Smart Contracts Security

Ethical Hacking

Alessandro Brighente
Eleonora Losiouk

Master Degree on Cybersecurity

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

Distributed Ledger Technology

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- What is a Distributed Ledger Technology (DLT)?
- Blockchain is a DLT

A DLT is a decentralized record of data managed and maintained by multiple untrusted entities without the need of a regulator authority

Distributed Ledger Technology

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

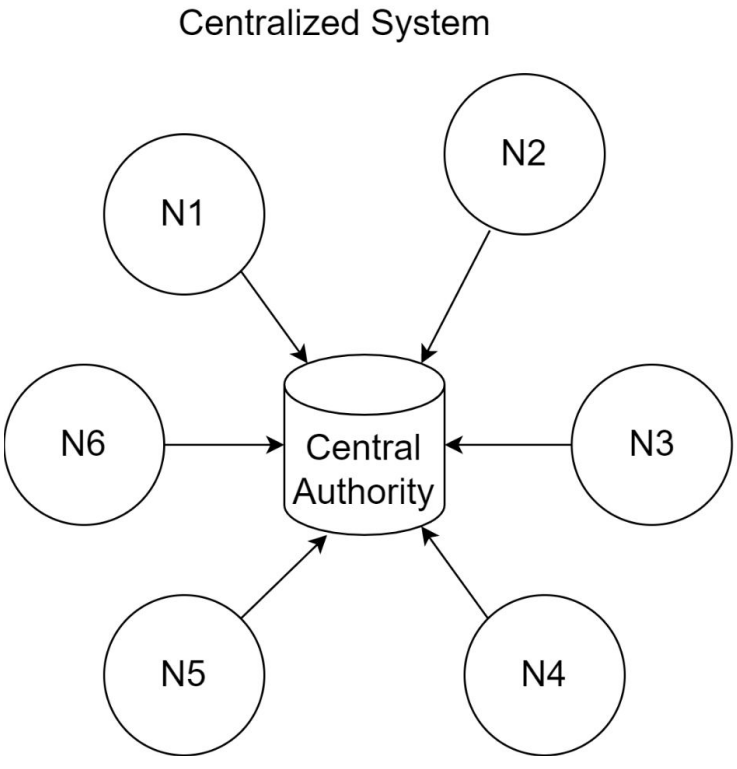
- What is a Distributed Ledger Technology (DLT)?
- Blockchain is a DLT

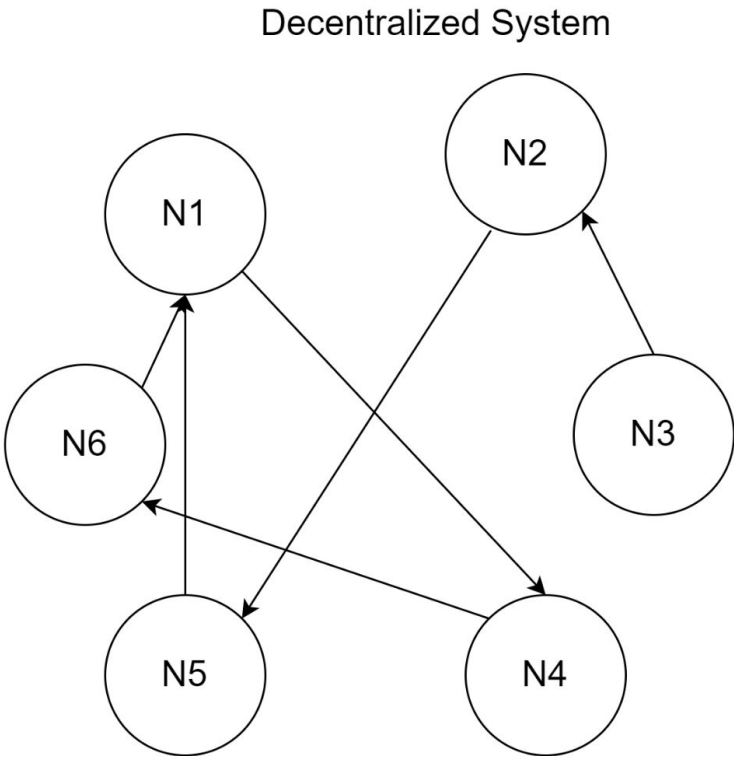
A DLT is a **decentralized** **replicated record of data**

managed and maintained by multiple **untrusted** entities

without the need of a regulator authority

Centralized vs. Decentralized





Decentralized

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- Each node (N1,N2,…) in a DLT holds its own copy of the ledger/record
- There is no central authority to which nodes in a DLT may refer to get updated information
- Each node in the DLT works to maintain and update its own copy of the ledger

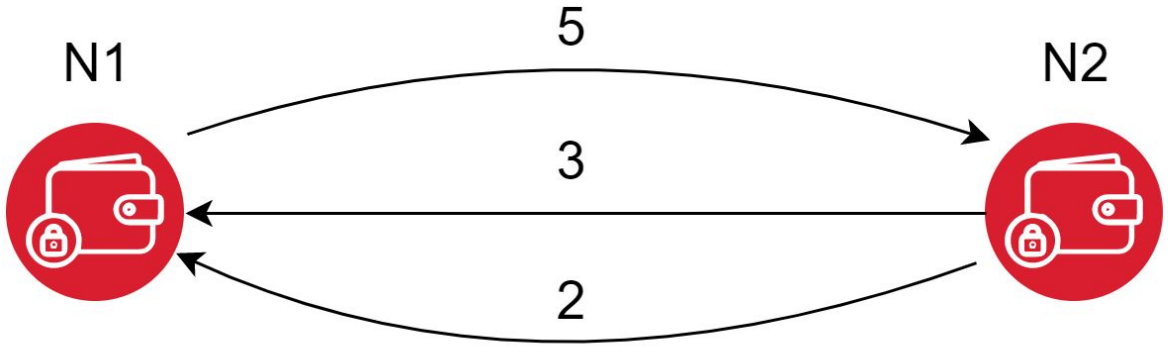
Replicated Record of Data

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- Data is organized in a list of records
- Each node replicates the list of records
- Each record represents a transaction (e.g., payment from N1 to N2)
- The last record defines the current **state** of the DLT
- DLTs can store any type of data:
  - Values
  - Contracts
  - Temperature value from an Internet of Things node
  - Intellectual property right

Record of Data



State update

Local Copy of the Ledger
1. N1 to N2: 5
2. N2 to N1: 3
3. N2 to N1: 2

Current state

Local Copy of the Ledger
1. N1 to N2: 5
2. N2 to N1: 3
3. N2 to N1: 2

Managed and Maintained

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- Each node has its own copy of the ledger
- Each node works to update its own copy
- Each node works for the benefit of the distributed ledger
- Copies may differ, so the majority hold the truth

Untrusted Members

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- Nodes do not trust other nodes in the network
- Each node directly communicates with other peer nodes in the network
- Each node has the same right to propose modifications to the ledger
- To provide immutability, the ledger follows an append only policy (no way to modify past states)

Blockchain

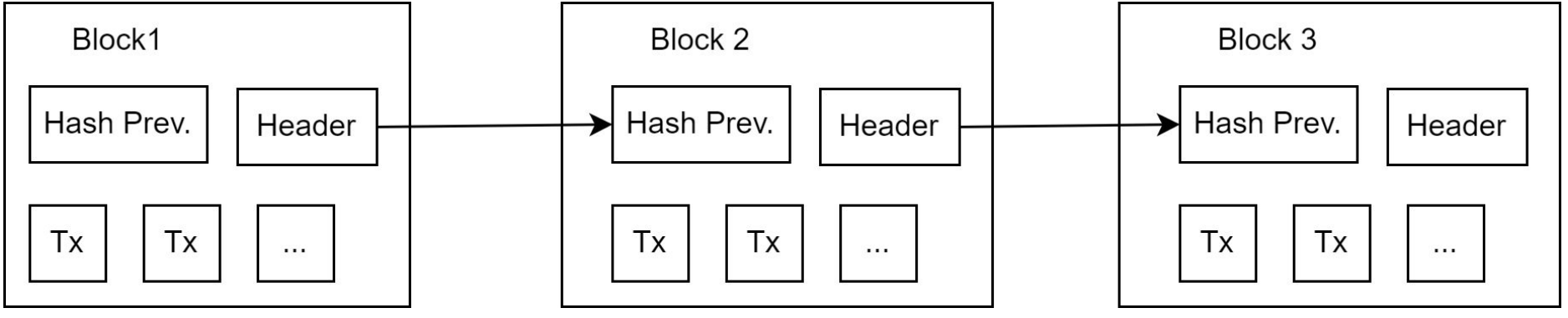
SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- How is Blockchain different from DLT?
- Transactions list are included in a block
- Blocks are organized on a chain
- Each block is cryptographically linked to the previous one

Blockchain

- Blocks are organized on a chain
- Each block is cryptographically linked to the previous one



Smart Contracts

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- A Smart Contract (SC) is a computer program stored in a blockchain that runs whenever specific conditions are met
- They follow simple if/when… then statements
- They are used to automate the execution of an agreement so that all participants can be immediately sure about the outcome
- No need for an intermediary party

Pragma ➔ version of solidity

```
// SPDX-License-Identifier: MIT
// compiler version must be greater than or equal to 0.8.20 and less than 0.9.0
pragma solidity ^0.8.20;

contract HelloWorld {
    string public greet = "Hello World!";
}
```

Smart Contracts

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- The SC code is compiled by the Ethereum Virtual Machine (EVM) and stored as bytecode in a transaction
- In order to interact with a smart contract, we need to send transactions to the SC address with specific data field that triggers the execution of certain functions
- Once the (possibly) triggered transaction is confirmed, the SC state is updated

ETH Wallet

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract EtherWallet {
    address payable public owner;

    constructor() {
        owner = payable(msg.sender);
    }

    receive() external payable {}

    function withdraw(uint _amount) external {
        require(msg.sender == owner, "caller is not owner");
        payable(msg.sender).transfer(_amount);
    }

    function getBalance() external view returns (uint) {
        return address(this).balance;
    }
}
```