SEC-205: Distributed Ledger and Blockchain

Lecture 1 – Introduction to Distributed Ledger and Blockchain

Instructed By:

Dr. Charnon Pattiyanon

Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer
Engineering (AICE) Program

Today’s Outline

- In today’s lecture, we will explore and learn about:
  - What is distributed ledger?
  - What are the differences between centralized and distributed ledgers?
  - What is Bitcoin and cryptocurrency?
  - What is Bitcoin’s blockchain?
  - How does Bitcoin’s blockchain work?

What is a Ledger?

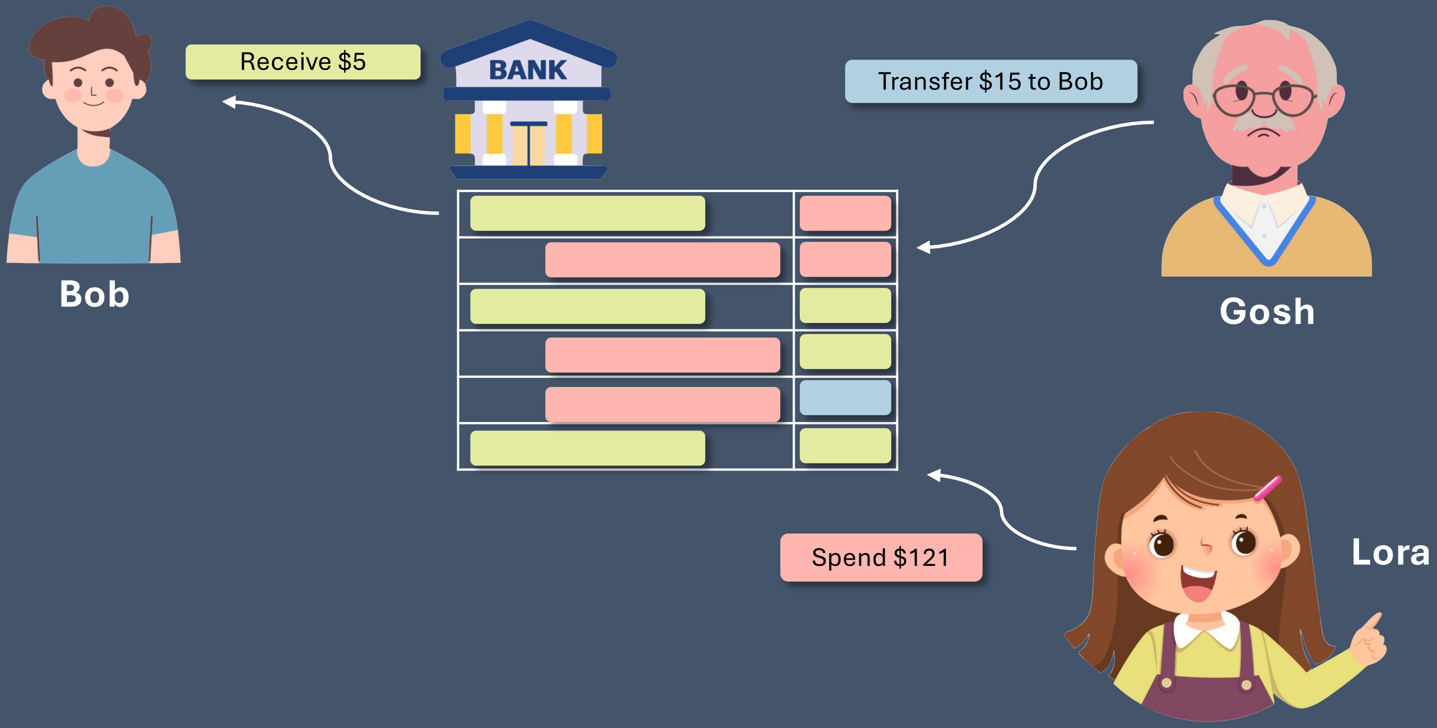
- A ledger is a record of a business's financial **transactions**.
- It summarizes all the **revenue** and **expenses** of the business, plus the **debts** owed and **assets** owned.

A General Ledger or Account

Transactions	Balance
Jack opens an account with $100	$100
Jack pays $15 for a food delivery	$85
Jack purchases an office supply for $65	$20
Jack pays $45 for a credit card from last month	($25)
Jack sells a product for $25	$0

What is a Ledger?

- Normally, the ledger is **centralized** and managed by **an authority**, like a bank.

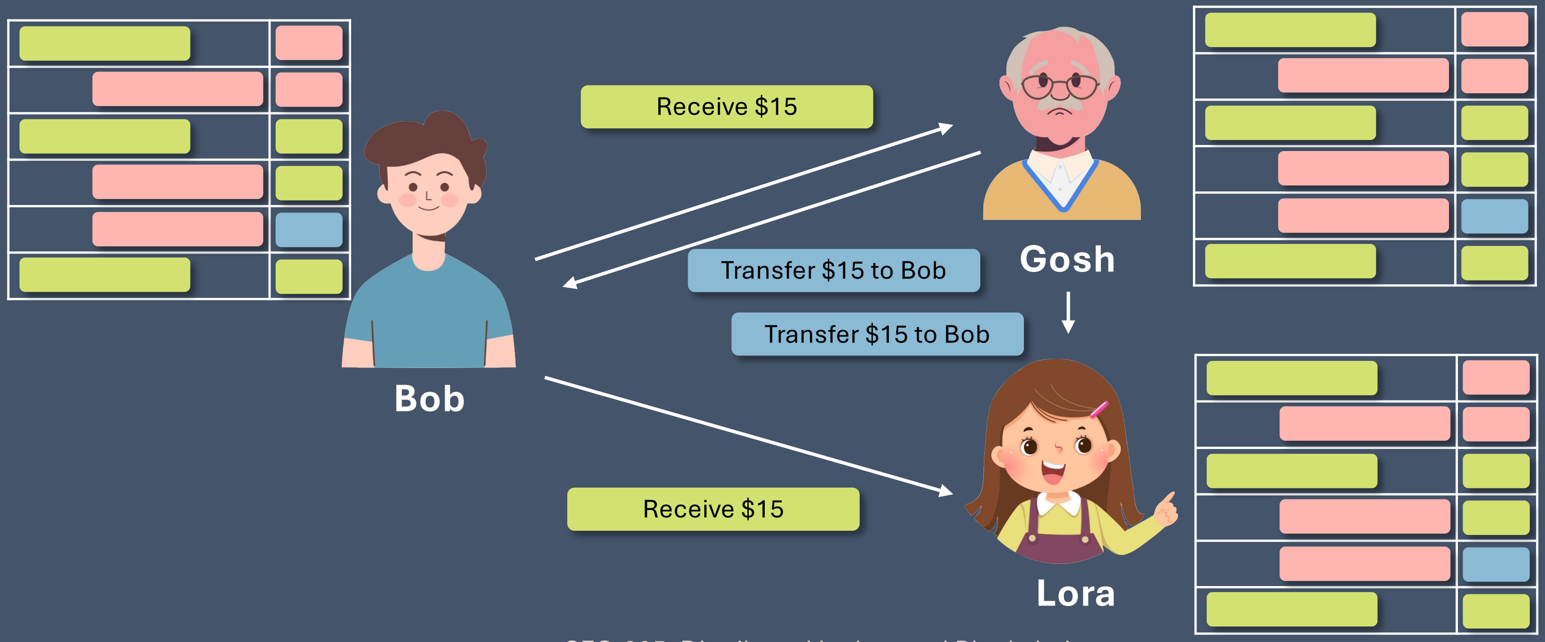


Problems of Centralized Ledgers

- Relying on an authority (e.g., Bank) to hold and manage a centralized ledger may expose some risks and problems:
  - **Single Point of Failure** – An authority will be set as a target of adversaries and it can be exploited easily.
  - **Require High Availability** – As everyone relies on the operation of the authority, their operational services must always be available whenever users need.
  - **High Cost** – Normally, authorities require some service and operational fees to maintain the ledger in a form of transaction fees. Although the fee seems to be a small amount of money, it can be piled up to a large amount when there are many transactions.

What is a Distributed Ledger?

- To address the problems with centralized ledgers, a new concept of distributed ledger was introduced by leveraging the **peer-to-peer network** capabilities.
  - It is simply the **distribution** of ledger management to **individuals**.

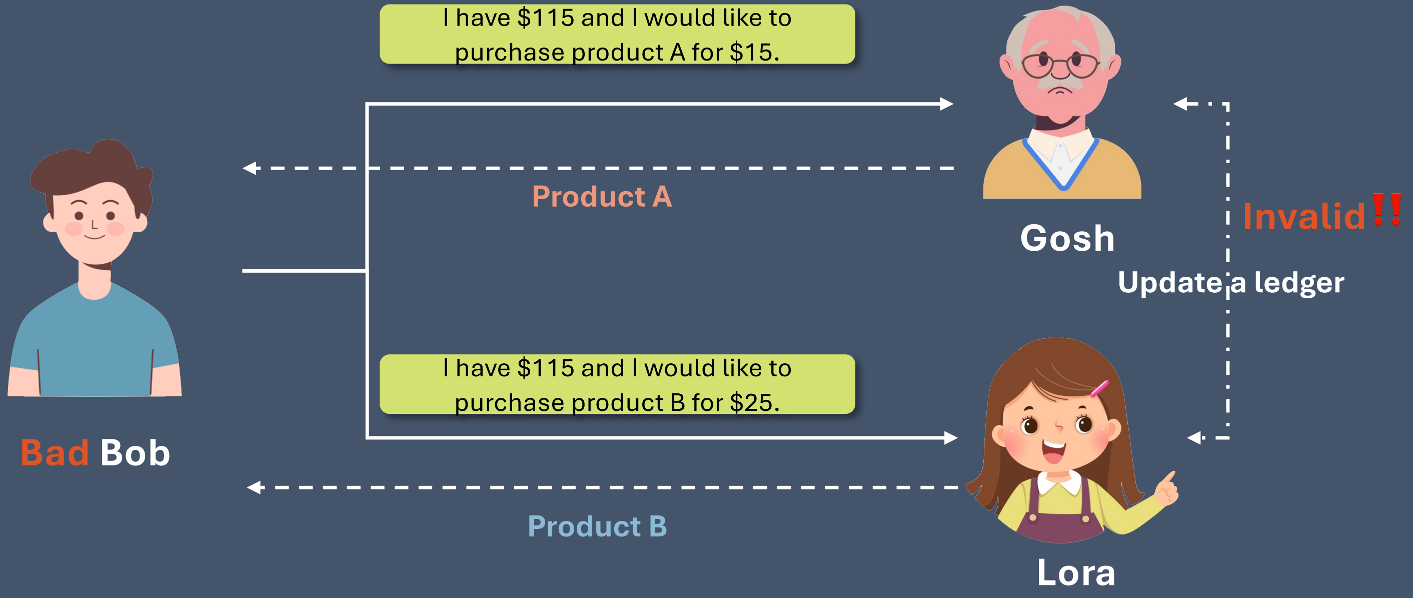


Problems of Distributed Ledgers

- Distributing the management of ledgers to individuals solves some problems with the centralized ledger, but it introduces other problems:
  - **Single Point of Failure**
  - **Require High Availability**
  - **High Cost** – Cost is transferred to individual to handle and maintain ledgers.
  - **Network Isolation** – If some individuals who hold a ledger got isolated by the network connectivity, it is hard to maintain consistency and integrity of the distributed ledger.
  - **Double Spending** – A dishonest individual can duplicate a transaction or money to spend with two or more receivers.
  - **Consensus Unreachable** – Some dishonest individuals change the ledger.

Double Spending Problem

- **Double Spending** – A dishonest individual can duplicate a transaction or money to spend with two or more receivers.


I have $115 and I would like to purchase product A for $15.
Product A
Gosh
Invalid!!
Update a ledger
Bad Bob
I have $115 and I would like to purchase product B for $25.
Product B
Lora

This is the reason why distributed digital cash systems are not practical.

Byzantine Generals Problem

Ref: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

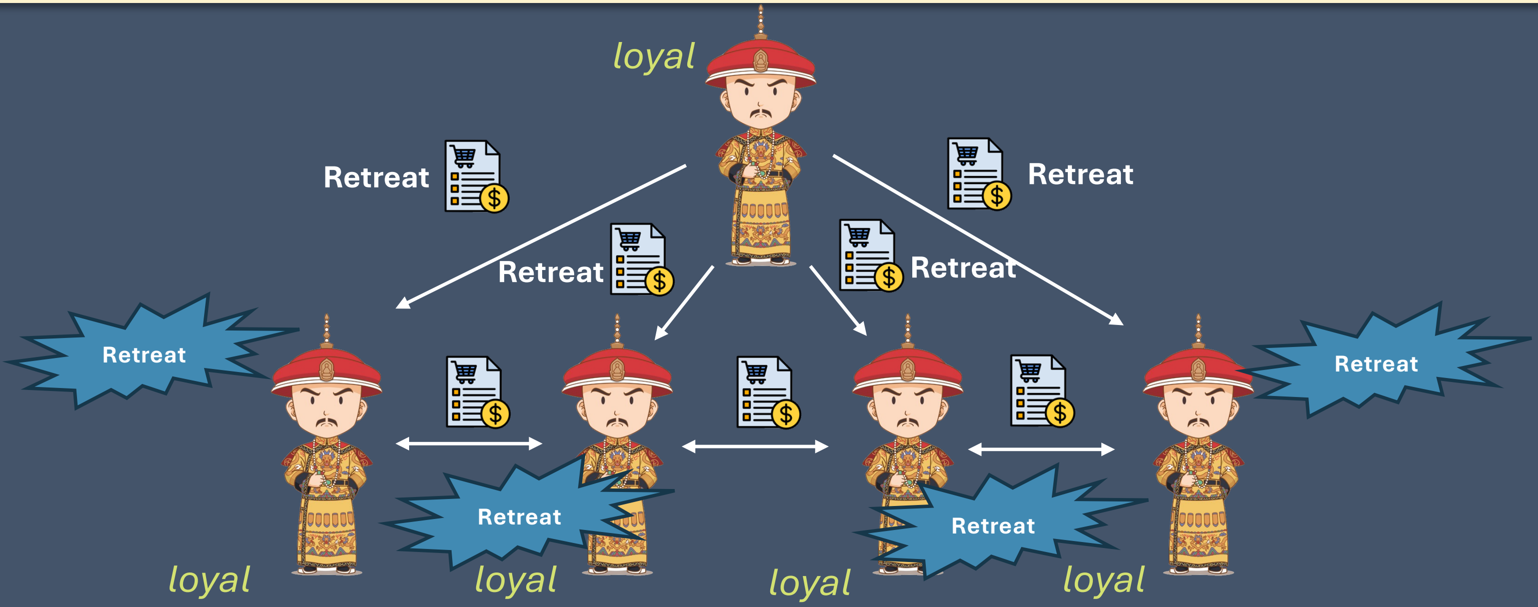
- BGP was introduced by Lamport et al., in 1982.
- Demonstrate the problem of ***reaching consensus*** between distributed entities.
- **Problem Statement:**

- There are n generals (where n is fixed), one of which is the ***commander***.
- Some generals are *loyal*, and some of them can be *traitors* (including the commander).
- The commander sends out an order that is either ***attack*** or ***retreat*** to each general.
- If the commander is *loyal*, it sends the same order to all generals.
- All generals take an action after some time.

Byzantine Generals Problem

Ref: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

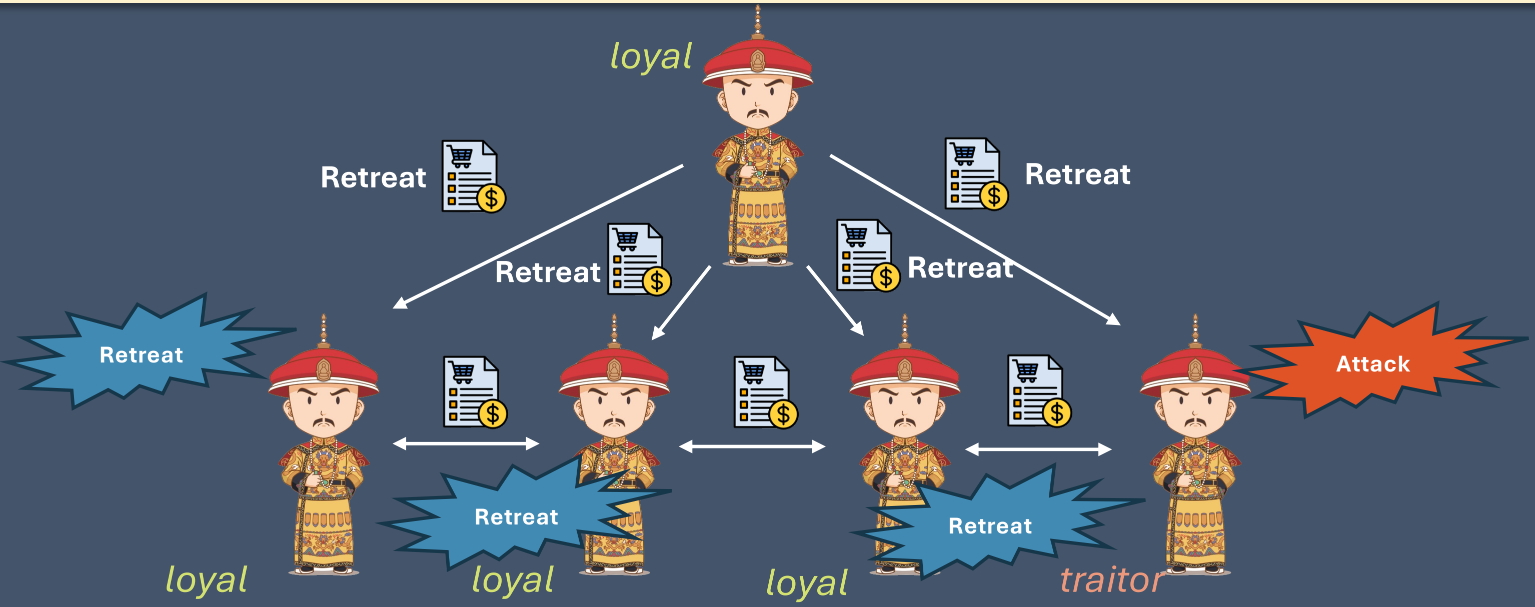
- **Goal:**
  - **Agreement:** ***No*** two *loyal* generals take ***different*** actions.
  - **Validity:** If the commander is *loyal*, then all *loyal* generals must take the action ***suggested by the commander***.
  - **Termination:** All *loyal* generals must eventually take some action.



Byzantine Generals Problem

Ref: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

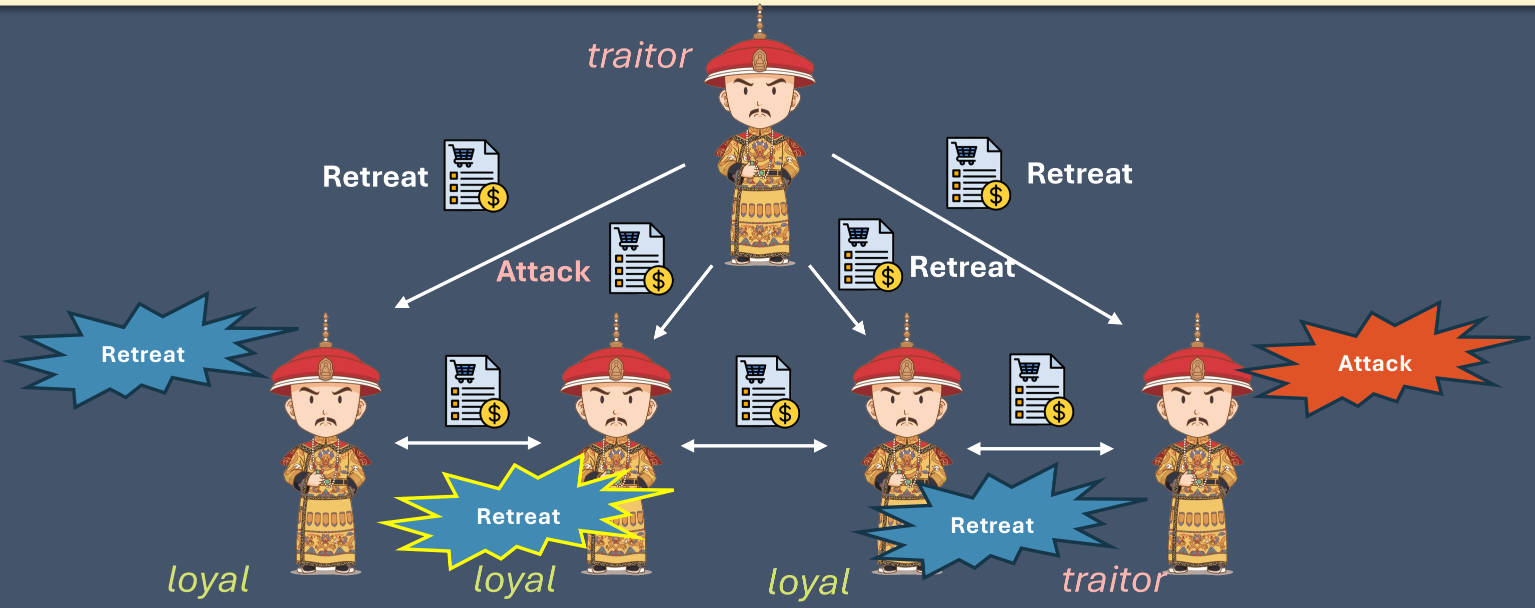
- **Goal:**
  - **Agreement:** ***No*** two *loyal* generals take ***different*** actions.
  - **Validity:** If the commander is *loyal*, then all *loyal* generals must take the action ***suggested by the commander***.
  - **Termination:** All *loyal* generals must eventually take some action.



Byzantine Generals Problem

Ref: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

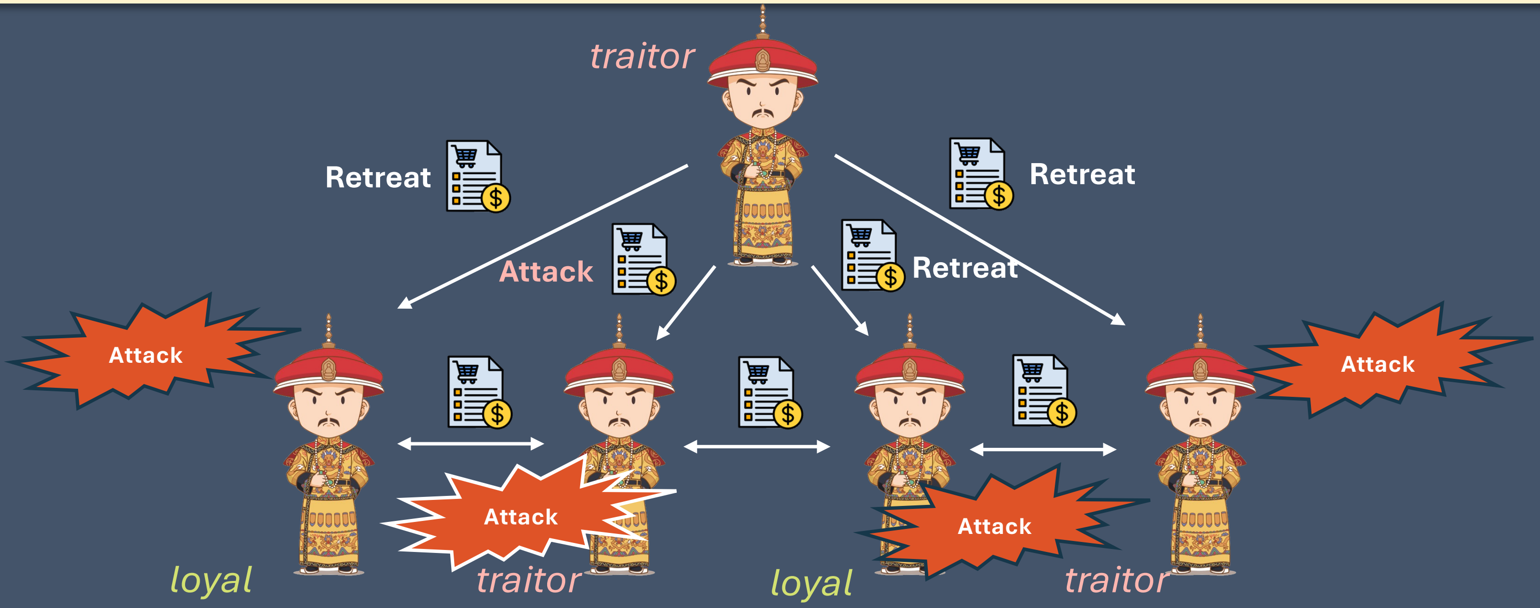
- **Goal:**
  - **Agreement:** ***No*** two *loyal* generals take ***different*** actions.
  - **Validity:** If the commander is *loyal*, then all *loyal* generals must take the action ***suggested by the commander***.
  - **Termination:** All *loyal* generals must eventually take some action.



Byzantine Generals Problem

Ref: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

- Goal:
  - Agreement: ***No*** two *loyal* generals take ***different*** actions.
  - Validity: If the commander is *loyal*, then all *loyal* generals must take the action ***suggested by the commander***.
  - Termination: All *loyal* generals must eventually take some action.



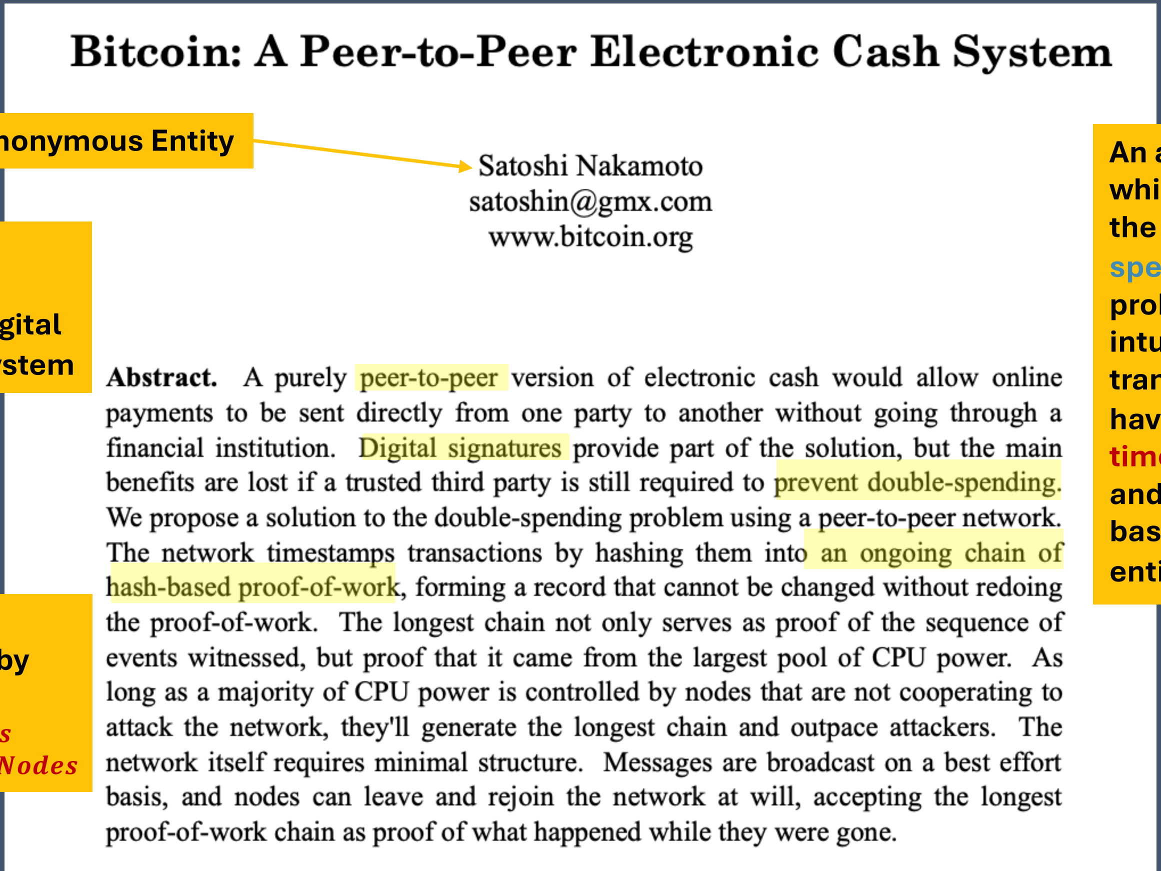
Both double spending and byzantine generals problems are not protected by distributed ledgers

These rationales make **distributed digital currencies** failed for a long time!

Some Failed Digital Currencies and Ledgers

- **DigiCash** (David Chaum) – 1989
- **Mondex** (National Westminster Bank) - 1993
- **CyberCash** (Lynch, Melton, Crocker & Wilson) – 1994
- **E-gold** (Gold & Silver Reserve) – 1996
- **Hashcash** (Adam Back) – 1997
- **Bit Gold** (Nick Szabo) – 1998
- **B-Money** (Wei Dai) - 1998
- **Lucre** (Ben Laurie) – 1999

Introducing Bitcoin



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Anonymous Entity

A fully functional trustless digital currency system

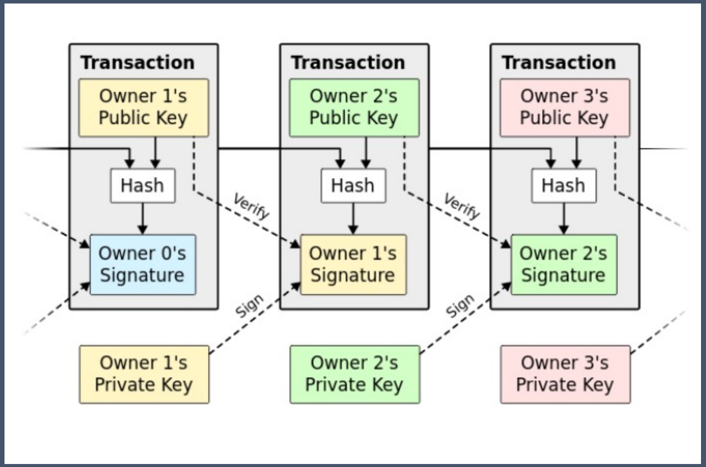
Security Guaranteed by

#HonestNodes > #MaliciousNodes

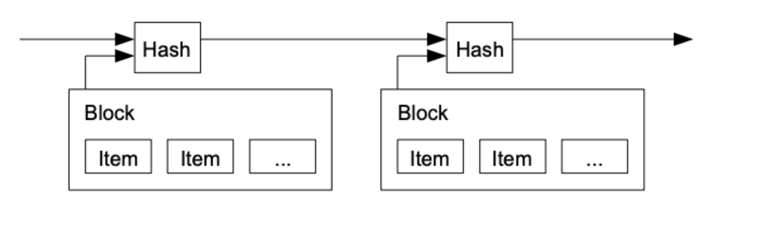
An algorithm which prevents the "double spend" problem. The intuition is that transactions have to be timestamped and trusted based on the entire network.

Bitcoin: A Chain of Blocks (Blockchain⛓️)

Chain of Digital Signatures



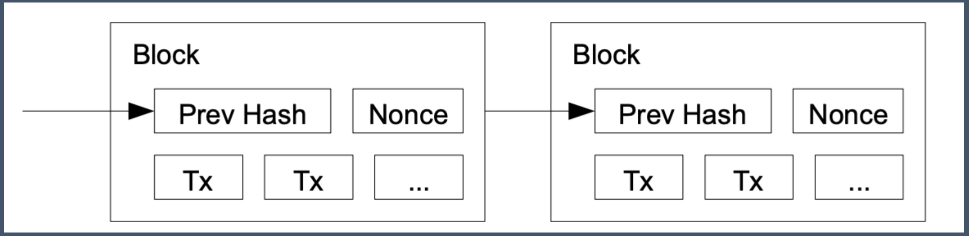
A Timestamp Server



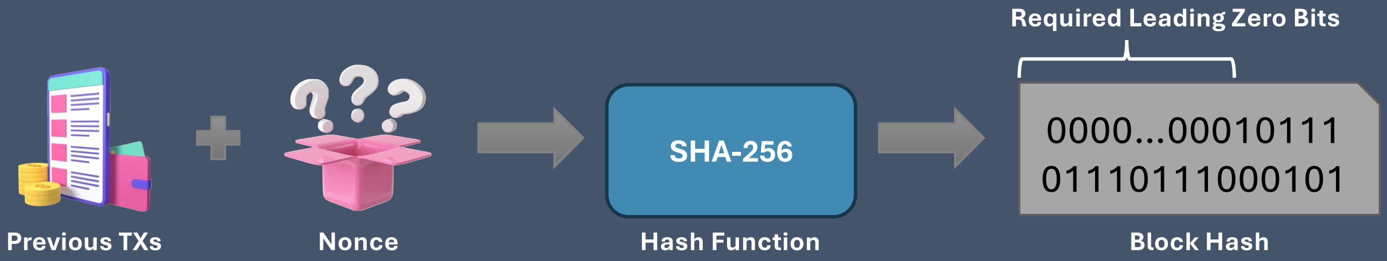
- This chain of signatures still expose to the double spending attack.
- We need **a trusted central authority** or **mint** that checks every transaction for double spending.
- To accomplish this **without a trusted party**, **transactions must be publicly announced**, and we need a system for participants to agree on a single history of the order in which they were received.

But, this one is not distributed!

Bitcoin: Proof-of-Work



- To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system.
- The proof-of-work involves scanning for a value that **when hashed**, such as with SHA-256, the hash begins with **a specific number of zero bits**.
  - By incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits (i.e., the difficulty of the puzzle).



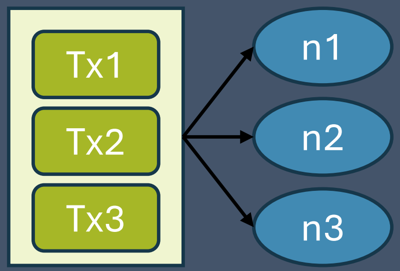
Bitcoin: Incentive

- If **most of the CPU power** is controlled by **honest nodes**, the **honest chain** will grow the fastest and outpace any competing chains.
  - To modify a past block, **an attacker** would have to **redo the proof-of-work** of the block and all blocks after it and then catch up with and **surpass the work of the honest nodes**.
- So, what incentivize the network to perform these computations (expending computational power)?
- One answer is simple to be able to use a secure network of value exchange.
- Another (less idealistic) reason is that nodes that verify transactions (i.e., miners) are **rewarded with bitcoins when validating a block.**

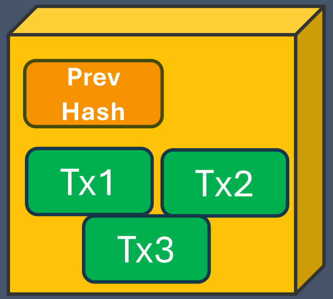
Bitcoin: The Network

- The steps to run the Bitcoin network are as follows:

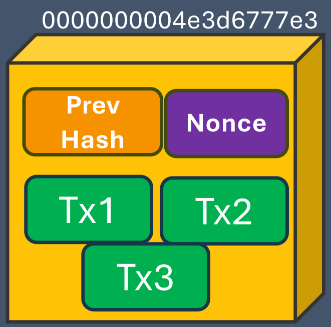
1 **Broadcast transactions to all nodes.**



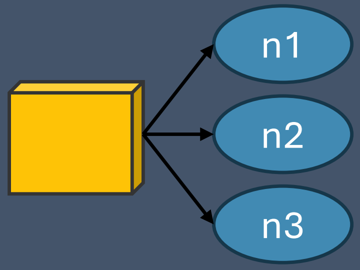
2 **Collect transactions into blocks.**



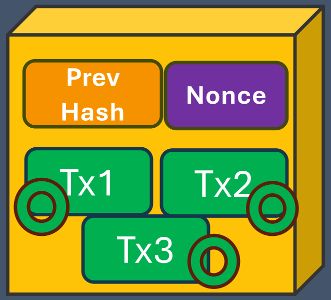
3 **Find a difficult proof-of-work for the block.**



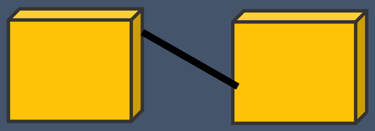
4 **Broadcast the proved block to all nodes.**



5 **Nodes accept the block if all transactions are valid and not already spent.**

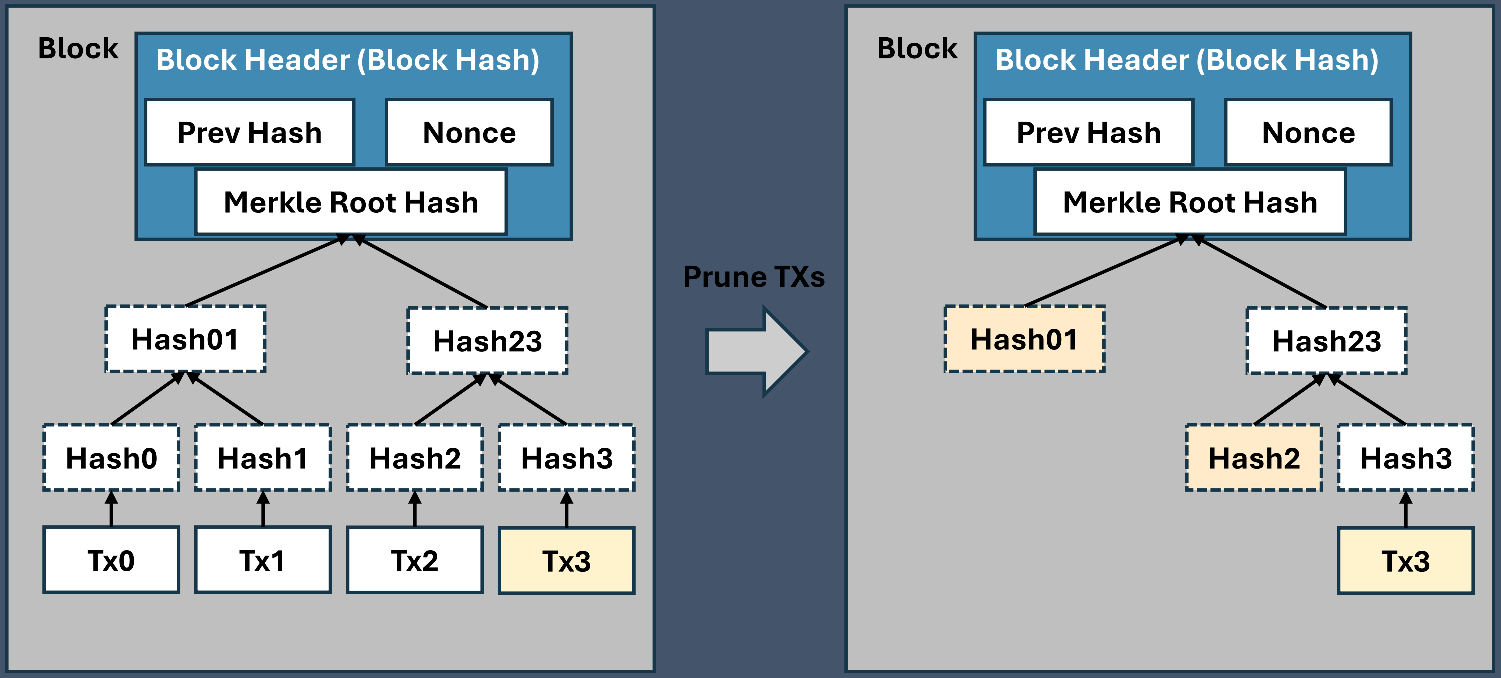


6 **Accept the block by continuing to create a new block.**

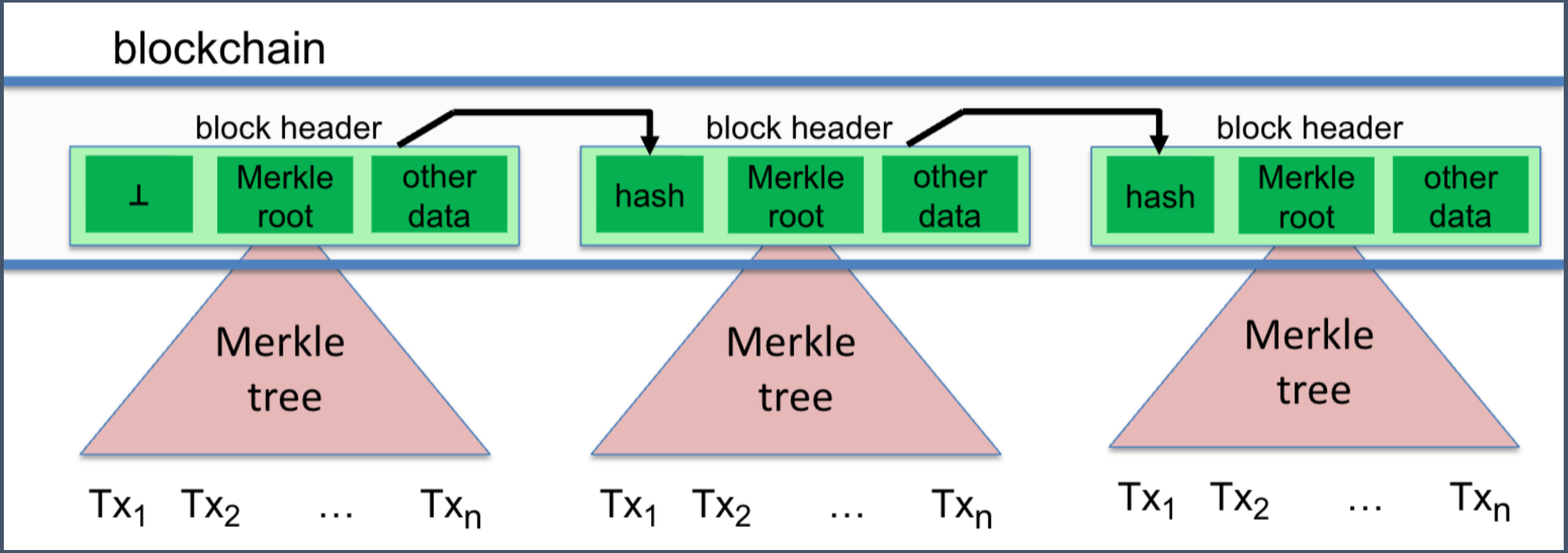


Bitcoin: Reclaiming Disk Space

- To save up disk space, old transaction can be **discarded**.
- A **Merkle Tree structure** is used so that the hash of the history is not changed.

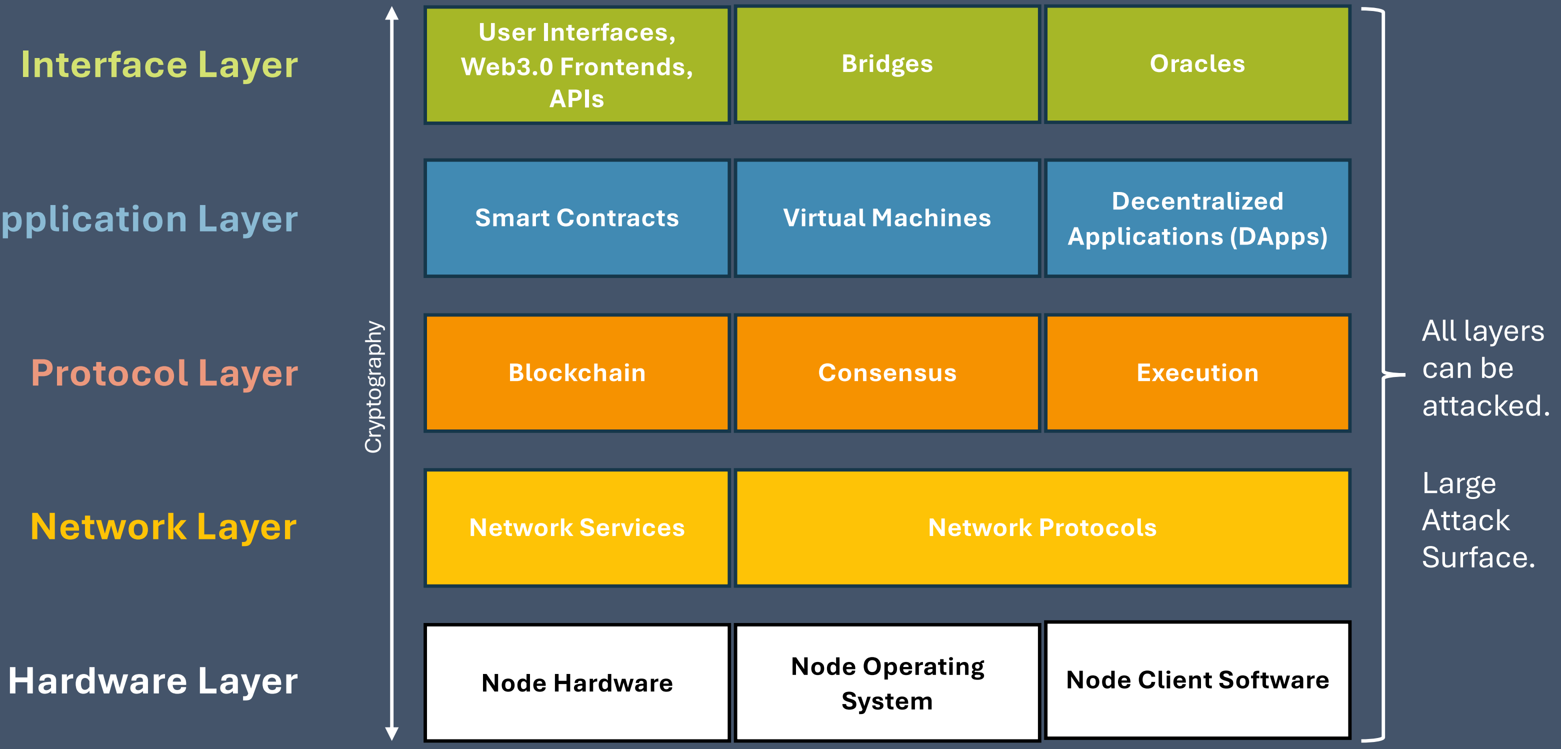


Abstraction of Blockchain



- Merkle proofs are used to prove that a Tx is “on the block chain.”

Blockchain Abstraction Layers



All layers can be attacked.

Large Attack Surface.

Summary of Today’s Lecture

- Upon successful of today’s lecture, we have learned about:
  - Distributed ledger is the **distribution of ledger management** to a network of individuals.
  - Centralized and distributed ledgers are facing the different problems, such as **double spending** and **Byzantine generals** problems.
  - **Bitcoin** is the gate to the new era of digital cash system that adopts **the chain of digital signatures**.
  - Technology behind Bitcoin is **the blockchain technology** to implement the cryptographically distributed ledger in the network.
  - Bitcoin’s blockchain starts with the compilation of transactions **into blocks** and uses the **block hash** to validate the append-only log.

End of the Lecture

Please do not hesitate to ask any questions to free your curiosity,

If you have any further questions after the class, please contact me via email (charnon@cmkl.ac.th).