Blockchain: Applications, Security Promises and Internals

Cyber Security & Information Systems Information Analysis Center (CSIAC)

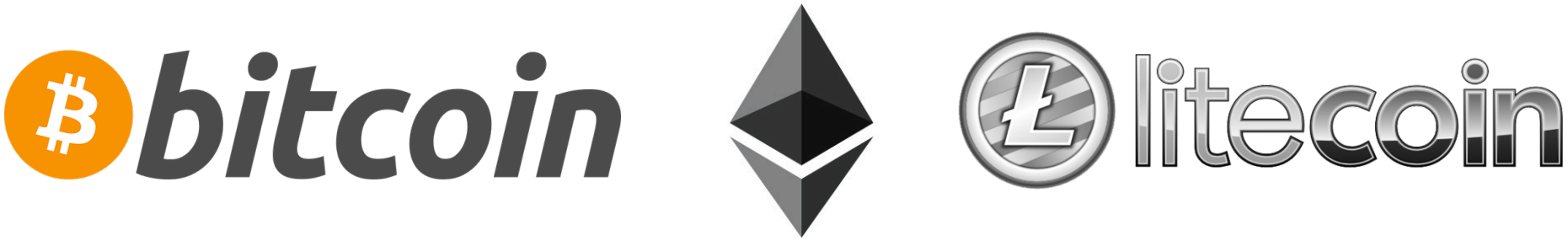
Dr. Yuzhe (Richard) Tang
Department of EECS,
Syracuse University
Dec. 19, 2017

Outline

1. **Introduction**
2. Blockchain applications and interfaces
3. Blockchain security promises
4. Blockchain internals (a brief)

1. Introduction

- Cryptocurrency:
  - "A cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets." (wiki)
  - BitCoin, Etheruem, Litcoin, etc.



1. Introduction

- How to compare the concept of BitCoin with fiat currency (e.g. US dollar)?

What's **Similar** about Bitcoin to US Dollar

Review of gov-issued (fiat) currency

- Workflow
  - Money created by a **mint**
  - Money circulated among owners thru. **transactions**.
  - BitCoin supports the same workflow

What's **Similar** about Bitcoin to US Dollar

Review of gov-issued (fiat) currency

- Threat 1: Print fake money
  - Dollar bills are secured by anti-counterfeit
  - US. mint is safeguarded
  - Bitcoin has to defend this threat

- Threat 2: Double spending (digital currency)
  - Visa's **ledger** database validates transactions
  - BitCoin has to prevent double-spending

Ledger to prevent double spending

Transaction	Amount
Joe->John	X$
Joe->Jane	X$

What's **Similar** about Bitcoin to US Dollar

Review of gov-issued (fiat) currency

- Threat 1: Print fake money
  - Dollar bills are secured by anti-counterfeit
  - US. mint is safeguarded
  - Bitcoin has to defend this threat

- Threat 2: Double spending (digital currency)
  - Visa's **ledger** database validates transactions
  - BitCoin has to prevent double-spending

Ledger to prevent double spending

Transaction	Amount	Status
Joe->John	X$	Accepted
Joe->Jane	X$	Rejected

Issues with US Dollar

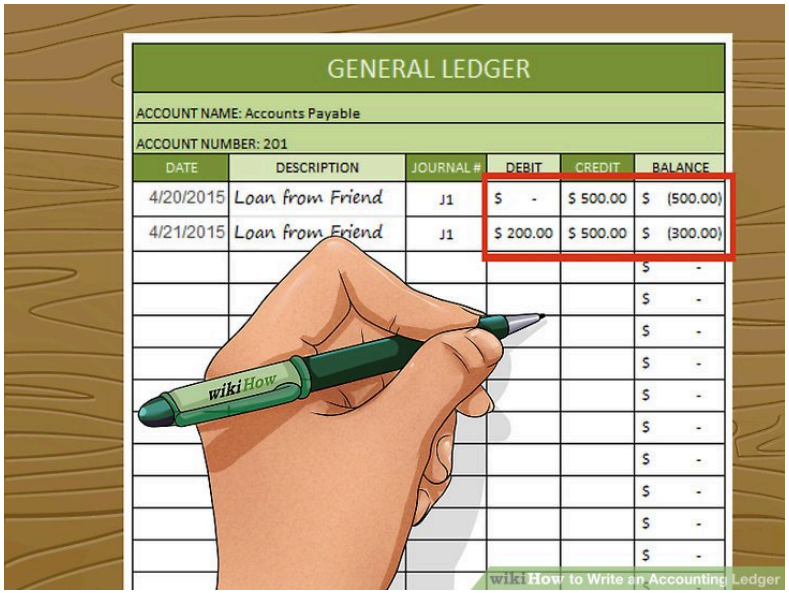
- Using dollar bills, you implicitly trust
  - Government, mint, credit-card org. (Visa)
  - These are **trusted central authorities**
- Are they trustworthy?
  - You may not want gov. to withdraw a tx after it's settled.
  - You may not want gov. to freeze your account
  - You may not want gov. to inflate the currency and depreciate your savings: Zimbabwe

Motivating BitCoin *(What's **unique** about BitCoin)*

- Get rid of central authorities by **decentralization**
  - No need to trust government and Visa
  - Instead trust the entire population on the planet
- Make transaction history public (**Transparency**)
  - Transparency invites trust
- Automate the process with **incentive-compatibility**
  - Automation lowers cost (transaction fee)

BitCoin and Blockchain

- Bitcoin tx history is recorded in **Blockchain**
  - Blockchain is the ledger for Bitcoin



Outline

1. Introduction

2. Blockchain applications and interfaces

3. Blockchain security promises

4. Blockchain internals (a brief)

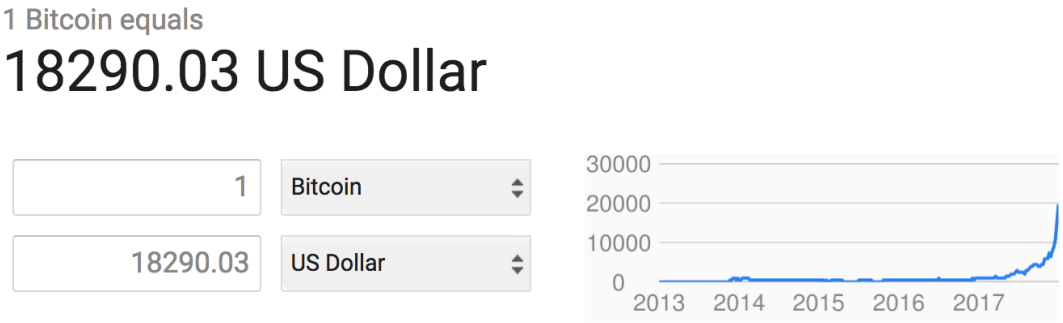
Scenario 1: Doing Transactions

- Get your first BitCoin
  - Exchange services: Coinbase, Coindesk, etc.

coinbase

CoinDesk

- Using BitCoin to sell and buy stuff (transaction)
- Or sell it till the price grows higher



Scenario 2: Mining

- Another way to get BitCoin: Mining
  - Get the money anonymously
- You can purchase hardware to do some (non-sense) computations
  - With some probability, your computation will be rewarded in BitCoin
  - The probability depends on how powerful your hardware is

Scenario 2: Mining

- Interested in mining?
  - How much is your budget?
    - Constant capital: buy machines, Variable capital: electricity consumption
  - Who you are up against (in winning the reward)?
    - State-level miners, bitcoin farm, data centers

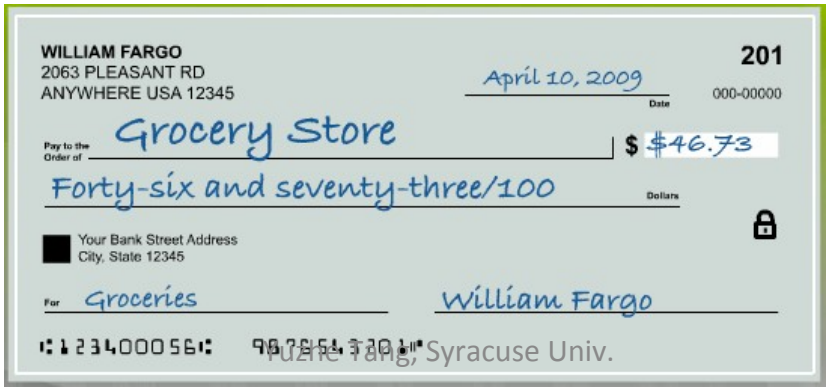
Scenario 3: Develop Applications

- Distributed app over Blockchain (Dapp)
  - FinTech: Insurance, trade, risk management, accounting, etc.
    - Examples: ERP, micro-payments, wallet, currency exchange, etc.
  - Other domains: Legal, medical/healthcare, IT, science/research, etc.

- "Blockchain is set to disrupt many industries"

Scenario 3: Develop Applications

- Dapp architecture: On-chain/off-chain
  - On-chain data : "Transactions" or meta-data
  - Off-chain data: some private data (e.g. keys)
- Interacting Blockchain thru. transaction API:
  - *send_tx(sender, receiver, money#, memo)*
  - Like writing a personal **check**



Scenario 3: Develop Applications

- Design issues
  - Partitioning application logic to suit on-/off-chain
  - Designing incentive schemes (what to reward mining?)
  - Dealing with the limitation of Blockchain (e.g. deferred finality)
- Building a BitCoin wallet Dapp
  - Developer working for CoinBase

Outline

1. Introduction

2. Blockchain applications and interfaces

3. **Blockchain security promises**

4. Blockchain internals (a brief)

Security: Immutable Storage

- Blockchain abstraction as tx storage
  - Readable to the public (**transparency**)
  - Appendable by honest miners
  - Cannot be modified (**immutability**)

- Building a trusted timestamp service for legal documents (signing contract, applying patent etc)

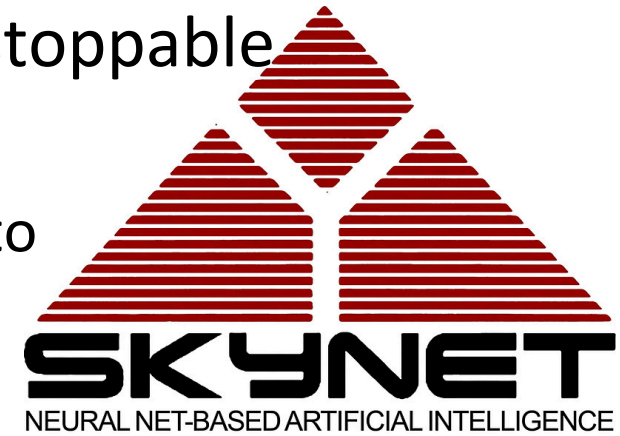
Security: No Double Spending

- No double-spending (Anti-counterfeit)

- Smart property
  - Smart ticket: Use BitCoin to represent baseball tickets.

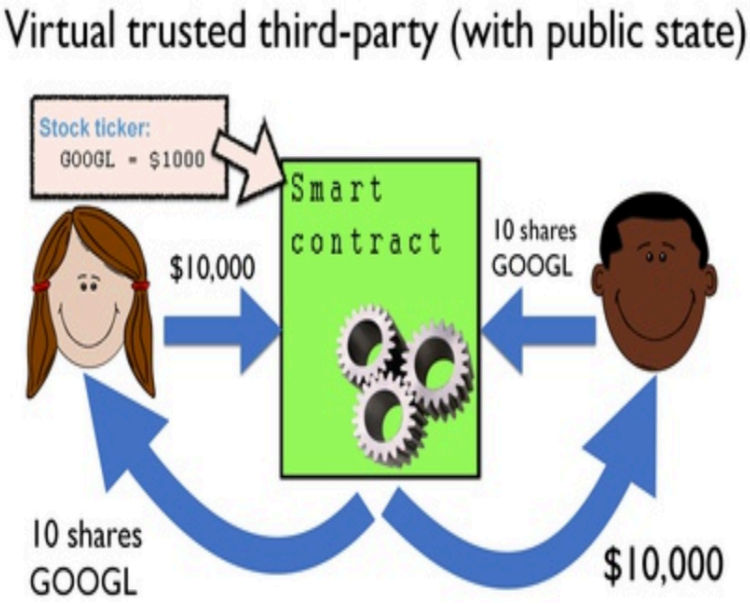
Security: Unstoppable Execution

- Programming lang. on Blockchain: Smart contract
  - Smart-contract program is an obj. running on Blockchain
  - Solidity in Ethereum
- Security properties:
  - Autonomously executed, unstoppable
  - Transaction fairness:
    - If I paid you, to be fair, I need to receive your goods.



Security: Unstoppable Execution

- Smart-contract applications:
  - Implement IFTTT logic that decides how to send tx
- A stock-exchange application
  - Alice will trade 10 shares for $10,000 when the stock price is below $1000.



Acknowledge: Prof. Ari Juels

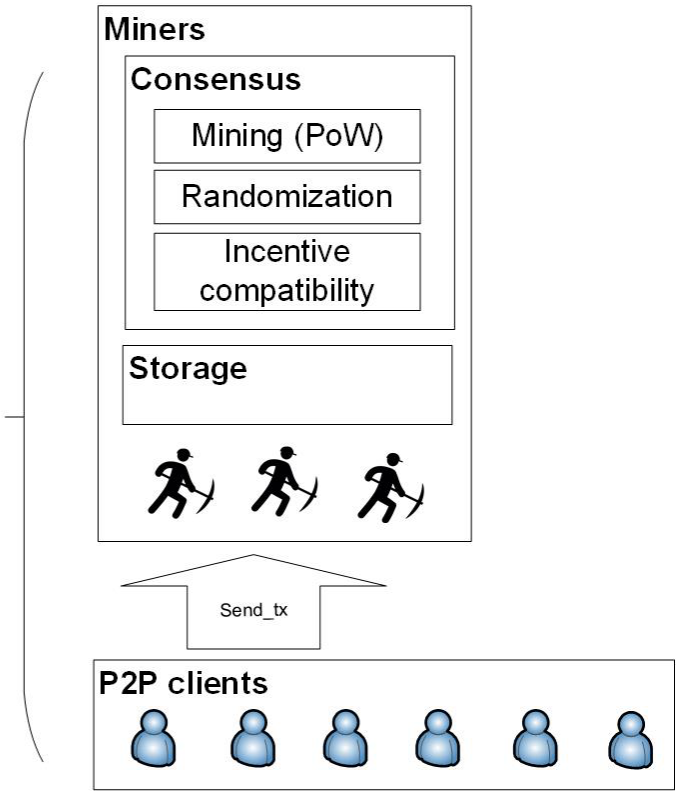
Outline

1. Introduction
2. Blockchain applications and interfaces
3. Blockchain security promises
4. **Blockchain internals** (a brief)

Blockchain internals

1. Blockchain: Immutable tx storage

2. Blockchain consensus:
   - How to add transaction to Blockchain in a decentralized way?



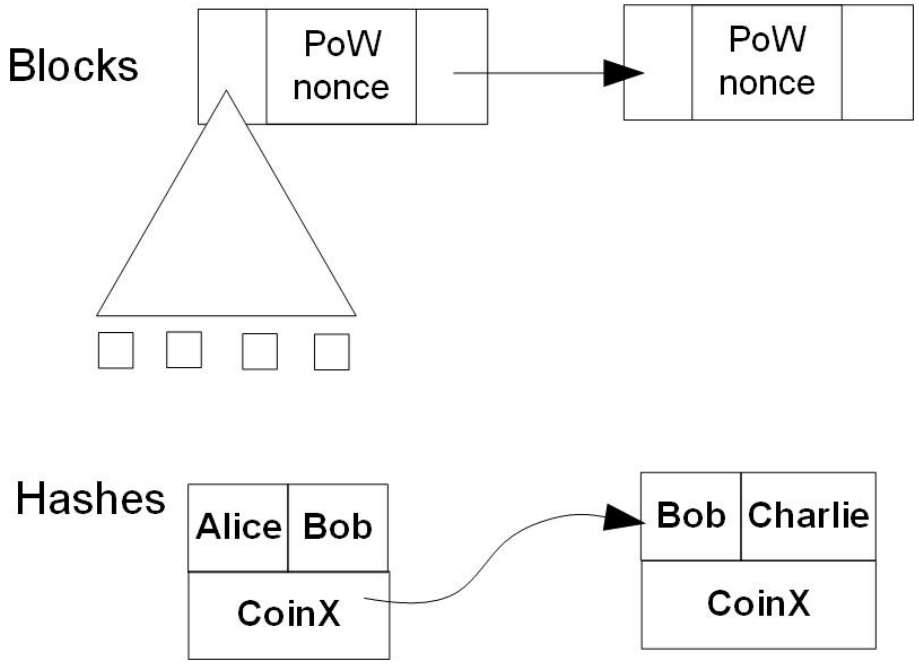
Blockchain: Immutable Tx Storage

- Create money
  - *coinX = mint.CreateCoin()*
    by ***bkc_as_mint.sign$_{mint_skey}$("CoinX is created")***
- Circulate money by transactions
  - *alice.PayCoin(bob,coinX)*
    by ***tx = alice.sign$_{alice_skey}$("CoinX is paid to Bob$_{bob_pkey}$")***
    bkc_as_visa.validate(tx)
  - Tx representation
    - How to represent coins, owner identity, ownership (binding btwn coin and identity)?

Blockchain: Immutable Tx Storage

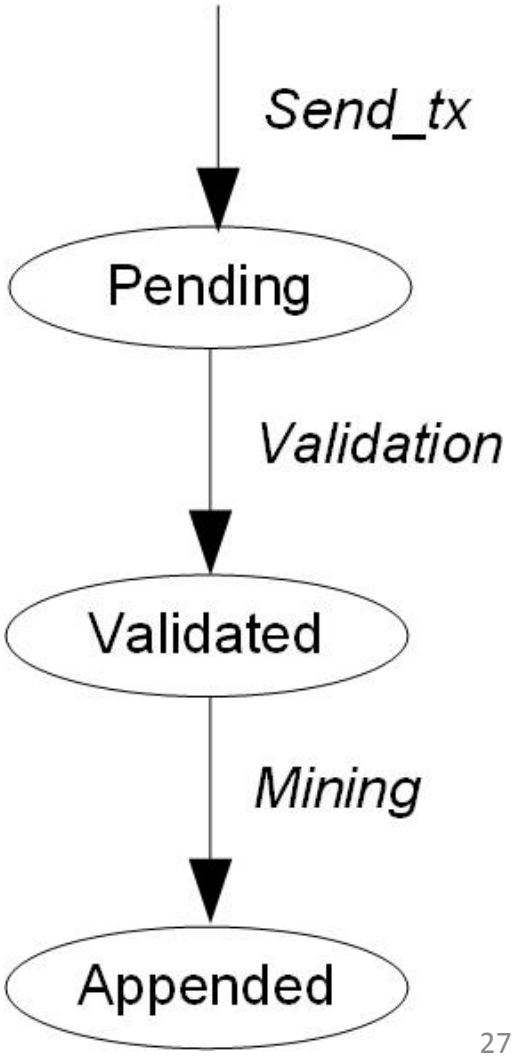
- Hash pointer: Representing coins in a tx
  - Bob's coin spent in a tx is the tx's hash pointer pointing to a prior tx where Bob receives the coin.

- Hash chain of transactions
- Block chain of transactions



Consensus

- Transaction-add workflow
  - Validation, Append
- Consensus mechanisms
  - Randomization
  - PoW mining
  - As mint: Incentive-compatibility
  - Bootstrap the trust



Q/A

Thank you!

Contact:

Yuzhe (Richard) Tang
Assistant Professor
Dept. of EECS
Syracuse University
ytang100@syr.edu
ecs.syr.edu/faculty/yuzhe