CS 5594: Blockchain Technologies

Blockchain Overview

Peng Gao
Assistant Professor

Spring 2022

Part of materials are derived from Prof. Thang Hoang’s SP 2021 course
Course Info Updates

• Course webpage: https://people.cs.vt.edu/penggao/resources/teaching/sp22/cs5594/index.html

• Office hours:
  – Instructor: Friday, 2:00pm EST – 2:45pm EST, Zoom
  – TA, Han Liu: Monday, 2:00pm EST – 3:00pm EST, Zoom
  – TA, Waad Aldndni: Wednesday, 3:00pm EST – 4:00pm EST, Zoom

• Project:
  – Single-person project encouraged; maximum 3 students per group; need to specify contribution of individual member in reports
  – Send your team info (name, email, ID) to both TAs with the subject line “CS5594_SP22_Project_Team_Info” by January 30
    ▪ Can coordinate on Canvas to find teams
    ▪ Register your team info on Canvas -> People -> Group
  – Project idea due: February 6
    ▪ One page summary describing the motivation and key ideas/proposed contributions (what you want to do & why you want to do it)
  – All reports and paper summaries will be submitted on Canvas

• Class attendance will be recorded using Zoom user meeting report (https://www.nyit.edu/files/ctl/CTL_TeachingWithTechnology_ZoomMeetingParticipants_2014.pdf) starting from Week 3
Outline

• Traditional Transaction Model and Issues
• Traditional Trust Models and Issues
• Why Blockchain?
• What Is Blockchain?
• Essential Blockchain Concepts You Need to Know
Outline

• Traditional Transaction Model and Issues
  • Traditional Trust Models and Issues
  • Why Blockchain?
  • What Is Blockchain?
• Essential Blockchain Concepts You Need to Know
**Traditional Transaction Model**

**Send(Alice, $10K)**

<table>
<thead>
<tr>
<th>Account #</th>
<th>Name</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>32136544</td>
<td>Bob</td>
<td>$100,000</td>
</tr>
<tr>
<td>32136545</td>
<td>Doge</td>
<td>$500,000</td>
</tr>
<tr>
<td>32136546</td>
<td>Eve</td>
<td>$700,000</td>
</tr>
</tbody>
</table>

**Transaction records**

**Ledger A**

<table>
<thead>
<tr>
<th>Account #</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>32136544</td>
<td>32136521</td>
<td>- $60,000</td>
</tr>
<tr>
<td>32136544</td>
<td>32136521</td>
<td>+ $200,000</td>
</tr>
<tr>
<td>32136554</td>
<td>32136521</td>
<td>- $10,000</td>
</tr>
</tbody>
</table>

**Ledger B**

<table>
<thead>
<tr>
<th>Account #</th>
<th>Destination</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>32136521</td>
<td>32136544</td>
<td>+ $60,000</td>
</tr>
<tr>
<td>32136521</td>
<td>32136544</td>
<td>- $200,000</td>
</tr>
<tr>
<td>32136521</td>
<td>32136544</td>
<td>+ $10,000</td>
</tr>
</tbody>
</table>
Issues of Traditional Transaction Model

• Centralized systems have many issues
  – Single point of failure
    ▪ System attacks, hacks
    ▪ Prone to errors
  – Require trust
    ▪ Counterparty risk/fraud
  – Security and privacy issues
  – Operational cost to maintain trusted third parties
Outline

• Traditional Transaction Model and Issues
• **Traditional Trust Models and Issues**
• Why Blockchain?
• What Is Blockchain?
• Essential Blockchain Concepts You Need to Know
What Is Trust?

- All decisions we make everyday are based on a degree of trust
  - Driving car, online purchase, buying a house
- Trust reduces operational cost and improves efficiency of our society
  - Without trust, one must verify the reliability of everything
  - However, impossible to verify everything
- Trust is gray-scale
  - Full trust, semi-trust, weak trust
- Trust is a complex psychological state combined with rational and emotional factors
  - “Trust begins where prediction ends.” – Trust as a Social Reality, J. David Lewis and Andrew Weigert
Traditional Trust Models

- Three trust architectural models
  - **P2P (peer-to-peer):** I trust you because of you
    - Trust counterparty
  - **Leviathan:** I trust you because of legal contracts established by trusted authorities
    - Trust dispute resolution mechanism (CA)
  - **Intermediary:** I trust you because of trusted platform we both operate on
    - Trust intermediary
A Crisis of Trust

• Trust forms the ways we interact and behave
  – High-trust societies are powerful and outperform low-trust societies

• However, trust is in crisis!
  – Americans’ declining trust in the government and in each other

A Crisis of Trust

“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”

- Satoshi Nakamoto
A Crisis of Trust

• Trust fails because of:
  – **Direct violation**: non-reputable organization
  – **Opportunistic behavior**: When benefits outweigh trust factors
    ▪ Facebook-Cambridge Analytica scandal
  – **Systematic collapse**: Unwanted behaviors (compromised, corrupted)
    ▪ Data breaches in Equifax, Apple iCloud, Sony PlayStation Network

Extremely hard to restore/recover trust when it fails

New model of trust?
Outline

• Traditional Transaction Model and Issues
• Traditional Trust Models and Issues
• Why Blockchain?
• What Is Blockchain?
• Essential Blockchain Concepts You Need to Know
Blockchain: A Revolution of Trust

• **Blockchain: a revolution of trust**
  – “Trustless trust” – Reid Hoffman (Co-founder of LinkedIn)
  – A trusted network without trusting anyone (counterparty, CA, intermediary)
Blockchain: A Revolution of Trust

- **Blockchain**: An open network where everybody can establish trust themselves
  - **Decentralized**: Trust distributed across multiple entities
    - No central authority
    - No single point of failure
    - Reduced operational cost
  - **Open**: Anyone can participate and verify the integrity and trustworthiness
  - **Anonymity**: Everybody is equal and his/her identity remains hidden
    - Eliminate impacts of counterparty identity in justifying the trustworthiness
  - **Enhanced confidentiality, integrity, and privacy**
Blockchain: A Revolution of Trust

• Blockchain establishes trust via software programs
  – Decentralized platform with reward incentive mechanisms
    ▪ Encourage honest and trustworthy behavior of many participants
  – Smart contract with pre-defined algorithms
    ▪ Dispute resolution

• In blockchain network, nothing to be trustworthy except its output

• All transactions validated via rigorous mathematical proofs (--- cryptographic primitives)
  – Anybody can verify proofs publicly

In Proof We Trust
Why Blockchain (Nice Properties)?

- **Enhanced security and reliability**
  - Via decentralization model and cryptography
  - Centralization is more vulnerable to corruptions, errors, mistakes

- **Tamper-proof**
  - Data alteration remains extremely difficult

- **Digital freedom**
  - Complete anonymity and transaction security and confidentiality
  - Transactions direct to recipients without routed to centralized trusted authority (e.g., bank)

- **Improved transparency**
  - Everybody can verify and track transactions
  - Nobody can modify transactions on their own

- **Better efficiency and reduced cost**
  - Automated process
  - Minimal transaction cost
  - No need of maintaining central authority
Blockchain Evolution

- **2008**: BTC Genesis block created
- **2009**: First BTC transaction (10,000 BTC for a pizza)
- **2010**: Silk Road launched
- **2011**: Frauds and attacks explored on Bitcoin
- **2012**: Devastating attacks on Mt.Gox, BTC price cratered
- **2013**: Bugs in ETH DAO code exploited
- **2014**: ETH Genesis block created
- **2015**: Linux unveils Hyperledger, BC protocol for decentralized apps
- **2016**: 1 BTC = 1 USD
- **2017**: 1 BTC = 100 USD
- **2018**: 1 BTC = 10,000 USD
- **2019**: Mainstream Adoption: Government, Central Banks
- **2020**: Widescale Adoption: Life Sciences, Healthcare, Supply chains, Energy resources

- **ORIGIN**: Bitcoin
- **TRANSACTIONS**: Paypal, MS accept BTC payment
- **LEGALIZATION**: Frauds and attacks explored, Mt.Gox
- **APPLICATIONS**: Bugs in DAO, DApps
- **Legalization**: Linux unveils Hyperledger, new BC protocol for decentralized apps
Outline

• Traditional Transaction Model and Issues
• Traditional Trust Models and Issues
• Why Blockchain?
• What Is Blockchain?
• Essential Blockchain Concepts You Need to Know
What Is Blockchain?

• First, Bitcoin is **NOT** blockchain
  – Bitcoin is a digital currency that uses blockchain as the underlying data structure

• Blockchain is a **data structure** where data blocks are linked together

• Data blocks in the chain cannot be deleted or altered (**Immutability**)
What Is Blockchain?

• Blockchain is a comprehensive system consisting of:
  – Transactions
  – Immutable ledgers
  – Decentralized network
  – Data encryption/decryption
  – Consensus mechanisms
  – Smart contracts
What Is Blockchain?

- Blockchain permits **transactions** to be gathered and recorded in the **block**
- Blocks are chained in chronological order via **cryptographic hash**

Alice pays Bob 3 BTC ✓
Bob pays Chris 2 BTC ✓
Eve pays Alice 5 BTC ✓
Reward myself 1 BTC
How Blockchain Works?

In digital transaction…

Bob wants to send money to Alice

The transaction Tx is represented as a block

Bob

The block is broadcast to all the distributed nodes in the network

Sufficient nodes verify and approve the transaction

Alice receives the money

Tx is appended to blockchain

Alice
## Types of Blockchain

- **Public** and **private**
- Many mechanisms in public blockchain are not needed in private blockchain

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Public blockchain</th>
<th>Private blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Anyone can read/write</td>
<td>Only private group can read/write</td>
</tr>
<tr>
<td>Authority</td>
<td>Decentralized</td>
<td>Partially Decentralized</td>
</tr>
<tr>
<td>Tx Speed</td>
<td>Slow</td>
<td>Fast</td>
</tr>
<tr>
<td>Consensus</td>
<td>Permissionless</td>
<td>Permissioned</td>
</tr>
<tr>
<td>Identity</td>
<td>Anonymous</td>
<td>Known</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Immutability</td>
<td>Full</td>
<td>Partial</td>
</tr>
</tbody>
</table>

**Examples**: Bitcoin, Ethereum, Ripple, Quorum, Hyperledger
Outline

• Traditional Transaction Model and Issues
• Traditional Trust Models and Issues
• Why Blockchain?
• What Is Blockchain?
• Essential Blockchain Concepts You Need to Know
Blockchain Transactions

- Smallest element
- Record every decision and action taken
- Proof of history, provides provenance
Blockchain “Block”

• A block contains multiple transactions
  – Transaction is immutable/indelible
• Write and read-only
• Once a block is chained, it is extremely difficult to change
  – Modification possible
  – Rework on all the subsequent blocks and consensus for each block
Chain of Blocks

- A chain contains multiple blocks
- Blocks linked using cryptographic hash
- An instance of distributed ledger
Distributed Network

- Blockchain operates on a decentralized/distributed P2P network
- Each node stores a copy of the ledger
  - Distributed ledger

Centralized Network
- Nodes interact with a single central node

Distributed Network
- Nodes interact with some central nodes

Decentralized Network
- Nodes interact with each other directly
Distributed Ledger

- **Blockchain is a distributed ledger**
  - **Centralized ledger**: stored by a central node
  - **Distributed ledger**: stored in every node
    - All nodes agree on the true state of the ledger (via a consensus protocol)

Alice pays Bob 3 BTC
Bob pays Chris 2 BTC
Eve pays Alice 5 BTC
Distributed Ledger

• Keep track of all transactions performed in the network
• Can be encrypted for confidentiality
• Can be used by individuals without a central authority
• Immutable: Ledger records are extremely difficult to be altered
  – Changing a record in the ledger requires a consensus from all participants
  – Rework an all subsequent records
Distributed Consensus

- Ensure the blocks in blockchain are valid and truthful
- Prevent malicious adversaries from system compromise and chain-forking
- Many consensus protocols, each with different pros and cons
  - Proof of Work (PoW), Proof of Stake (PoS), Proof of Elapsed Time (PoET), Proof of Activity (PoA), Proof of Burn (PoB)
  - Paxos, PBFT, Streamlet

We will discuss many of these consensus protocols
Smart Contract

- A computer program **stored on a blockchain** that run when predetermined conditions are met
  - Control the transfer of digital assets between parties
  - A “contract” that can **automatically** execute
- Enable broader blockchain applications beyond cryptocurrencies
  - Decentralized applications (**DApps**)
- Can run in a **secure environment** to preserve confidentiality of blockchain transactions
  - Running in a **Trusted Execution Environment (TEE)**
  - Confidential smart contracts

Source: https://blockgeeks.com/guides/smart-contracts/
Smart Contract

• Smart contract is a computer program that:
  – Defines rules
  – Enforces obligations and penalties
  – Executes actions required by clauses
  – Autonomous without ownership

• Written in a high-level programming language (e.g., Solidity)

<table>
<thead>
<tr>
<th>Blockchain Techniques</th>
<th>Smart Contracts?</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>✗</td>
<td>C++</td>
</tr>
<tr>
<td>Ethereum</td>
<td>✓</td>
<td>Solidity</td>
</tr>
<tr>
<td>Hyperledger</td>
<td>✓</td>
<td>GoLang, C++, etc.</td>
</tr>
</tbody>
</table>
Encryption

• Confidential transaction
• Prevent sensitive information to be leaked to malicious attacker
• Blocks can be partially or fully encrypted
  – Symmetric/asymmetric encryption
• Some (private) blockchains employ access control for visibility
Challenges

• Energy consumption
• Resource-wasteful
• Scalability
• Standardization
  – Limited interoperability
• Awareness and understanding
• Interaction with legacy infrastructure
Summary

- Blockchain is interdisciplinary
- **Distributed systems** and **cryptography** are fundamental building blocks

---

<table>
<thead>
<tr>
<th>Operation</th>
<th>Crypto Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init &amp; Broadcast Transactions</td>
<td>• Digital Signature</td>
</tr>
<tr>
<td></td>
<td>• Private/Public Keys</td>
</tr>
<tr>
<td>Transaction Validation</td>
<td>• Proof-of-Work</td>
</tr>
<tr>
<td>Chaining blocks</td>
<td>• Hash Function</td>
</tr>
</tbody>
</table>
Key Things to Remember

• Blockchain revolutionizes the trust
• Blockchain is a distributed ledger that records the provenance of a digital asset
• Blockchain is based on some key technologies
  – Distributed systems: P2P, consensus (e.g., PoW)
  – Cryptography: hash, digital signature,
  – Smart contracts
• Blockchain is fast-evolving with new concepts and techniques
• Blockchain can transform many fields beyond financial services
• “Blockchain + X” provides many research opportunities
Some Important Questions

• Does blockchain network follow the CAP theorem?
• Can anonymity lead to money laundering?
• How is blockchain different from P2P?
• How to identify a block in the blockchain?
• How many transactions in a block?
• How are transactions organized in a block?
• What is a node on the blockchain?
• How is a block generated? What is the miner and how are miners different from nodes?
• Do I need to be a node/miner to use Bitcoin? Do I need to run a Bitcoin full node?
• How does one know the transaction is made by the rightful owner?
Thanks!