Blockchain: Systems, Security and Applications

Dr. Yuzhe (Richard) Tang

Department of EECS,

Syracuse University

May 10, 2018

Outline

A. **Introduction**

B. What's Public Blockchain?

- External views
- Internal views

C. Blockchain Models, Problems and Applications

A. Introduction: Cryptocurrency

- Cryptocurrency in the field:
  - BitCoin, Ethereum, Litecoin, etc.

Cryptocurrency that is like US Dollars

- Support conventional money flows:
  - Create money in a **mint**
  - Circulate money among owners through **transactions**
- Security under threats:
  - Threat 1: Print fake money
  - Threat 2: Double spending (digital currency)

Cryptocurrency that is unlike US Dollars

- US dollar is fiat currency controlled by autorities
  - Issued and printed in gov. mint
  - Circulated with monitoring by Visa
- Authority may not be trustworthy

SPECIAL AGRO-CHEQUE

100000000000

AA9568185

RESERVE BANK OF ZIMBABWE

Pay the bearer on demand

ONE HUNDRED BILLION DOLLARS

on or before 31st December 2008

for the Reserve Bank of Zimbabwe

Issue date: 1st July 2008

100 BILLION

Dr. G Gono
Governor

RESERVE BANK OF ZIMBABWE

100000000000

02022900

- Cryptocurrency removes **centralized authority**.

Key Ideas of Cryptocurrency

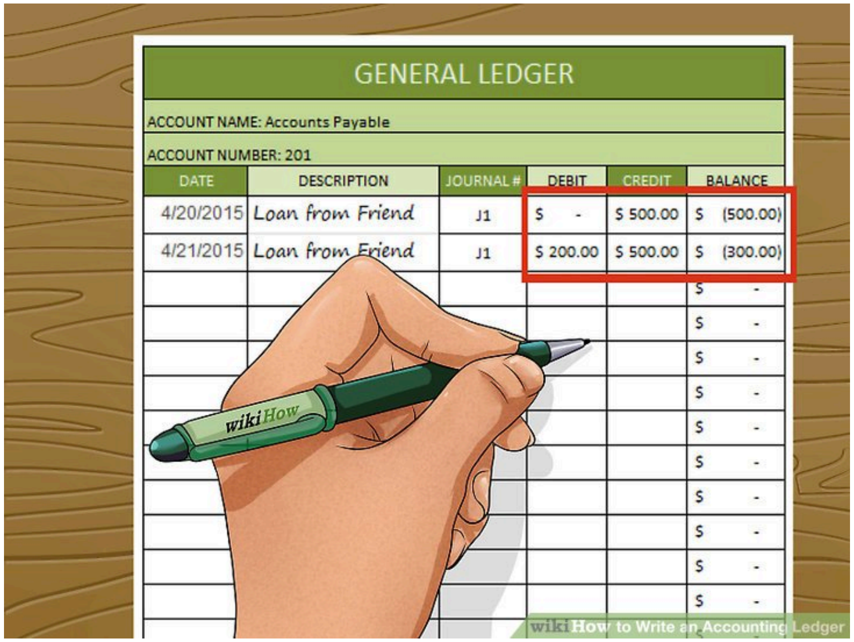
- Get rid of authority by **trust decentralization**
  - Don’t trust gov. and Visa, instead trust the entire population on planet.

- Make the network **open-membership** and transaction history **transparent**.
  - Transparency & open-membership helps network reach the planet scale.

- Automate the entire process with **incentive compatibility**.
  - Automation removes labor and reduces costs.
  - Pay people who help maintain the system.

Introduction: Cryptocurrency and Blockchain

- Blockchain is the place to record cryptocurrency transactions.
  - Blockchain is the ledger for Bitcoin
- Blockchain is the system materializing the above ideas.



GENERAL LEDGER

ACCOUNT NAME: Accounts Payable

ACCOUNT NUMBER: 201

DATE	DESCRIPTION	JOURNAL #	DEBIT	CREDIT	BALANCE
4/20/2015	Loan from Friend	J1	$ -	$ 500.00	$ (500.00)
4/21/2015	Loan from Friend	J1	$ 200.00	$ 500.00	$ (300.00)
					$ -
					$ -
					$ -
					$ -
					$ -
					$ -
					$ -
					$ -
					$ -
					$ -

Outline

A. Introduction

B. What's Public Blockchain?

- **External views**
- Internal views

C. Blockchain Models, Problems and Applications

What’s Blockchain: Overview

- Blockchain is …

What's Blockchain: Overview

- Blockchain is …
  1. A transaction storage system

What’s Blockchain: Overview

- Blockchain is …
  1. A transaction storage system
  2. A cryptocurrency mine
  3. A program-execution platform

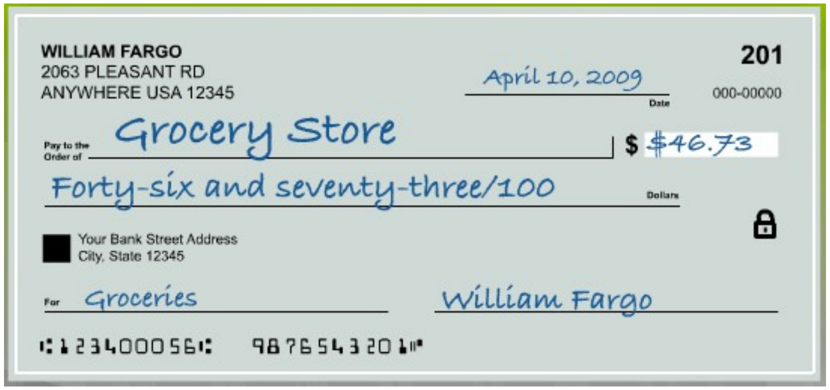
What's Blockchain: Overview

- Blockchain is …

1. A transaction storage system
2. A cryptocurrency mine
3. A program-execution platform
4. A consensus protocol
5. A proof system
6. Many other things

1. Blockchain as Transaction Storage

- Interface:
  - *sendTransaction({from:account1, to:account2, value: amount})*
  - *getTransaction(txid)*



WILLIAM FARGO
2063 PLEASANT RD
ANYWHERE USA 12345

201

April 10, 2009
Date

000-00000

Pay to the Order of Grocery Store $ $46.73

Forty-six and seventy-three/100 Dollars

Your Bank Street Address
City, State 12345

For Groceries William Fargo

⑆123400056⑆ 9876543201⑈

- Scenario:
  - Get your first bitcoin through exchange/wallet service

coinbase CoinDesk

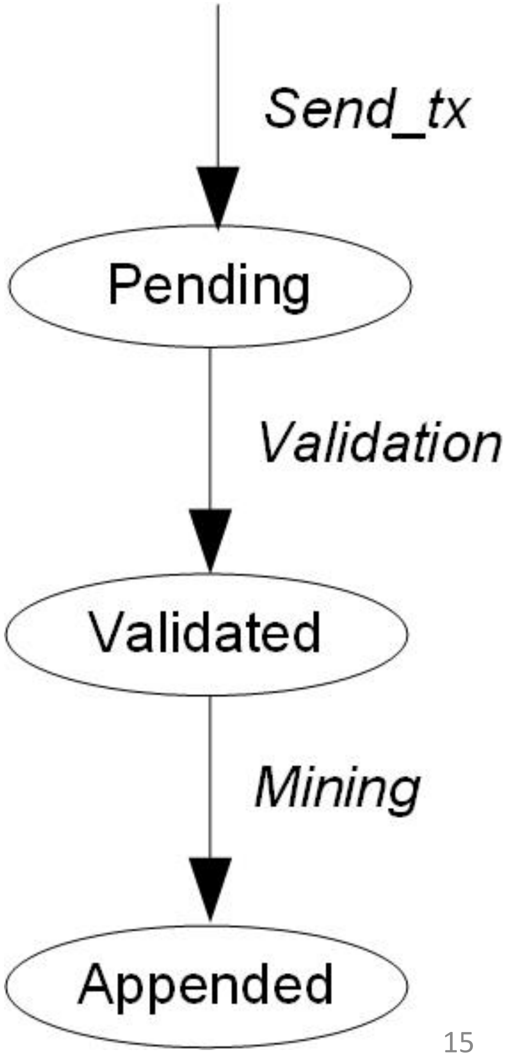
Security of Transaction Storage

- Blockchain as transaction storage
  - Readable to the public (**transparency**)
  - Appendable by honest clients sending **valid** transactions
  - Once committed, cannot be modified (**immutability**)

- Transaction validity: No double spending
  - After Alice pays Bob coinX, Alice can't spend coinX.

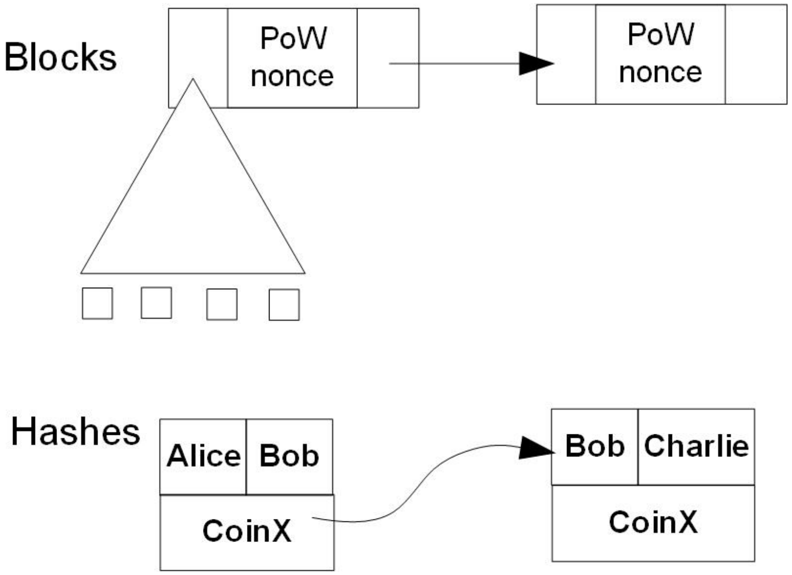
Internal of Transaction Storage

- Add-transaction flow
  - Recently sent txs broadcast and buffered in memory pools.
  - Pending txs are validated
    - Ensuring no double-spending
  - Append txs to Blockchain
    - Validated txs are grouped to blocks
    - Blocks are appended to the blockchain.



Internal of Transaction Storage

- Transactions form a DAG
  - Hash pointer: Represent spending relationship btwn txs
- Transaction DAG (100GB) is stored in the Blockchain network.
- Blocks (32 MB) are chained and replicated in the Blockchain network.



- Immutability is ensured by
  - Security of hash (collision resistance)
  - Blocks are replicated.

2. Blockchain as a Mine

- Like gold mine, the Blockchain will give valuables (in Bitcoins) to people who put efforts in.

- Scenarios: You purchase some hardware and run some (non-sense) computations
  - With some probability, your computation will be rewarded in BitCoin
  - The probability depends on how powerful your hardware is and how many others are competing

2. Blockchain as a Mine

- How likely it is to get BitCoin thru. mining?
  - – How big is your budget?
    - Constant capital: buy machines, Variable capital: electricity consumption
  - – Who you are up against (racing to win the reward)?
    - State-level miners, bitcoin farm, data centers

Security: Sybil Attack Resilience

- Open-membership network: anyone can join
- Honest majority miners: Security assumption
- Sybil attack
  - An individual can create a large number of miners to become and control the majority of network.
- Mining: Make it hard to do Sybil attack.
  - Having a miner win consumes resources.
  - Having many miners win consumes so many resources that an (adversarial) individual cannot afford.

3. Blockchain as Program-Execution Platform

- Programming interface: **Smart contract**
  - Smart-contract program is an executable running on the Blockchain network
  - Examples:

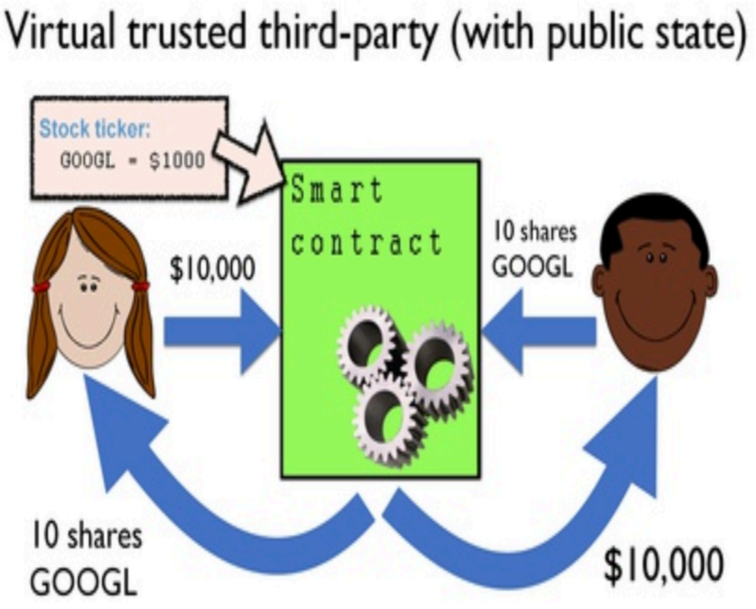
Ethereum Solidity

Solidity is designed to compile to coc
for the Ethereum Virtual Machine.

Chaincode (Smart Contract)

3. Blockchain as Program-Execution Platform

- Common use of smart contract:
  - Decision-making logic (IFTTT)
    - When to send tx, who can spend the tx
  - General program (Turing complete language on chain)
- Application: Stock-exchange
  - Alice will trade 10 shares for $10,000 when the stock price is below $1000.
    - (BitCoin can represent both $10K and shares as digital goods)



Acknowledge: Prof. Ari Juels

Security: Unstoppable Execution

- Security properties:
  - Autonomously executed, unstoppable
  - Transaction fairness:
    - If I paid you, to be fair, I need to receive your goods.
    - Replace the role of conventional banks in a supply chain.
- Internally, it is ensured by
  - Replicated execution
  - Honest majority

Outline

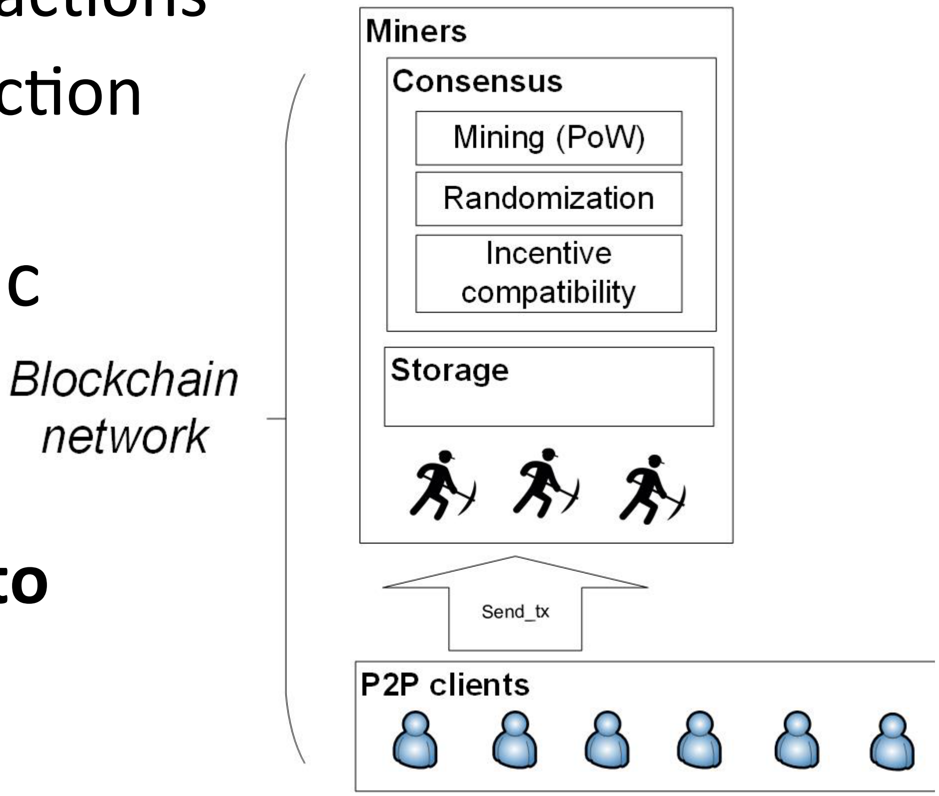
A. Introduction

B. What's Public Blockchain?
   - External views
   - **Internal views**

C. Blockchain Models, Problems and Applications

Internal-Mechanism Overview

1. Blockchain is a P2P network of two layers
   - Clients send/read transactions
   - Miners maintain transaction storage
2. Miners run add-tx logic
   1. Broadcast pending txs
   2. Validate txs
   3. **Append validated txs to Blockchain**



Outline

A. Introduction

B. What’s Public Blockchain?

- External views
- Internal views

C. **Blockchain Models, Problems and Applications**

Alternative Blockchain Models

- Private/Permissioned blockchain
  - Quorum from JP Morgan Chase, Hyperledger from IBM
  - Runs in a consortium of miners (closed network)
- Privacy-preserving Blockchain
  - zCash/zeroCash: encrypted transactions

- They feature: closed-membership, private transactions, private contract state.

Big Problems of Blockchain Today

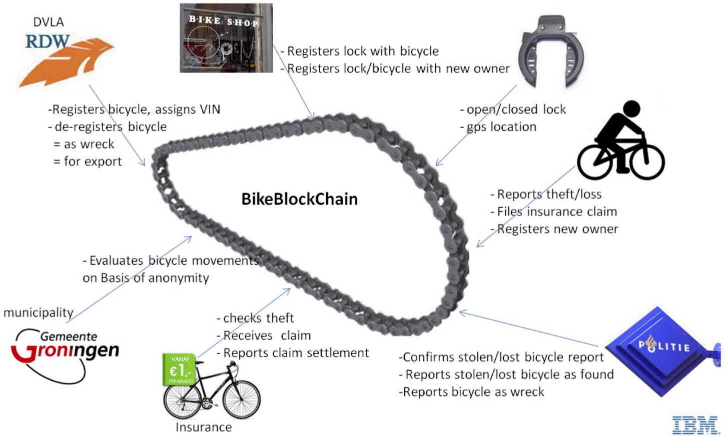
- **Energy** consumption by PoW
- **Scalability**
  - bounded by block size and mining rate.
- Computing power **centralization**
  - Mining pool
- **Cyber-crime** through cryptocurrency
- **Privacy** leakage thru. side channels

Blockchain Applications Beyond Bitcoins

- DNS servers
  - Blockstack
- Personal key managment
  - Keybase.io,
- Identity management
  - International travelling and Canadian border control
- Service discovery in VMWare
- Incentivized fitness
  - Fry Egg
- Streamlined incident reporting
  - BikeBlockchain

blockstack

FRY EGG



- Registers lock with bicycle
- Registers lock/bicycle with new owner

-Registers bicycle, assigns VIN
- de-registers bicycle
 = as wreck
 = for export

- open/closed lock
- gps location

- Reports theft/loss
- Files insurance claim
- Registers new owner

- Evaluates bicycle movements
on Basis of anonymity

- checks theft
- Receives claim
- Reports claim settlement

-Confirms stolen/lost bicycle report
- Reports stolen/lost bicycle as found
-Reports bicycle as wreck

What's Next?

- Online Blockchain Labs at Syracuse Univ.:
  - https://goo.gl/hFmfQc

- SEED workshop in May, 2018 in Syracuse, NY
  - An education workshop for college and high-school teachers
  - http://www.cis.syr.edu/~wedu/seed/workshop.html

- Blockchain course
  - CIS 600 & FIN 600: Blockchain and Cryptocurrencies (in Fall, 2018, at SU)
    - http://tristartom.github.io/docs/syl-4600.pdf
    - Other online materials

Q/A

Thank you!

Contact:

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