Assume thefts are in payments above 10 BTC
  - From 19:49:42, 2014-02-03 to 00:28:17, 2014-02-06




  - 153 graph vertices are picked from large transactions
  - For simplicity, start with 70,510 BTC in 14 nodes
    - Might be only a small portion of lost coins

IOWA STATE UNIVERSITY

# Summery and Future Works

- Bitcoin and various Altcoins pose new challenges to digital forensics:
  - Where and how to identify and recover artifacts (evidence)
  - How to analyze them?
- Future directions:
  - Large dynamic Bitcoin transactions graph analysis for anti-money laundering
  - Provide solid evidence on proof-of-work in cryptocurrency systems against Vigilante Attack

IOWA STATE UNIVERSITY

# Thanks

## Q&A

Yong Guan
guan@iastate.edu
Iowa State University