Chapter 5

CONTRACT AND SMART CONTRACT

TP. HCM 2022

OVERVIEW

- Contract
- Smart Contracts
- Blockchain Design with Smart Contracts
- Brieft explanation of Dapps, Token, NFT
- Legal Issues

CONTRACT

promise or **performance**
given in exchange for
promise or **performance**

SMART CONTRACT

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

/**
 * @title Ballot
 * @dev Implements voting process along with vote delegation
 */
contract Ballot {

    struct Voter {
        uint weight; // weight is accumulated by delegation
        bool voted;  // if true, that person already voted
        address delegate; // person delegated to
        uint vote;   // index of the voted proposal
    }

    struct Proposal {
        // If you can limit the length to a certain number of bytes,
        // always use one of bytes1 to bytes32 because they are much cheaper
        bytes32 name;   // short name (up to 32 bytes)
        uint voteCount; // number of accumulated votes
    }

    address public chairperson;

    mapping(address => Voter) public voters;

    Proposal[] public proposals;

```

Code is law

SMART CONTRACT

"A set of promises, specified in digital form, including protocols within which the parties perform on these promises."

Nick Szabo, 1996

However…

- Smart Contracts may not be "**Smart**"
- Smart Contracts may not be "**Contracts**"

SMART CONTRACT

"A set of promises, specified in digital form, including protocols within which the parties perform on these promises."

Nick Szabo, 1996

However…

- Smart Contracts may not be "**Smart**"
- Smart Contracts may not be "**Contracts**"

SMART CONTRACT

- Replaces traditional contracts in blockchain context
- Authority-less autonomous program, that directly controls numeric securities (digital assets), based on mutually agreed terms
- Looks like “if-then” instructions that automatically evaluate predefined conditions and do transactions
- Has an owner and a life cycle, and is executed on Ethereum Virtual Machine (EVM)

SMART CONTRACT

Pros

- Immutability characteristic
- Autonomy and automaticity characteristics

Cons

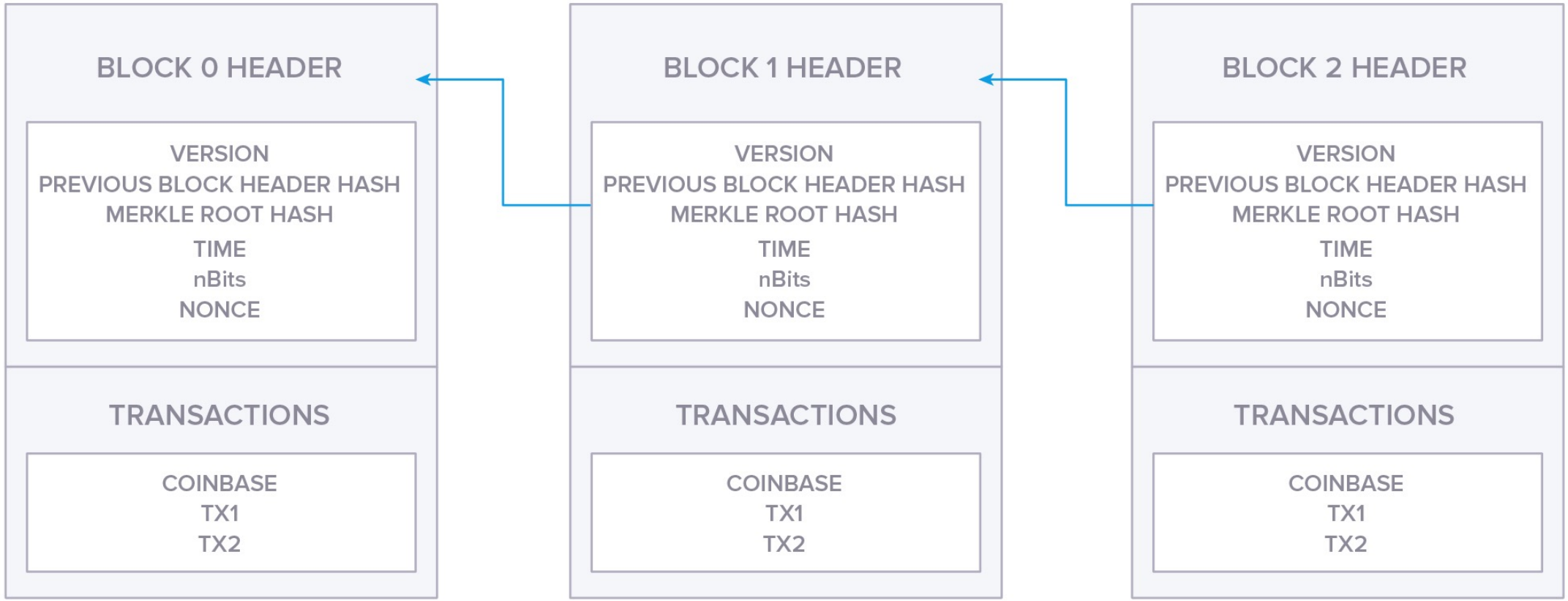
- Not suitable for all kinds of contracts
- Simple and only include “if a, then b” patterns

BUGS???

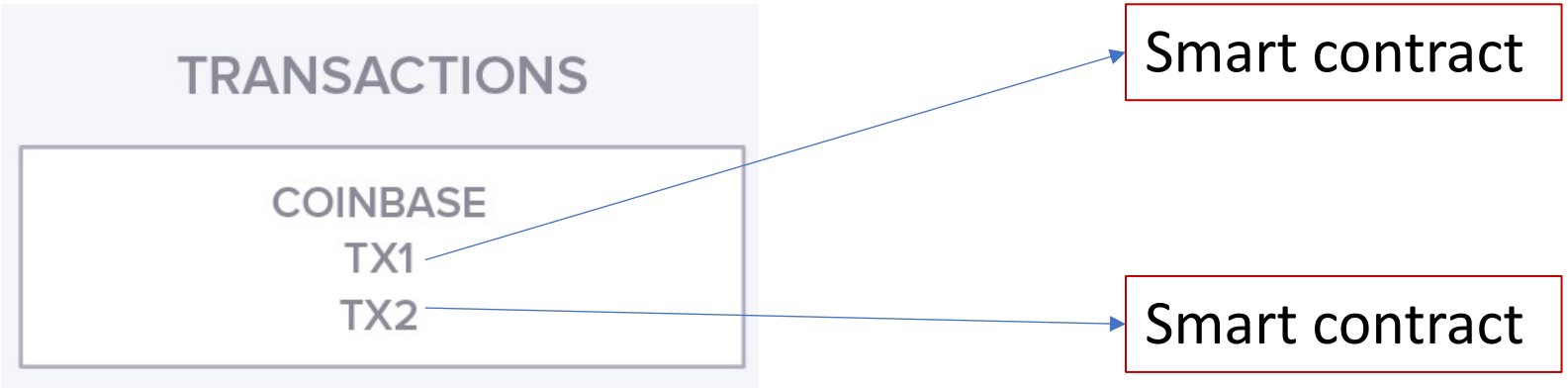
INTERACTING WITH A SMART CONTRACT

- Smart contract is not self-executable
- It requires an external call to be executed. Otherwise, it is pending till one calls one of its implemented functions
- Once it is executed, transactions resulting from the execution are transcribed on the blockchain and eventually smart contract's meta data are updated

BLOCKCHAIN DESIGN WITH SMART CONTRACTS



BLOCKCHAIN DESIGN WITH SMART CONTRACTS



Smart contract execution may or may not change blockchain state

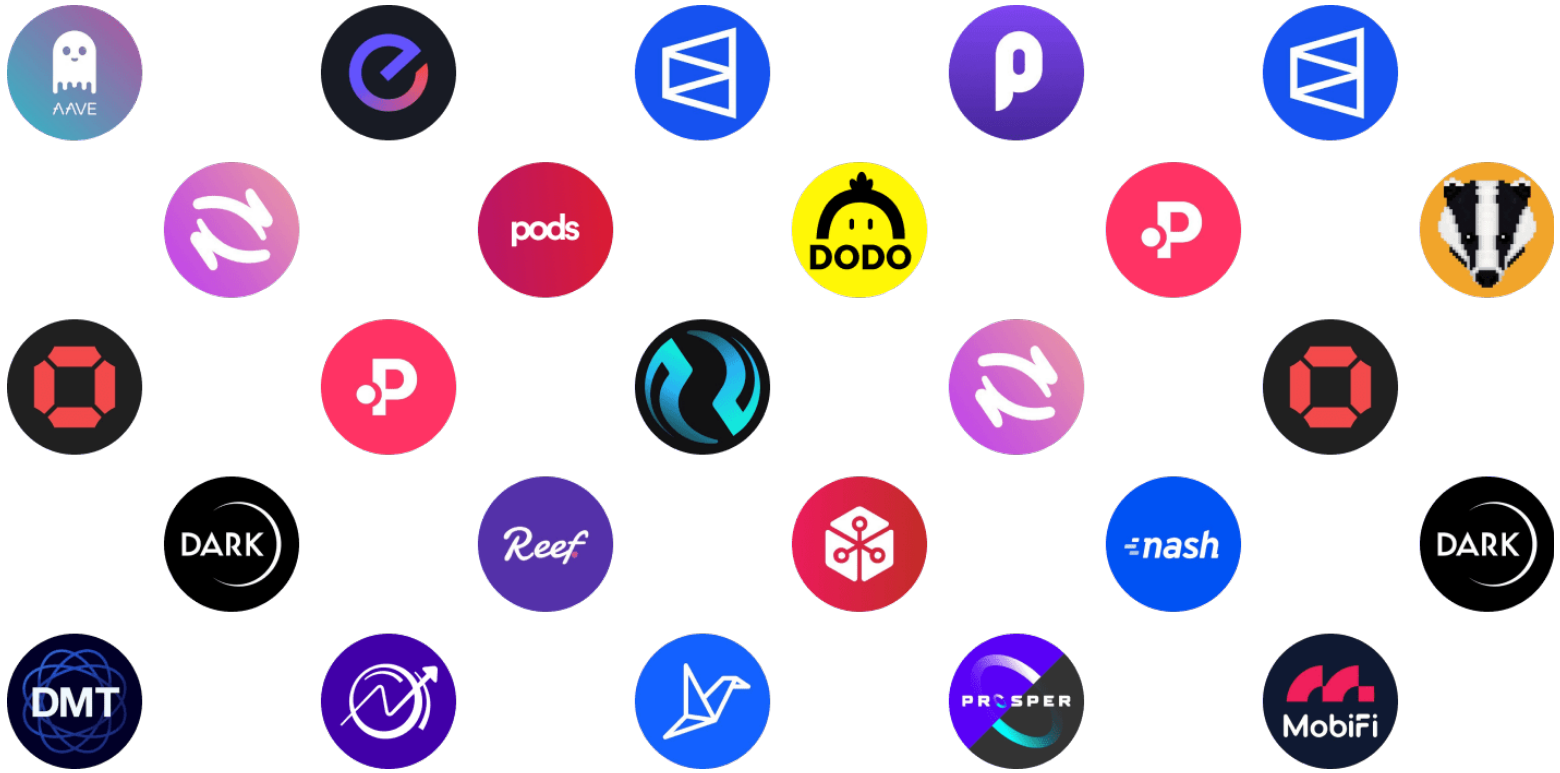
USE CASES

- Lending & borrowing
- Security
- Mortgage
- Supply chain
- Trade finance
- …

DAPPS & TOKEN

Dapps

- Applications run on a Decentralized Blockchain Network
- They generally have a Native Token & Run as a Smart Contract



https://dappradar.com/

NFTs

- NFTs (non-fungible tokens) are unique cryptographic tokens that exist on a blockchain and cannot be replicated.
- NFTs can represent real-world items like artwork and real estate.
- "Tokenizing" these real-world tangible assets makes buying, selling, and trading them more efficient while reducing the probability of fraud.
- NFTs can also function to represent individuals' identities, property rights, and more.

INITIAL COIN OFFERING (ICO)

- Proceeds used to build networks
- Tokens usually issued prior to being functional
- Development, while open source, is largely centralized
- Promoters allocate themselves ‘premined’ tokens
- Tokens are fungible & transferable
- Scarcity is fostered with preset ‘Monetary policy’
- Purchasers anticipate profits through appreciation

INITIAL COIN OFFERING (ICO)

Advantage:

- Young enterprises do not have to wait for months before having the "go" of an investment fund

Disadvantages:

- Difficult to verify the relevance and quality of a project that does not exist yet
- Absence of control authority to regulate the market "anyone can issue a digital title, so there are mechanically a lot of scams of all kinds"
- Volatility of cryptocurrency can quickly raise or lower the amount raised depending on the technical developments of the platform and of other exceptional events

DISCUSSION

READINGS

- Enterprises building Blockchain Confront Early Tech Limitations
- Technical difference between Ethereum, Hyperledger fabric and R3 Corda
- ‘What is Corda?
- A Blockchain Plaform for the Enterprise, Introduction
- What is Digital Asset? / Distributed Ledgers for Financial Institution