463.10 Bitcoin

Computer Security II
CS463/ECE424
University of Illinois
• Bitcoin: A Peer-to-Peer Electronic Cash System
• Satoshi Nakamoto
• Manuscript
• Currency systems rely on trust (government, bank). Is it possible to build a currency without trusted authorities?
• Use a Proof of Work scheme to place authority in the hands of a distributed preponderance of capability.
• The Bitcoin approach has been implemented in practice and now sees a multi-billion dollar capitalization.
• This has inspired a fresh look at crypto currency and at the underlying techniques of Bitcoin.
Bitcoin’s three main protocols

**Network:** How can we share transactions & history?

**Transactions:** How can we agree what the history means?

**Consensus:** How can we agree on one global history?
Introduction to Cryptographic Currencies

Claudio Orlandi

cs.au.dk/~orlandi

Thanks to: Jon K. Sørensen and Peter S. Nordholt
Outline

• **Part 0**: a little history

• **Part 1**: TheoryCoin
  – *How to create* coins
  – *How to transfer* coins
  – *How to store* coins

• **Part 2**: \( \text{diff}(\text{T}, \text{Bitcoin}) \)

• **Part 3**: Problems and issues
The 1990s
David Chaum and anonymous ecash

“The difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy”

(attributed to Chaum)
Anonymous payments

"withdraw"

BANK

M or L?

shop

"withdraw"
Chaum’s anonymous e-cash

anonymous
secure (no double-spending)
only transfer (no creation/storage)

...and bankrupted in 1999
The advent of Bitcoin

• 2009: **Bitcoin announced** by Satoshi Nakamoto  
  – Pseudonym for person or group of people

• 2009-2011: slow start...

• 2011-2013: Silk Road and Dread Pirate Roberts

• **End 2013**: **Bitcoin price skyrockets**  
  – and the world notices!
Outline

• **Part 0**: a little history

• **Part 1**: TheoryCoin
  – How to *create* coins
  – How to *transfer* coins
  – How to *store* coins

• **Part 2**: \( \text{diff}(T, \text{Bitcoin}) \)

• **Part 3**: Problems and issues
TheoryCoin: How to create money

1. Everyone tries to solve a puzzle

2. The first one to solve the puzzle gets 1 TC

3. The solution of puzzle $i$ defines puzzle $i+1$
TheoryCoin:
How to *create* money

\[ L \in \{0,1\}^* \quad R \in \{0,1\}^* \quad T \in \{0,1\}^d \]

(a random function)

\[ H \]

The puzzle:
given \( L \), find \( R \) such that \( T=0^d \)

* aka *Proof-of-Work*

SolvePuzzle(L) {
    repeat{
        \[ R = \text{my\_name} || \text{i++} \]
        \[ T = H(L,R) \]
    } while (T ≠ 0^d)
    return R
}
TheoryCoin: (coins to ppl)

How to create money

\[
x_0 = \text{Start!}
\]

\[
x_1 = (P_1, i_1)
\]

\[
x_2 = (P_2, i_2)
\]

\[
x_3 = (P_3, i_3)
\]

* aka the blockchain

\[
000...000
\]

\[
000...000
\]

\[
000...000
\]

SolvePuzzle(L) {
    \text{repeat} {
        \text{R = my\_name || i++}
        \text{T = H(L, R)}
    } \text{while (T ≠ 0^d)}
    \text{return R}
}
TheoryCoin:
How to **create** money

*aka the 51% attack*
TheoryCoin: How to create money

Recap:

Solve the next puzzle → get a coin

– To “solve” puzzle i find $x_i$ s.t. $H(x_{i-1}, x_i) = 0$

– The longest chain defines “next puzzle”

– The name in block $x_i$ “gets” coin i.
Outline

• **Part 0:** a little history

• **Part 1:** TheoryCoin
  – How to create coins
  – How to transfer coins
  – How to store coins

• **Part 2:** \( \text{diff}(\text{T}, \text{bitcoin}) \)

• **Part 3:** Problems and issues
TheoryCoin: How to transfer money

(Digital) Signatures
– Only you can sign
– Everyone can verify
– You cannot deny

Give coin 3 to Jesper

Claudio
How to transfer money

TheoryCoin

"Your pin code"
message
secret key
Sign
message, signature
Gen
"Your username"
public key
Verify
accept/reject
TheoryCoin: How to **transfer** money

m = "P3 gives coin 3 to P1"

s = Sig(sk3, m)

If Ver(pk3, m, s) = accept and P3 owns coin 3 then return accept
**TheoryCoin:**

**How to transfer money**

$m_1=\text{"P3 gives coin 3 to P1"}$

$s_1=\text{Sig}(sk_3, m_1)$

$m_2=\text{"P3 gives coin 3 to P2"}$

$s_2=\text{Sig}(sk_3, m_2)$

* aka double spending*
TheoryCoin: How to **transfer** money

- write \((m_1, s_1)\)
- write \((m_2, s_2)\)
- read \((m_1, s_1)\)
- read \((m_2, s_2)\)
- read \((m_4, s_4)\)
- read \((m_2, s_2)\)
- read \((m_4, s_4)\)
- write \((m_4, s_4)\)

- accept
- reject

\[ m_1 = "P_3\ gives\ coin 3\ to\ P_4" \]
\[ s_4 = \text{Sig}(sk_3, m_4) \]

\[ m_2 = "P_3\ gives\ coin 3\ to\ P_2" \]
\[ s_2 = \text{Sig}(sk_3, m_2) \]
Outline

• **Part 0**: a little history

• **Part 1**: TheoryCoin
  – How to **create** coins
  – How to **transfer** coins
  – How to **store** coins

• **Part 2**: $\text{diff}(\text{T}, \text{BTC})$

• **Part 3**: Problems and issues
TheoryCoin: How to store money

Main Idea:
Record transfers in the blockchain

\[ x_0 = \text{Start!} \quad x_1 = (P_1, i_1) \quad x_2 = (P_2, i_1) \quad x_3 = (P_3, i_3) \]
TheoryCoin: How to **store** money

SolvePuzzle(L,...){
    repeat{
        R = my_name || (m,s) || i++
        T = H(L,R)
        }while(T ≠ 0)
    return R
}

\[ x_0 = \text{Start!} \quad x_1 = (P_1, i_1) \quad x_2 = (P_2, i_1) \quad x_3 = (P_3, i_3) \quad x_4 = (P_4, (m,s), i_4) \]
Outline

• **Part 0**: a little history

• **Part 1**: TheoryCoin
  – How to **create** coins
  – How to **transfer** coins
  – How to **store** coins

• **Part 2**: \text{diff}(T, \text{Bitcoin})

• **Part 3**: Problems and issues
How is money created in Bitcoin?

- New block **every ~10 mins**
  - \( d \) adjusted every ~2000 blocks

- \( H = 2^{\text{SHA2}} \)

- Initial reward: **50 BTC**
  - Halved every ~4 years (now about to decrease from 12.5 to 6.25 BTC)
How is money transferred in Bitcoin?

Example: P1 wants to give 60 to P2

... gives 50 to P1

... gives 25 to P1

P1 gives 14 to P1

Transaction fee 1

P1 gives 60 to P2
How is money stored in Bitcoin?

- **Transaction in orphaned blocks** are invalid
  - **Wait 6 blocks** (~1 hour) before accepting transaction.
  - **Checkpoints** to prevent complete history rollback.

- **All transactions** are stored in the blockchain
  - *(Currently ~242.39 GB)*
Outline

• **Part 0**: a little history

• **Part 1**: TheoryCoin
  – How to create coins
  – How to transfer coins
  – How to store coins

• **Part 2**: diff(TheoryCoin, Bitcoin)

• **Part 3**: Problems and issues
Anonymity?

• Problem:
  – Every transaction ever made is recorded forever

• Solution?
  – Use new identity for each transaction

• But:
  – Heuristics allow to **cluster** identities

• Anonymous alternatives:
  – Zerocoin, Zerocash…
A final word…

Distributed currencies: for the **good guys** or the **bad guys**?

– Crime is bad! Tax evasion is bad!
– But sometimes governments are bad too!

Thanks! Questions?
Sources:
Learn about signatures/ecash/cryptography at csaudk
https://services.brics.dk/java/courseadmin/crypto/
https://services.brics.dk/java/courseadmin/cpt
https://services.brics.dk/java/courseadmin/CryCom
Story of Chaum and DigiCash (to be taken with a grain of salt)
http://cryptome.org/jya/digicrash.htm
Bitcoin paper and announcement
http://article.gmane.org/gmane.comp.encryption.general/12588/
http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html
This pizza cost 750,000 usd
http://motherboard.vice.com/blog/this-pizza-is-worth-750000
Lily Allen turns down btcs
https://twitter.com/lilyallen/statuses/419942070770741249
Signature attack
http://eprint.iacr.org/2013/734
Deanonymizing
http://eprint.iacr.org/2012/584
Zerocoin/Zerocash
http://zerocoin.org/
Graphs, stats etc
www.blockchain.info
Comparison with Altcoins
http://www.coinwarz.com/cryptocurrency
Bitcoin stolen from TV
Visa/Mastercard vs Wikileaks
Not in the talk, but very interesting:
Silkroad essentials
The value overflow bug
https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures#CVE-2010-5139
The March 2013 chain fork
Buggy transaction, mistery miner
https://blockchain.info/tx-index/3618498/4005d6bea3a93fb72f006d23e2685b85069d270cb57d15f0c057ef2d5e3f78
https://bitcointalk.org/index.php?topic=67634.0
The problem with "checkpointed" bitcoin
This presentation contains copyrighted images the use of which has not always been specifically authorized by the copyright owner. I am making the material available for educational purposes only and I believe this constitutes a ‘fair use’.
MP4 Overview

• Code skeleton is provided

• Checkpoint 1:
  – Get familiar with Bitcoin API
  – Get familiar with blockchain structures

• Checkpoint 2:
  – Cluster bitcoin addresses
  – Generate and analyze user graph

• Report: one-page

• Due date: by midnight on Apr 7
MP4 Checkpoint 1

• Blockchain structures: Blocks
MP4 Checkpoint 1

• Blockchain structures: Transactions

- **TX 0**
  - Input 01
  - Output 01

- **TX 1**
  - Input 01
  - Output 01
  - Output 02

- **TX 2**
  - Input 01
  - Input 02
  - Output 01

- **TX 3**
  - Input 01
  - Output 01
  - Output 02

- **Coinbase Transaction**

- **Normal Transactions**
Cluster Addresses

Joint control assumption:
- Addresses used as inputs to a common transaction are controlled by the same entity

Download all the transactions on 10/25/2013, and cluster the addresses
Why 10/25/2013?

FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road

The Silk Road made a small fortune during its two and a half years as the web's biggest anonymous black market for illegal drugs. As of Friday, at least one $28.5 million chunk of that fortune now belongs to the FBI.
Discussion

• Is Bitcoin a waste of electricity?
• Will Bitcoin enable criminal activity? Will it support democracy?
• What new capabilities might be enabled by Bitcoin?
• What are the prospects for alternative forms of crypto-currency ("altcoins")?