SEC-205: Distributed Ledger and Blockchain

Lecture 5 - 6: Blockchain Security and Privacy

Instructed By:

Dr. Charnon Pattiyanon

Assistant Director of IT and Instructor
CMKL University

Artificial Intelligence and Computer
Engineering (AICE) Program

This lecture material is adopted from a presentation prepared by Le Duc Phong Fintech Research, Bank of Canada

Today’s Agenda

- In today’s lecture, we will explore and learn about:
  - Background of Blockchain Security and Historic Attacks.
  - Threats and Vulnerabilities at Each Layer of Blockchain Layered Model, including smart contract security, blockchain layer security, and security at other layers, how to address them, and best practices.
  - Privacy and Its Types.
  - Layer 0, Layer 1, and Layer 2 Protocols for Privacy on Blockchain

Blockchain Security

What is Blockchain Security? 🔐

- **Blockchain security** refers to the measures and practices implemented to protect the integrity, confidentiality, and availability of data and transactions within a blockchain network.
- **Security Requirements of Blockchain:**

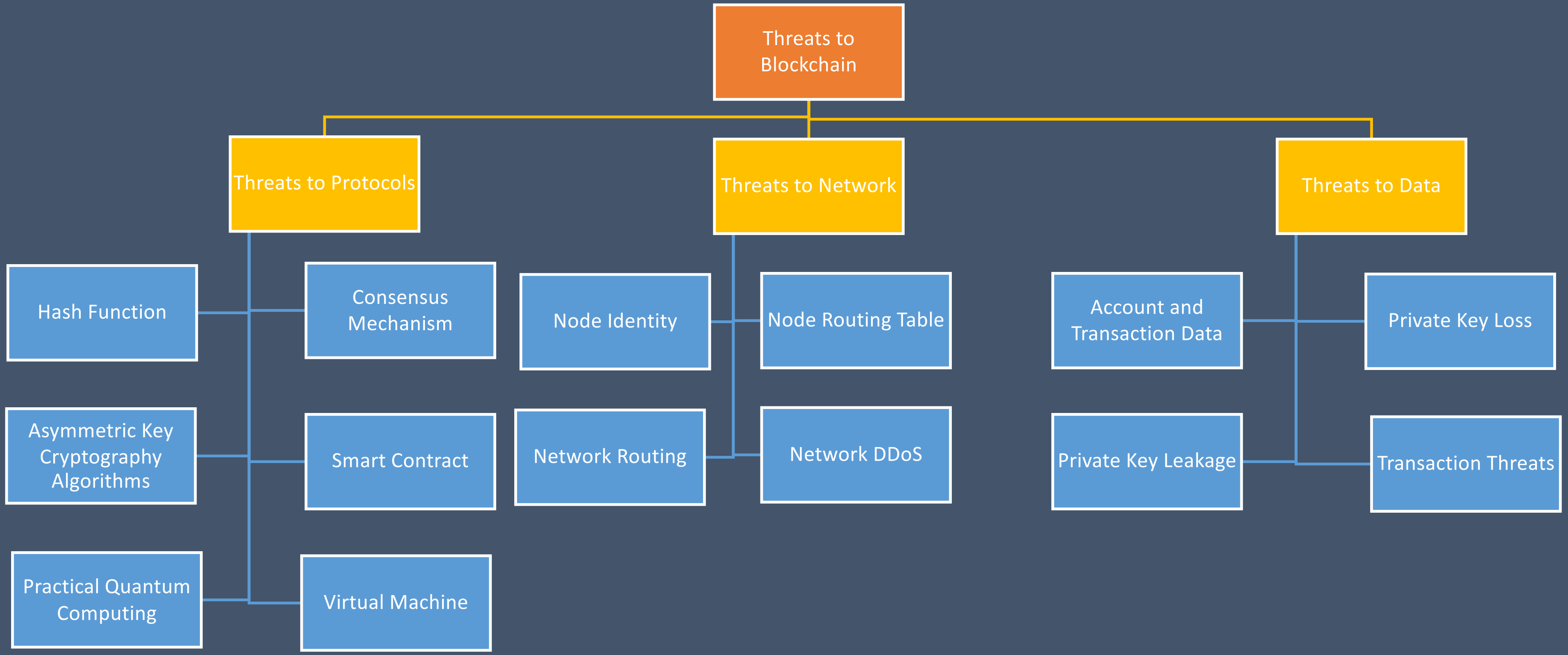
Integrity and Availability of the System

Consistency of the Ledger Across Institutions

Confidentiality, Integrity and Availability of Transaction Data

Prevention of Double Spending

Threats and Vulnerability of Blockchain



Security Impacts of the Blockchain

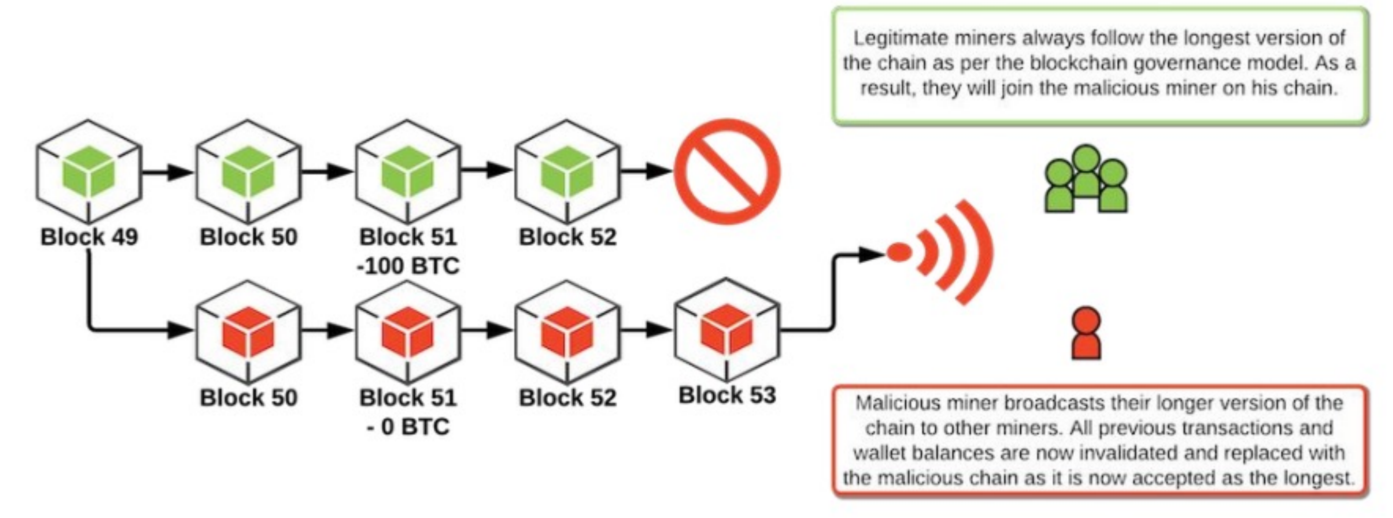
- **Protocols:** significantly impact on the integrity of the blockchain system.
  - For example, a successful attack against consensus mechanism allows the attacker to control the blockchain system entirely.

- **Network:** Impact to the availability of the system
  - For example, a successful attack on the network connections between nodes allows the attacker to isolate some nodes from the network.

- **Data:** Impact to the confidentiality and Asset's Ownership.
  - Private Key Loss: No more control over digital assets.
  - Private Key Leakage: Unauthorized Transactions.

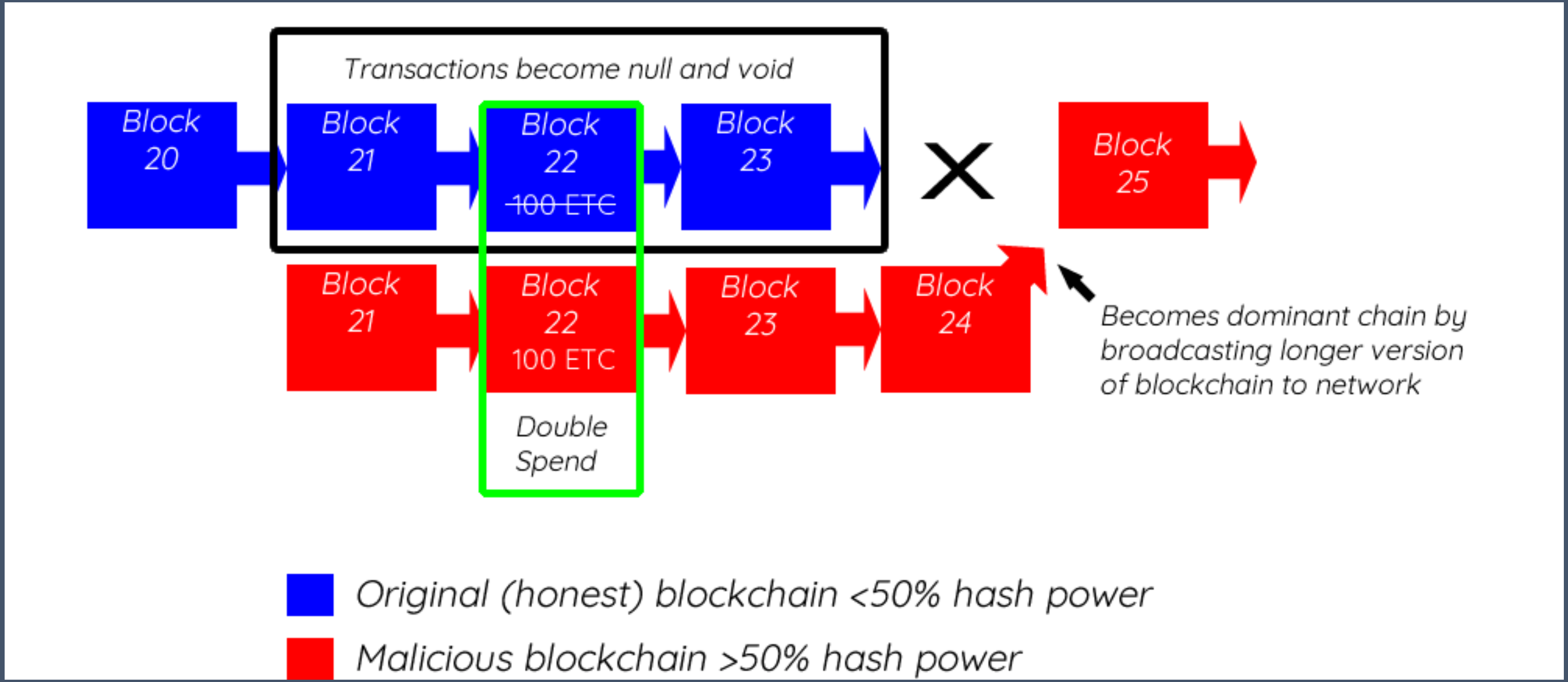
Security of Consensus Mechanism: **51% Attacks**

Consensus is the process by which a group of peers – or nodes – on a network determine which blockchain transactions are valid and which are not


Legitimate miners always follow the longest version of the chain as per the blockchain governance model. As a result, they will join the malicious miner on his chain.
Block 49
Block 50
Block 51
-100 BTC
Block 52
Block 50
Block 51
- 0 BTC
Block 52
Block 53
Malicious miner broadcasts their longer version of the chain to other miners. All previous transactions and wallet balances are now invalidated and replaced with the malicious chain as it is now accepted as the longest.

"If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains." -- Satoshi Nakamoto.

51% Attack (Double Spending)



Transactions become null and void

Double Spend

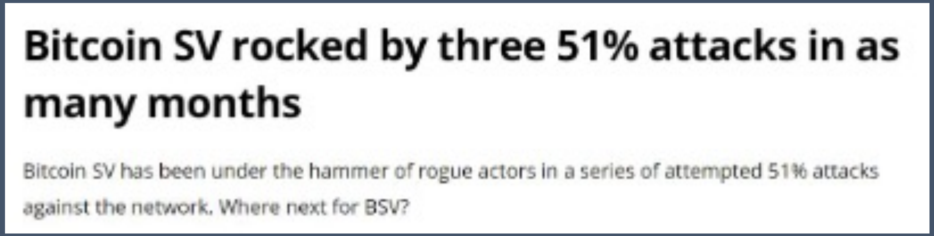
Becomes dominant chain by broadcasting longer version of blockchain to network

🟦 Original (honest) blockchain <50% hash power

🟥 Malicious blockchain >50% hash power

51% Attack Stories

- **Ethereum Classic (ETC)**, several times
  - Three attacks in August 2020: reorganized over 7,000 blocks, or two days' worth of mining.
  - 88,500 ETC (roughly $450,000) were falsely deposited on the OkEX crypto exchange.
  - On January 8th, 2020, Ethereum Classic had just 8.8 terra-hash, compared to **over 39 million terra-hash** of **Bitcoin**.
- BSV, reported in August 2021
  - Nearly 100 blocks were compromised.



Bitcoin SV rocked by three 51% attacks in as many months

Bitcoin SV has been under the hammer of rogue actors in a series of attempted 51% attacks against the network. Where next for BSV?

  - Many other stories, including BTG, Verge, Mona, Aurum, ZenCash, etc.

Why Does Data Security Concern?

Data on Blockchain includes public/private key, wallet address, transaction data, etc.

- Losing private key results in losing funds.
- **Stories:**
  - A 35-year-old British man threw out a hard drive containing 7,500 BTC (around $350 Million).
  - A German engineer who forgot the password to his encrypted device containing 7,002 BTC.
  - Canada exchange QuadrigaCX's CEO went and allegedly died in India in 2018. This tragedy affects more than 115,000 users' coins being lost, including 6,500 BTC; 11k BCH; 200k LTC and 430k ETH.
  - And many more stories, … Just google "bitcoin private key lost stories."

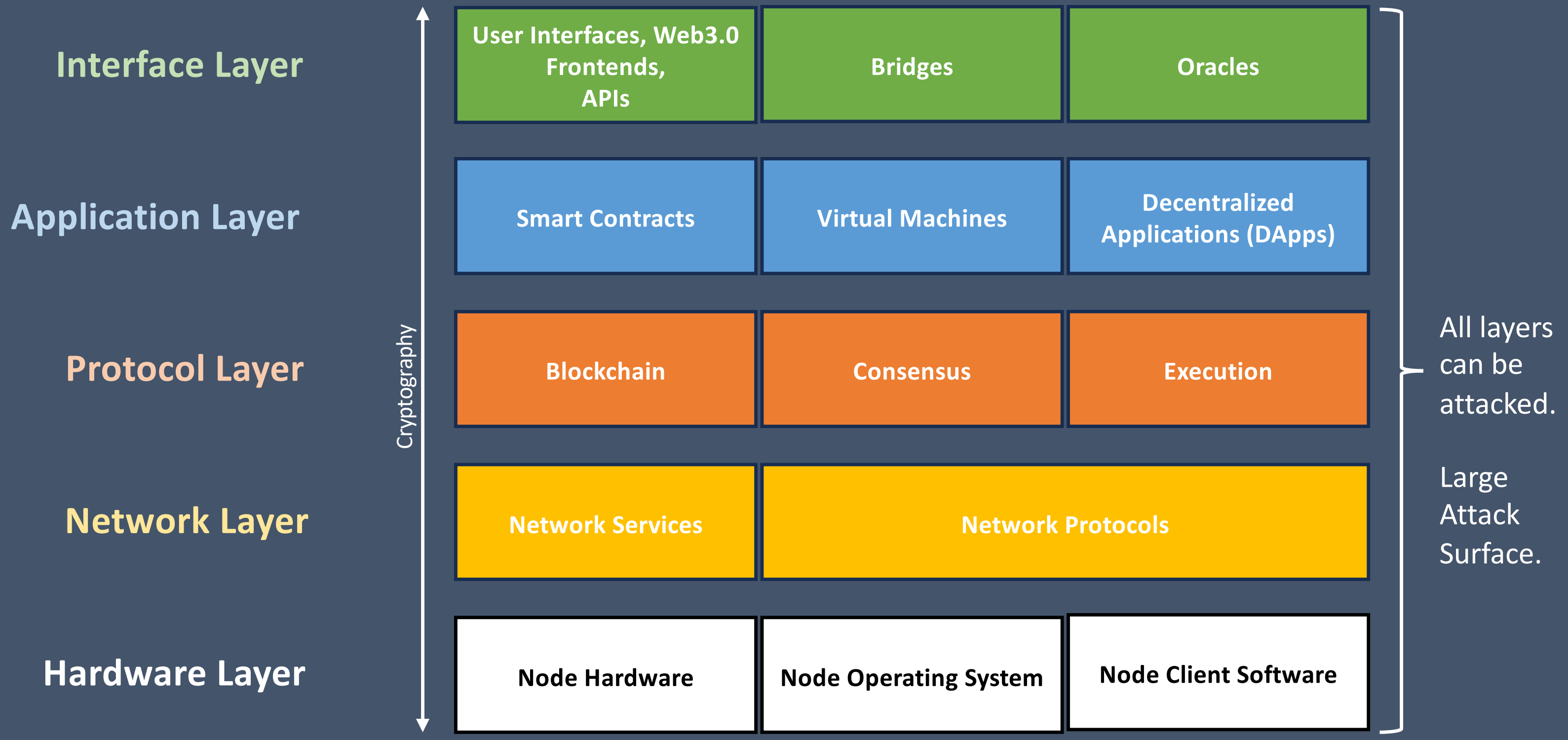
Security of Smart Contract

The Decentralized Autonomous Organization (DAO) Hack

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code

- DAO is an organization represented by rules encoded as a computer program (i.e., a smart contract).
- The DAO is built on Ethereum, designed for building decentralized applications.
- When launching in 2016, the DAO raised $150m worth of ETH through a token sale.
- On 20 July 2016, hackers exploited a flaw in the DAO project's smart contract.
- Hackers stole 3.6 million ETH (Approx. $50 million that time, and approx. $6 billion today), showing that the DAO was All Too Human.
- Ethereum made a hard fork to restore the money.

Blockchain Layered Model



Interface Layer	User Interfaces, Web3.0 Frontends, APIs	Bridges	Oracles
Application Layer	Smart Contracts	Virtual Machines	Decentralized Applications (DApps)
Protocol Layer	Blockchain	Consensus	Execution
Network Layer	Network Services	Network Protocols	
Hardware Layer	Node Hardware	Node Operating System	Node Client Software

Cryptography

All layers can be attacked.

Large Attack Surface.

Security Issues at the Hardware Layer (Layer 0)

- This layer is compsed of hardware that runs the operating system and node software.
- This layer is impacted by usual threats, e.g., viruses, malware, and unauthorized access.
- Blockchain-specific malware also exists to especially target on cryptojacking, so called **Crypto-Malware**.
  - Cryptojacking is a method of taking over a computer or web browser to mine for cryptocurrency without the user's permission.
  - Cryptojacking is the unauthorized use of computing resources that belong to someone to mine cryptocurrency.
- **Denial of Service (DoS)** attack can cause the resources on the blockchain node to struggle to keep up with the incoming requests.

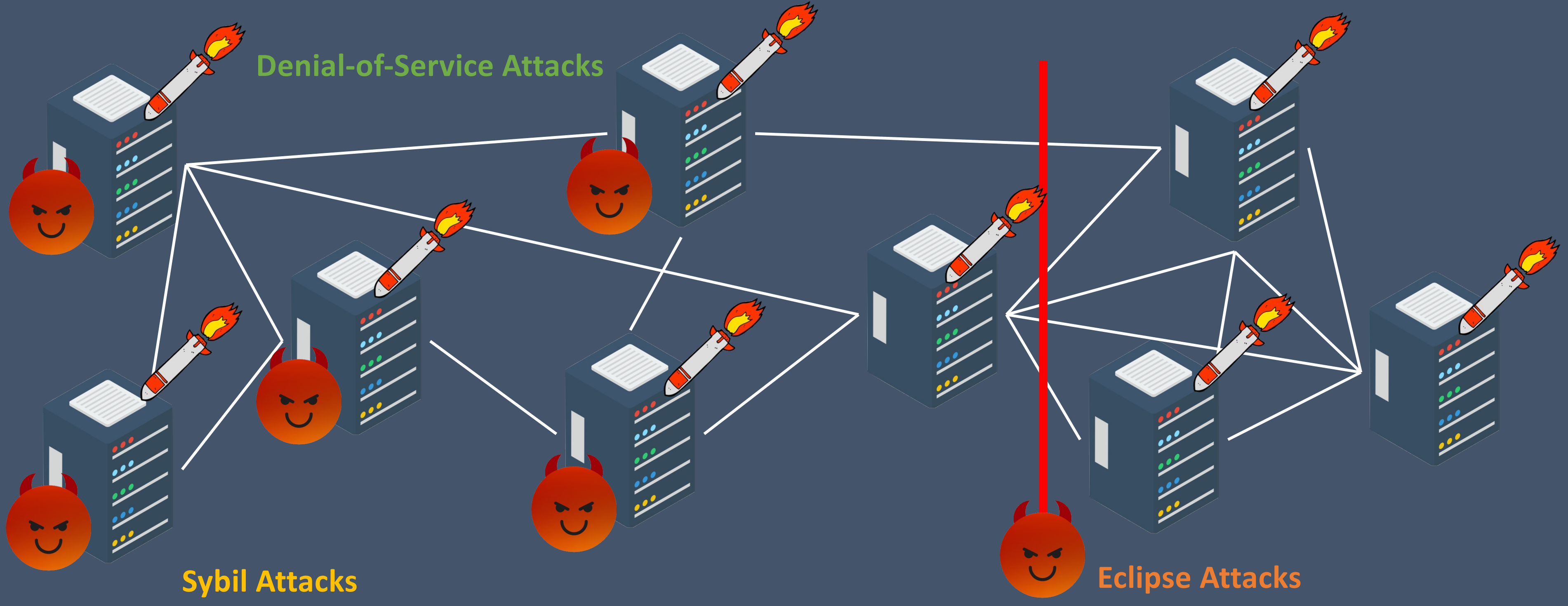
Security Issues at the Network Layer (Layer 1)

- There are many possible security attacks on the network layer:

1. **Sybil Attacks:** is a type of network attack in which an attacker creates and uses multiple fake identities, or “Sybil nodes,” to gain an unfair advantage or perform malicious actions within a network.
2. **Denial-of-Service Attacks:** overwhelming the network with unnecessary traffic to make it inaccessible to users.
3. **Eclipse Attacks:** is a type of attack on a blockchain network in which an attacker tries to isolate a specific node or some nodes from the rest of the network, effectively “eclipsing” them and making them unable to communicate with other nodes, stopping them from receiving new information.

Security Issues at the Network Layer (Layer 1)

- There are many possible security attacks on the network layer:



Security Issues at the Protocol Layer (Layer 2)

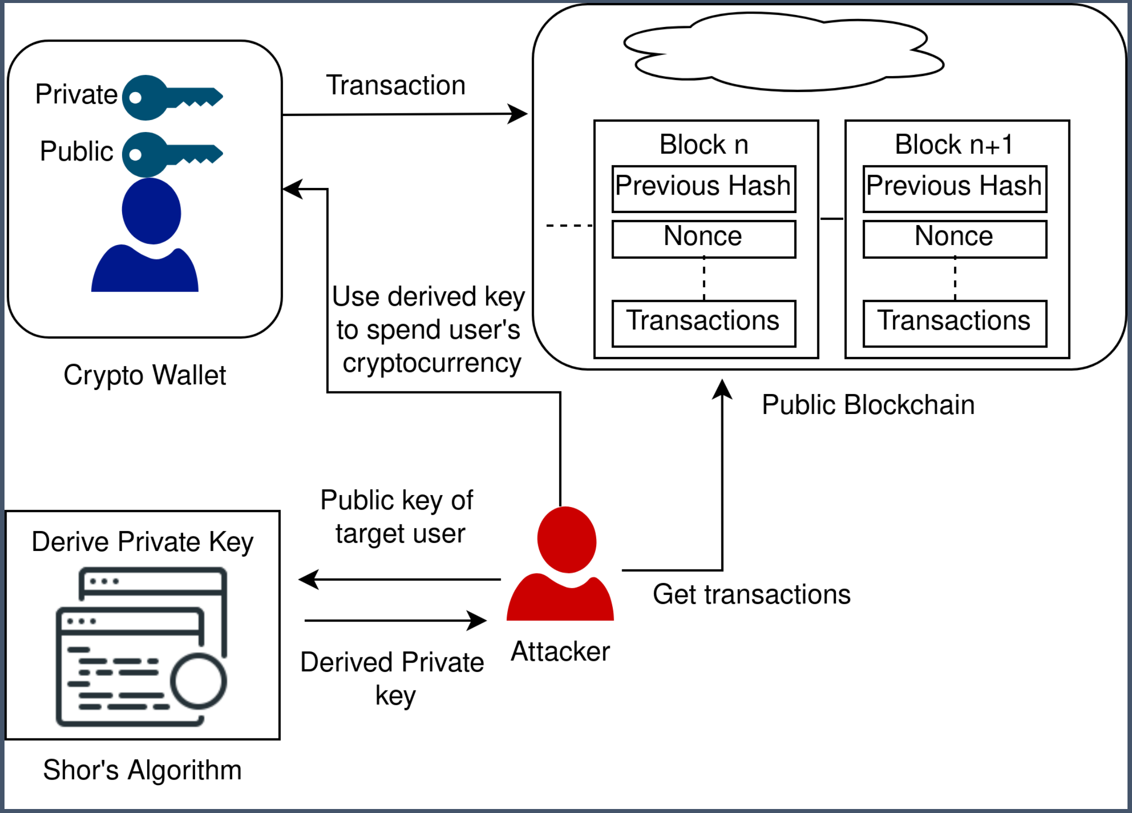
- There are many attacked carried out at this layer:
  - **Attack on Transactions or Transaction Mallability Attacks:**
    - The transactions are constructed by the users, and they can be malformed or invalid.
    - As transactions are propagated to all nodes and all nodes process all transactions, transactions especially crafted to cause harm can become an attractive attack vector for hackers.
    - While invalid and incorrectly signed transactions with invalid signatures will be rejected by all nodes, it is possible that the transaction is properly signed and passes all checks before executing transactions and ending up executing some rogue code that results in an undesirable effect.
    - **One example** is from 2010 when over 184 billion Bitcoins were created out of thin air due to an integer overflow vulnerability in the Bitcoin core node software.

Security Issues at the Protocol Layer (Layer 2)

- There are many attacked carried out at this layer:
  - **Transaction Replay Attacks:**
    - In a transaction replay attack, an attacker captures a valid transaction from a network and tries to reuse it by "replaying" it on the same or a different network.
    - If the transaction is replayed on a different network, it can potentially be used to transfer funds or other assets to the attacker's own account.
    - During the hard fork, the Ethereum network split into two separate networks: **Ethereum (ETH)** and **Ethereum Classic (ETC)**. This meant that transactions on one network would not be recognized on the other network, and vice versa. However, because both networks were using the same keys to sign transactions, an attacker was able to capture a valid transaction on one network and replay it on the other network.

Security Issues at the Protocol Layer (Layer 2)

- There are many attacked carried out at this layer:
  - **Transaction Replay Attacks:**

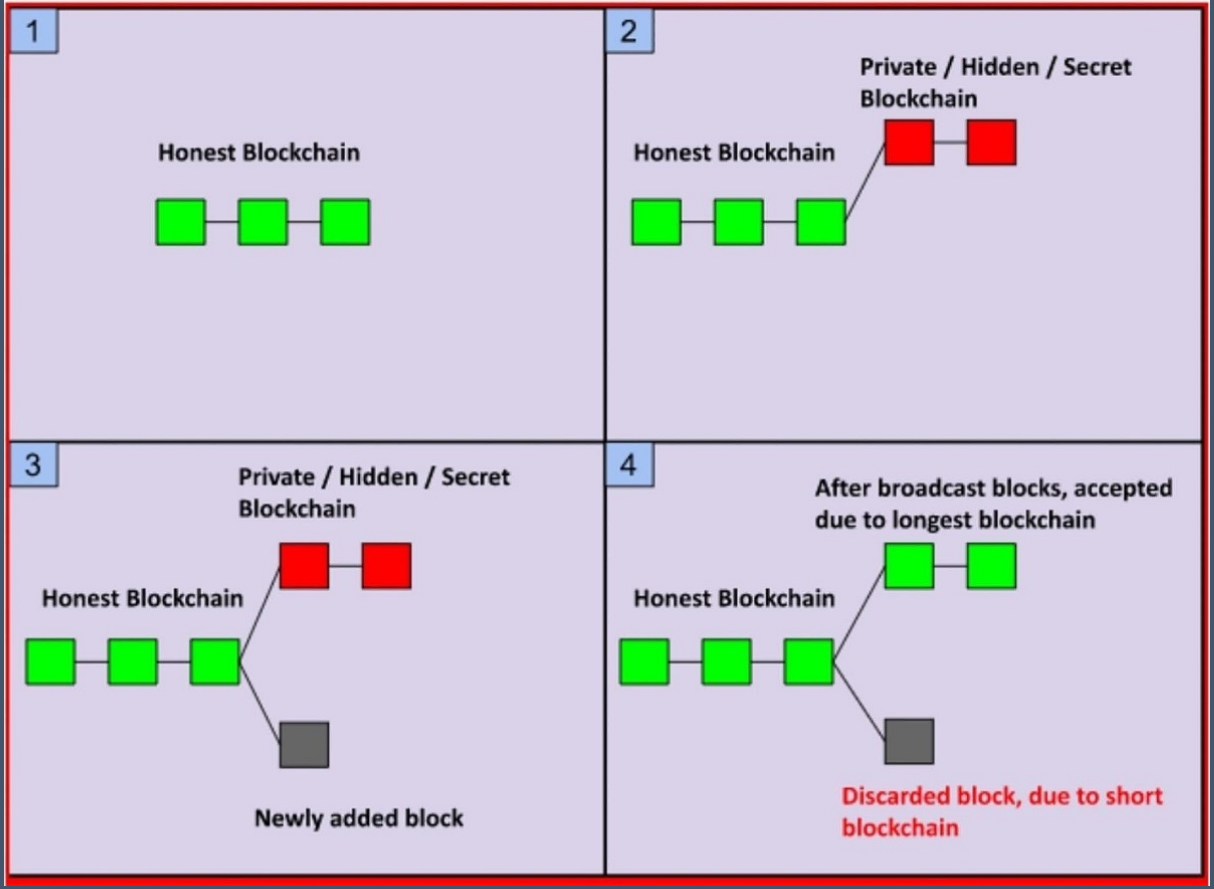


Security Issues at the Protocol Layer (Layer 2)

- Attacks on Consensus Protocols:
  - **A 51% attack:** This occurs when a miner or group of miners controls more than 50% of the mining power on the network, allowing them to control the confirmation of transactions and potentially double-spend coins.
  - **Selfish mining:** This occurs when a miner withholds the blocks they mine from the network in order to increase their chances of finding the next block and earning the block reward.
  - **A nothing-at-stake attack:** This occurs in PoS-based blockchain where validators are not required to put up any collateral, allowing them to vote on multiple chains and potentially undermine the integrity of the network.

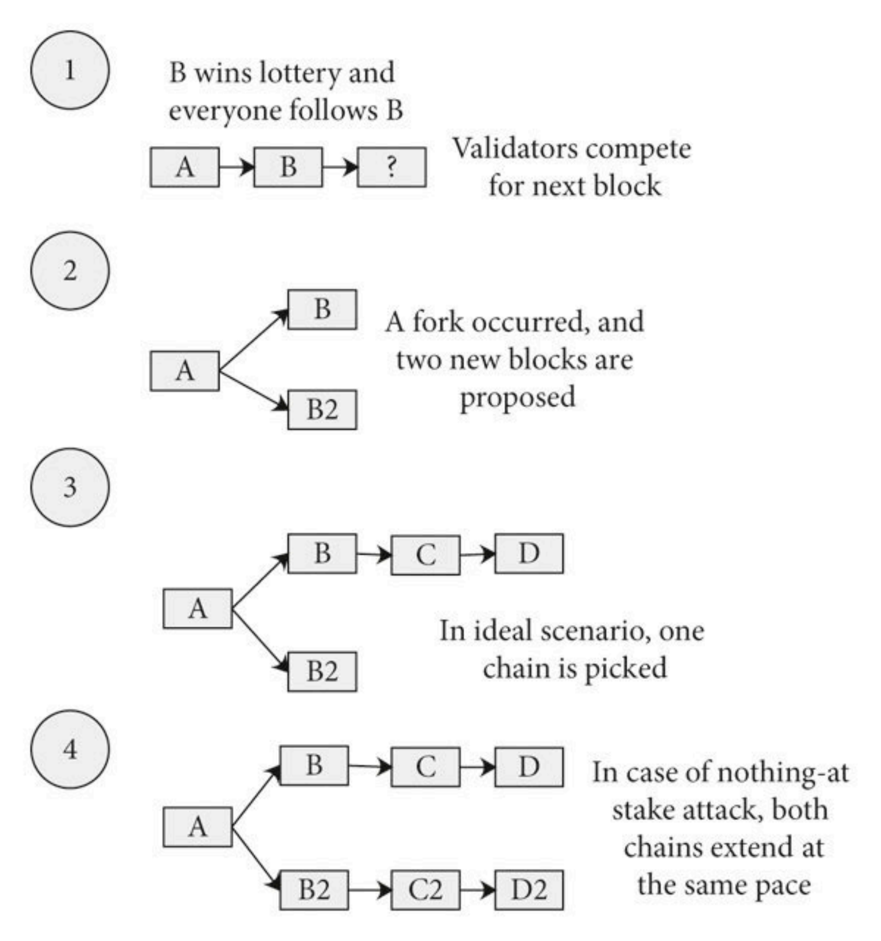
Security Issues at the Protocol Layer (Layer 2)

- Attacks on Consensus Protocols:
  - **Selfish mining:** This occurs when a miner withholds the blocks they mine from the network in order to increase their chances of finding the next block and earning the block reward.


1
Honest Blockchain
2
Private / Hidden / Secret Blockchain
Honest Blockchain
3
Private / Hidden / Secret Blockchain
Honest Blockchain
Newly added block
4
After broadcast blocks, accepted due to longest blockchain
Honest Blockchain
Discarded block, due to short blockchain

Security Issues at the Protocol Layer (Layer 2)

- Attacks on Consensus Protocols:
  - **A nothing-at-stake attack:** This occurs in PoS-based blockchain where validators are not required to put up any collateral, allowing them to vote on multiple chains and potentially undermine the integrity of the network.


1
B wins lottery and everyone follows B
A
B
?
Validators compete for next block
2
A
B
B2
A fork occurred, and two new blocks are proposed
3
A
B
C
D
B2
In ideal scenario, one chain is picked
4
A
B
C
D
B2
C2
D2
In case of nothing-at stake attack, both chains extend at the same pace

Security Issues at the Application Layer (Layer 4)

- There are several vulnerabilities that can exist at this layer. The most prominent are smart contract-related vulnerabilities:

1. **The transaction ordering dependency bug** basically exploits scenarios where the perceived state of a contract might not be what the state of the contract changes to after execution. This allows a transaction to be submitted before another transaction, thus leading to controlling the behavior of a smart contract.
2. **Timestamp dependency bugs** are possible in scenarios where the timestamp of the block is used as a source of some decision-making within the contract, but timestamps can be manipulated by the miners (block producers).

Security Issues at the Application Layer (Layer 4)

- There are several vulnerabilities that can exist at this layer. The most prominent are smart contract-related vulnerabilities:

3. **Send fail issue**: When sending funds to another contract, sending can fail, and even if throw statement is used as a catch-all mechanism, it will not work.
4. **Timestamp dependency** is another vulnerability that is quite common. Usually, the timestamp of a block is accessed via `now` or `block.timestamp`, but this timestamp can be manipulated by miners, leading to influencing the outcome of a function that relies on timestamps.
5. **Integer overflow and underflow** are also quite significant, and any use of integer variables should be carefully implemented in Solidity. For example, uint8 cannot handle integers over 256.
6. Many more….

Security Issues at the Interface Layer (Layer 5)

- **Oracle Attacks / Oracle Manipulation Attacks:**
  - Oracles provide trusted information based on the outside-world sources to the smart contracts.
  - These oracles, typically implemented as smart contracts, have the capability to supply incorrect data, which can result in detrimental consequences for processes linked to the data feed.
  - Some oracle attacks include:
    - **Tampering with data sources:** Attackers can manipulate the data sources that the oracles rely on to feed false information.
    - **Bribing oracles:** Attackers can bribe oracles to feed false information into the blockchain
    - **Oracle censorship:** Attackers can prevent oracles from accessing certain data sources, leading to a lack of information for the smart contract to make decisions.

Security Issues at the Interface Layer (Layer 5)

- **Wallet Attacks:**
  - **Cryptocurrency wallets** can be subject to several attacks, listed below:
    - Phishing attacks: Where an attacker creates a fake wallet website or app that looks similar to a real one.
    - Malware attacks: Where malware infects the computer or mobile device used to access the cryptocurrency wallet and steals seed phrases or private keys.
    - Man-in-the-Middle (MITM) attacks: Where an attacker intercepts and manipulates transactions by posing as a trusted entity during the communication between the wallet and the Ethereum network.
    - Security vulnerabilities in the cryptocurrency wallet code: Where a hacker exploits a weakness in the wallet code to gain access to private keys and consequently the funds.

Security Issues at the Interface Layer (Layer 5)

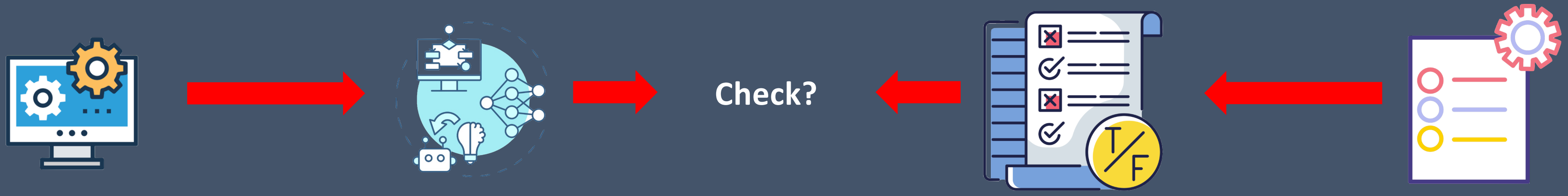
- **Wallet Attacks:**
  - **Hardware wallets** can be subject to several attacks, listed below:
    - Supply chain attacks: Where an attacker modifies the wallet during production to gain access to private keys or seed phrases.
    - Physical tampering: Where an attacker physically opens the wallet and accesses the private keys.
    - Malware attacks: Where malware infects the computer used to connect to the wallet and steals private keys.
    - MITM attacks: Where an attacker intercepts and manipulates transactions during the communication between the hardware wallet and the computer.

Security Analysis Tools and Mechanisms for Blockchain

- There are many tools and techniques that could be used to analyze and ensure security of blockchain application, including smart contracts and consensus mechanisms.
- Examples of tools and mechanisms are:
  - Formal Verification of Smart Contracts
  - Formal Verification of Consensus Mechanisms.
  - Threat Modeling.

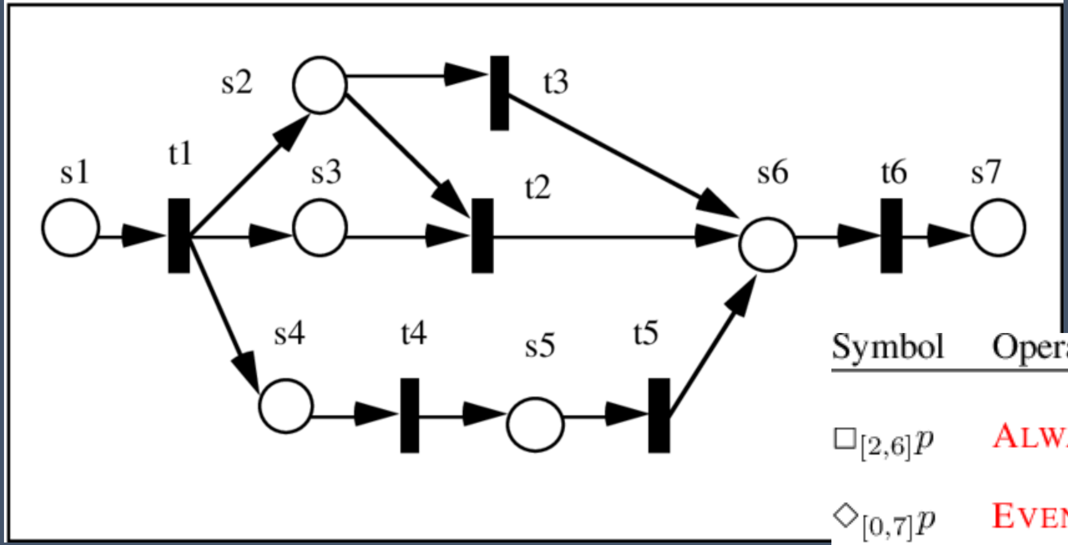
What are Formal Verification and Formal Methods?

- Formal methods are the set of techniques used to model systems as mathematical objects.
- Formal methods can be divided into two broad disciplines called formal specifications and formal verification.
- In an essence, the formal verification consisted of three steps:
  1. Create a formal model of the system to be checked.
  2. Write a formal specification of the properties that are expected to be satisfied by our model.
  3. The model is checked to ensure that the model satisfies the specification.



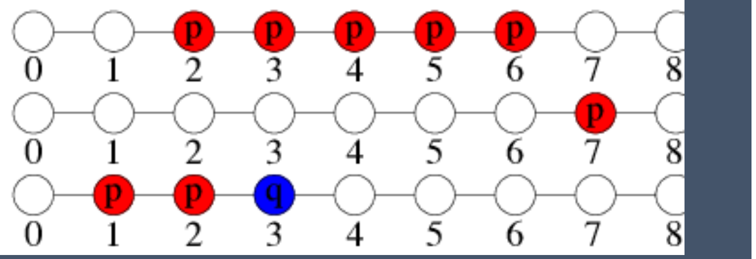
What are Formal Verification and Formal Methods?

- **Formal Models of the System** – FSM, Petri Nets



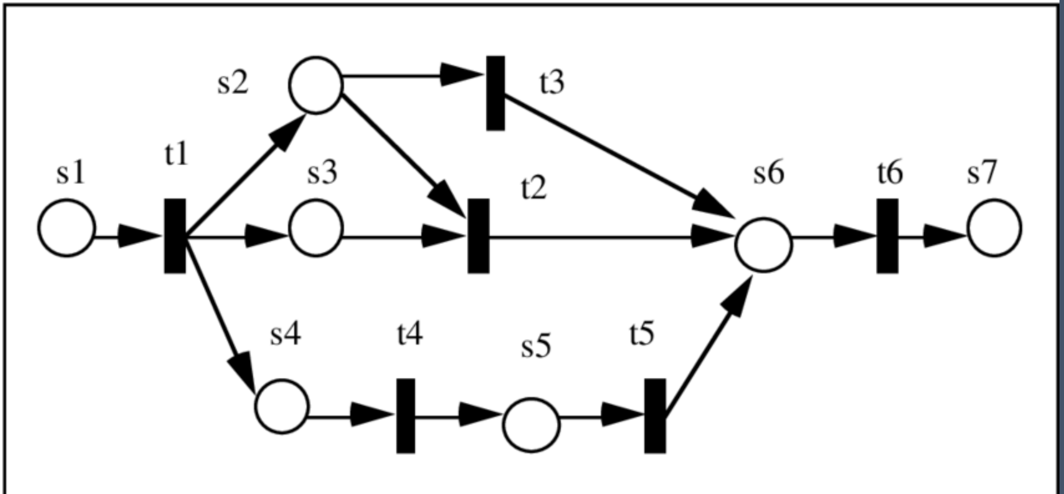
- **Formal Specification** – Linear Temporal Logics

Symbol	Operator	Timeline
$\Box_{[2,6]}p$	ALWAYS$_{[2,6]}$	○ ○ p p p p p ○ ○ 0 1 2 3 4 5 6 7 8
$\Diamond_{[0,7]}p$	EVENTUALLY$_{[0,7]}$	○ ○ ○ ○ ○ ○ ○ p ○ 0 1 2 3 4 5 6 7 8
$p\,\mathcal{U}_{[1,5]}\,q$	UNTIL$_{[1,5]}$	○ p p q ○ ○ ○ ○ ○ 0 1 2 3 4 5 6 7 8

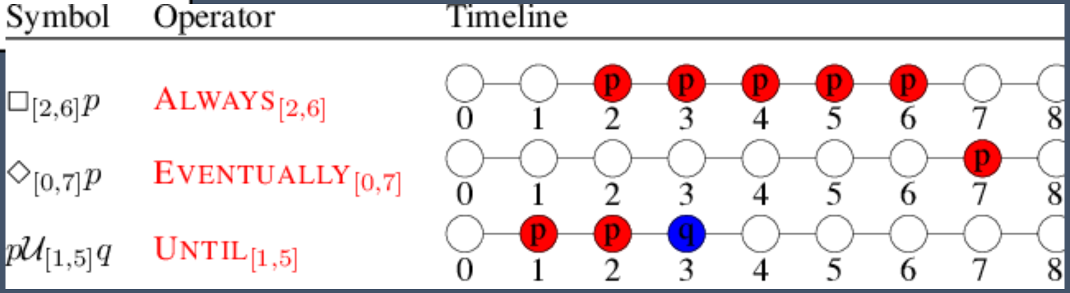


What are Formal Verification and Formal Methods?

- **State Exploration Approach**



- **State Space**
  - s1-t1-s2-t3-s6-t6-s7
  - s1-t1-s2-t2-s6-t6-s7
  - s1-t1-s3-t2-s6-t6-s7
  - s1-t1-s4-t4-s5-t5-s6-t6-s7



Symbol	Operator	Timeline
$\square_{[2,6]} p$	ALWAYS$_{[2,6]}$	○ ○ p p p p p ○ ○ 0 1 2 3 4 5 6 7 8
$\diamond_{[0,7]} p$	EVENTUALLY$_{[0,7]}$	○ ○ ○ ○ ○ ○ ○ p ○ 0 1 2 3 4 5 6 7 8
$p\,\mathcal{U}_{[1,5]}\,q$	UNTIL$_{[1,5]}$	○ p p q ○ ○ ○ ○ ○ 0 1 2 3 4 5 6 7 8

Summary of Blockchain Security

- There are many kinds of security issues or attacks that can be happened or targeted in the blockchain system.
- Attack surfaces can be located in every layer of the blockchain system.
- The consequences of security threats in the blockchain system can be varied from the loss of cryptocurrencies to a destruction of the blockchain system.
- There are many methods to analyze the blockchain security, such as formal verification, and threat modeling.

Blockchain Privacy

What is Blockchain Privacy?

- Privacy in blockchain can be divided into two main categories based on the type of service required:
    - **The Anonymity of the Users:** Hiding the sender's or receiver's identity.
    - **The Confidentiality of the Transactions:** Hiding transaction values.

- The fundamental reason why blockchains are not privacy-preserving is that every transaction in a blockchain needs to be verified and executed by every participant on the network.
- One solution that comes to mind is that we could somehow encrypt the data, but if the values are hidden, then the transactions cannot be verified.

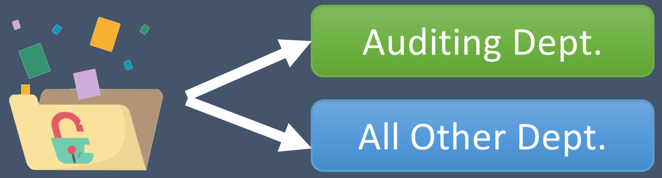
Anonymity of Users

- **Anonymity** is desirable in situations where the identity of users is required to be hidden from other participants on a network.
- This can be due to regulatory requirements, enterprise requirements, or just due to the sensitive nature of the transactions.

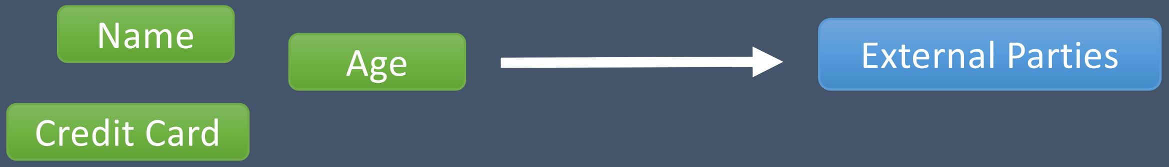
- The properties used to achieve anonymity:
  - ***Unlinkability:*** An observer is unable to deduce the link between transactions and their participants, or the relationships between transaction participants (senders and receivers).
  - ***Untraceability***: To hide the trace of a transaction from one party to another in a network.

Confidentiality of Transactions

- When we think about confidentiality we can divide it into two further optional requirements:
  - **Conditional Privacy:** A system should have the ability to conditionally make data visible to a third party such as auditors, but keep the data hidden from all other parties except those who are privy to the transactions.

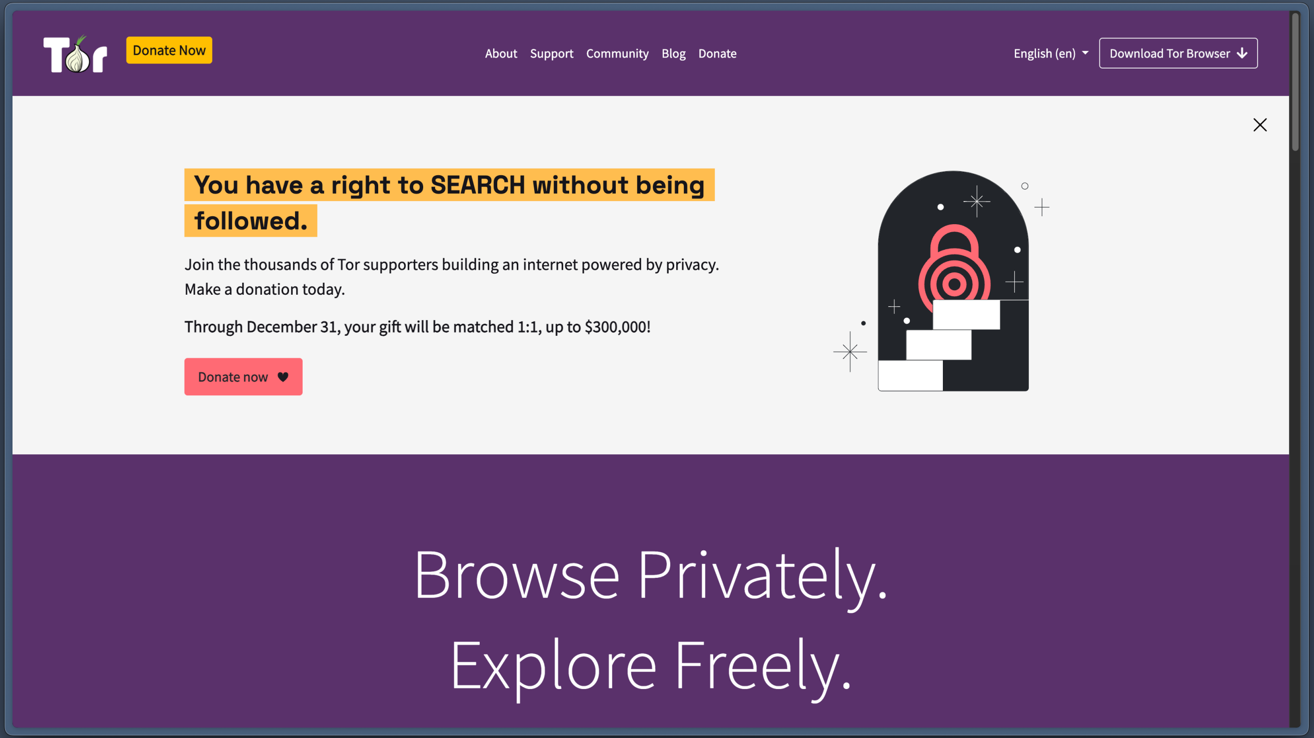


  - **Selective Disclosure:** A system should have the ability to selectivity share some part of the data, such as age only, from a larger dataset containing personal information.



Tools and Techniques for Blockchain Privacy

- There are many tools and techniques to preserve privacy in blockchain systems:



You have a right to SEARCH without being followed.

Join the thousands of Tor supporters building an internet powered by privacy. Make a donation today.

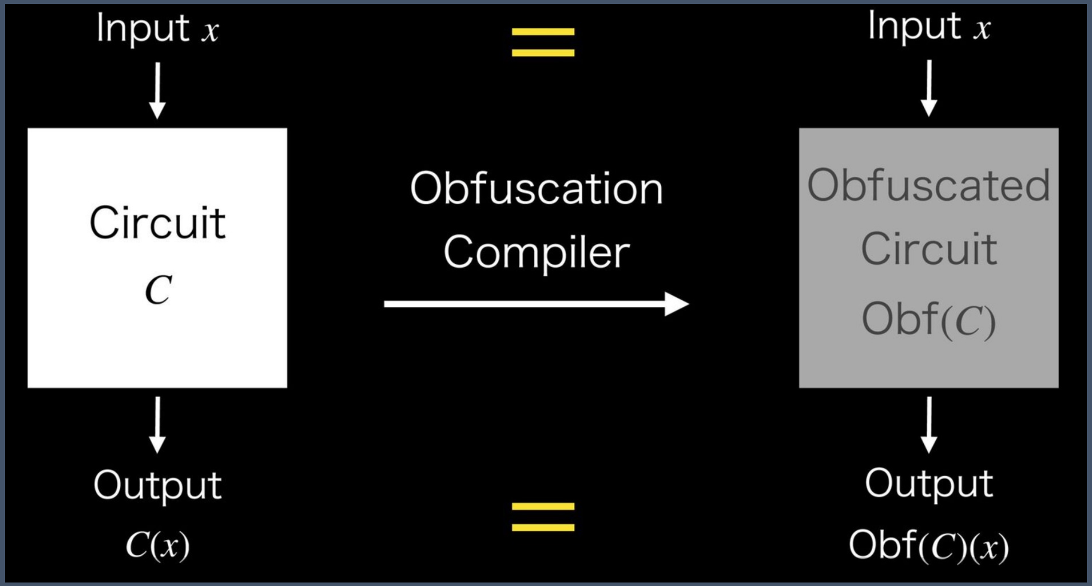
Through December 31, your gift will be matched 1:1, up to $300,000!

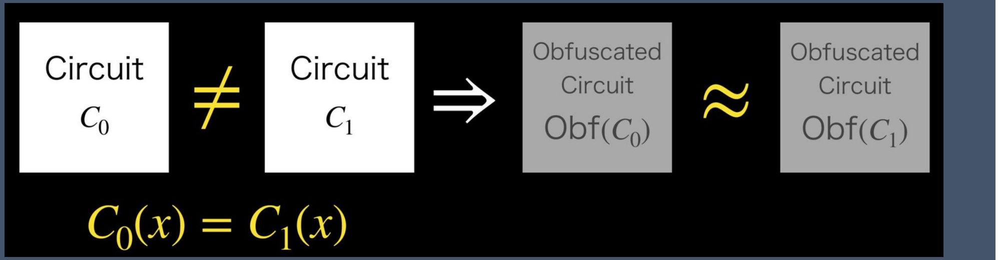
Browse Privately.
Explore Freely.

The Onion Router (TOR) is a software that enables anonymous communications.

Tools and Techniques for Blockchain Privacy

- There are many tools and techniques to preserve privacy in blockchain systems:



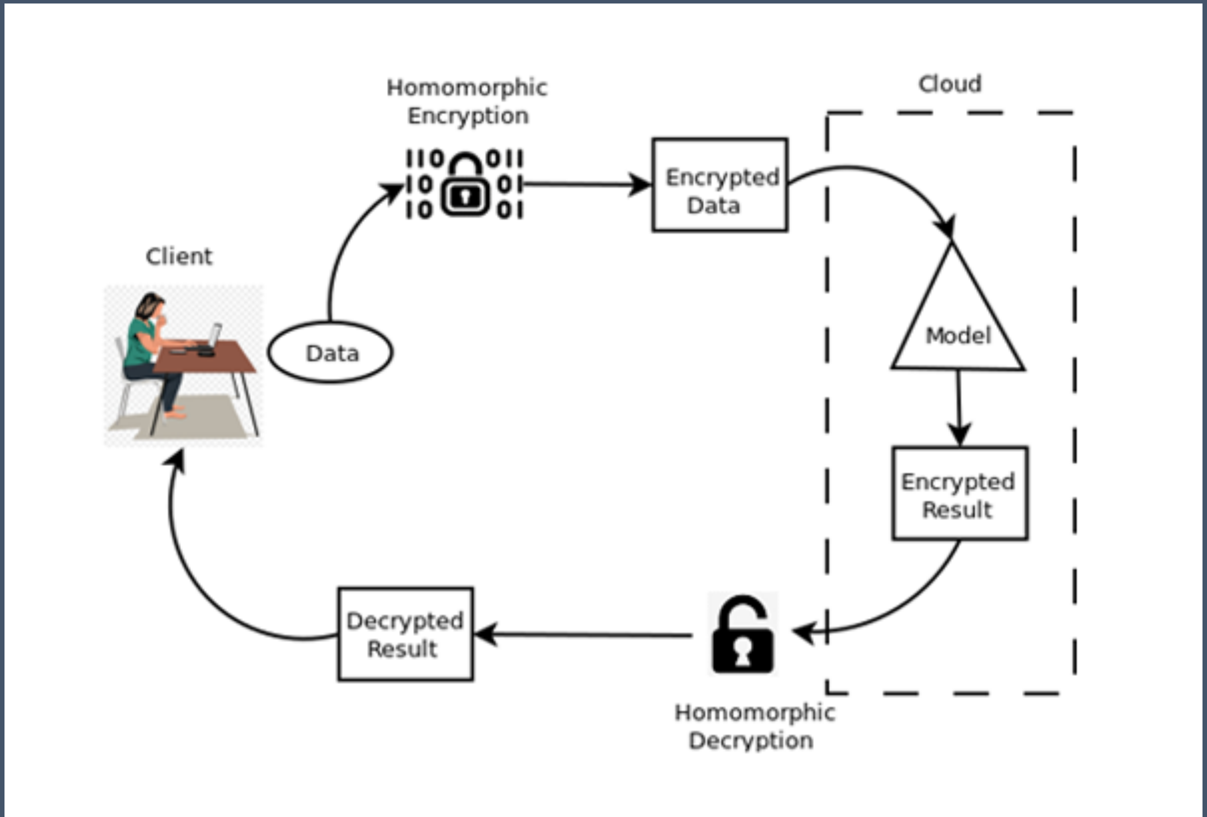


Indistinguishability Obfuscation (IO)

can serve as an unbreakable obfuscation mechanism that will turn smart contracts into a black box where the behavior of the obfuscated code is indistinguishable.

Tools and Techniques for Blockchain Privacy

- There are many tools and techniques to preserve privacy in blockchain systems:

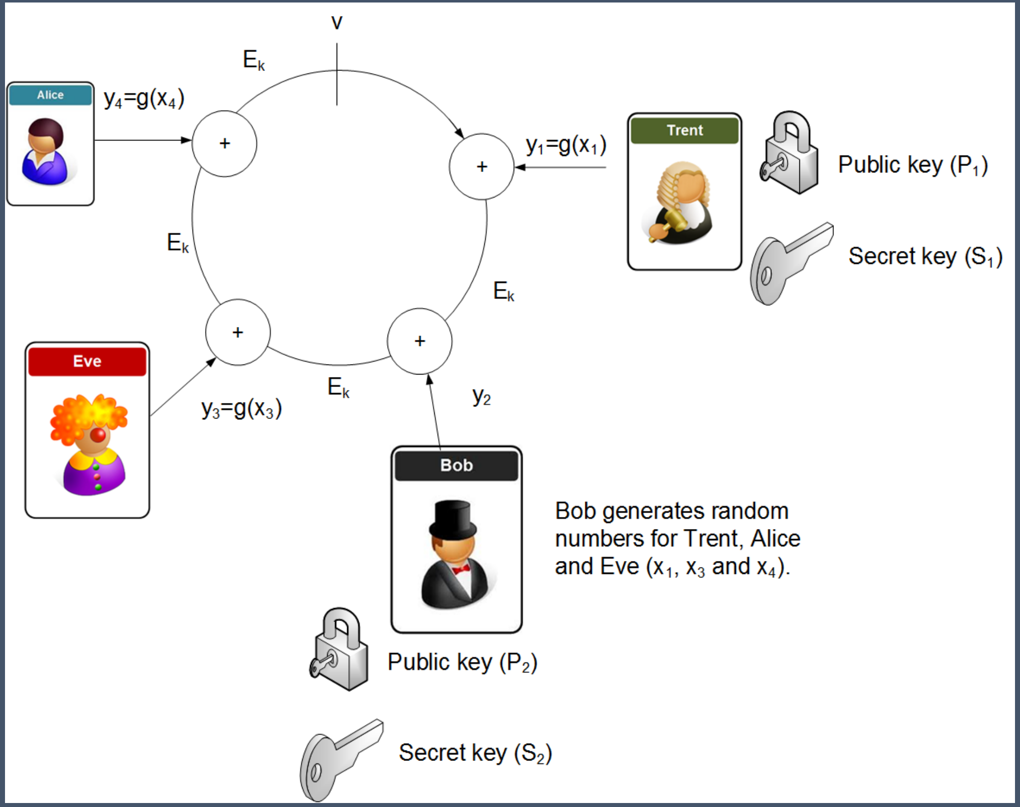


Homomorphic Encryption

This type of encryption allows operations to be performed on encrypted data. Imagine a scenario where the data is sent to a cloud server for processing. The server processes it and returns the output without knowing anything about the data that it has processed.

Tools and Techniques for Blockchain Privacy

- There are many tools and techniques to preserve privacy in blockchain systems:



Anonymous Signatures

Anonymous signatures are types of digital signatures where the signatures do not reveal the identity of the signer. There are primarily two schemes available for anonymous signatures:

- **Group signatures** allow a set of signers to form a group managed by a group manager.
- **Ring signatures** allow a set of signers to form a group (a ring) of members. Each member in this group is able to sign messages on behalf of the ring.

Summary of Blockchain Privacy

- Privacy is also important to the blockchain system.
- However, the nature of blockchain is not fit with the privacy requirements, since it requires nodes in the network to read and verify the transactions.
- There are two properties for blockchain privacy, i.e., ***anonymity*** and ***confidentiality***.
- There are two constraints to ensure the ***anonymity of users***, incl. *unlinkability* and *untraceability*.
- There are two methods to ensure the ***confidentiality of transactions***, incl. *conditional privacy*, and *selective disclosure*.
- Many **tools** and **techniques** were introduced to help preserving privacy in blockchain systems, such *TOR browser*, *IO*, *Homomorphic Encryption*, *Anonymous Signatures*, etc.

End of the lecture! 🥳

Please feel free to ask any questions.

If you need further discussion, please contact me:

- Email me at charnon@cmkl.ac.th
- Appoint me for 1-on-1 discussion during the office hours.