LECTURE 3

ICO BASICS

TOPICS

- Definition
- Origins
- History
- Standard Structure

ICO DEFINITION

An unregulated means by which funds are raised for a new cryptocurrency venture. An Initial Coin Offering (ICO) is used by startups to bypass the rigorous and regulated capital-raising process required by venture capitalists or banks.

In an ICO campaign, a percentage of the cryptocurrency is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, but usually for Bitcoin.

Source: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

ORIGINS AND SHORT HISTORY

- Originated from Crowd sourcing and community projects
- Born from:
  - The frustration of dealing with VCs
  - The desire to implement use cases less popular with traditional investors
- Got hijacked by its own success. Scams at every level.
- Constantly evolving

ICO MILESTONES

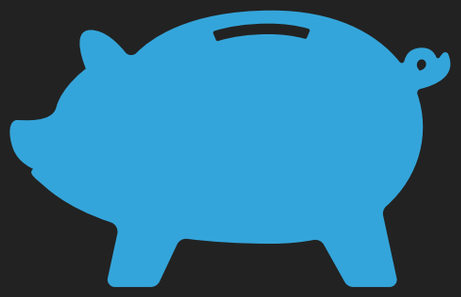
- 2013 July: Mastercoin. The first ICO.
- 2014 August: Ethereum ICO. Raised 31,519 BTC, 18m USD at that time. 429 million today.
- 2015 August: Augur ICO, already on the Ethereum network.
- 2016: 14 ICOs raised 62 million dollars
- 2017: 92 ICOs raised 2.2 billion dollars

ICOS

STANDARD STRUCTURE

- ERC-20 contract
- Multisig wallet
- ICO contract

MULTI SIGNATURE WALLETS

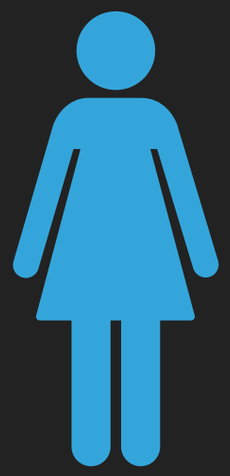


Wallet address

MULTISIG WALLET

ICO CONTRACT

Recipient



Owner 1

Owner 2

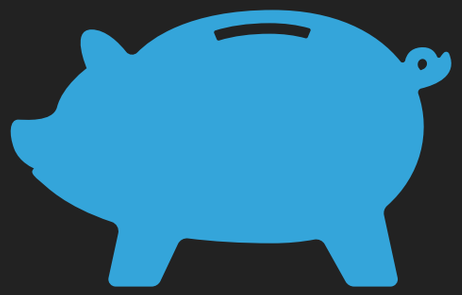
ERC-20 CONTRACT

```
1  // ----------------------------------------------------------------------
2  // ERC Token Standard #20 Interface
3  // https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
4  // ----------------------------------------------------------------------
5  contract ERC20Interface {
6      function totalSupply() public constant returns (uint);
7      function balanceOf(address tokenOwner) public constant returns (uint balance);
8      function allowance(address tokenOwner, address spender) public constant returns
(uint remaining);
9      function transfer(address to, uint tokens) public returns (bool success);
10     function approve(address spender, uint tokens) public returns (bool success);
11     function transferFrom(address from, address to, uint tokens) public returns (bool
success);
12
13     event Transfer(address indexed from, address indexed to, uint tokens);
14     event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
15 }
```

```
1      string public constant name = "Token Name";
2      string public constant symbol = "SYM";
3      uint8 public constant decimals = 18;  // 18 is the most common number of decimal
places
```

ICO CONTRACT

ERC 20 CONTRACT

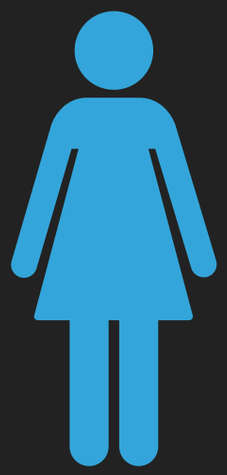


Wallet address

MULTISIG WALLET

ICO CONTRACT

Contributor



Owner 1

KYC PROCESS

Wallet address

MULTISIG WALLET

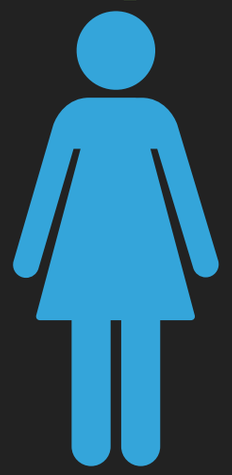
ERC 20 CONTRACT

ICO CONTRACT

Presale Contributor

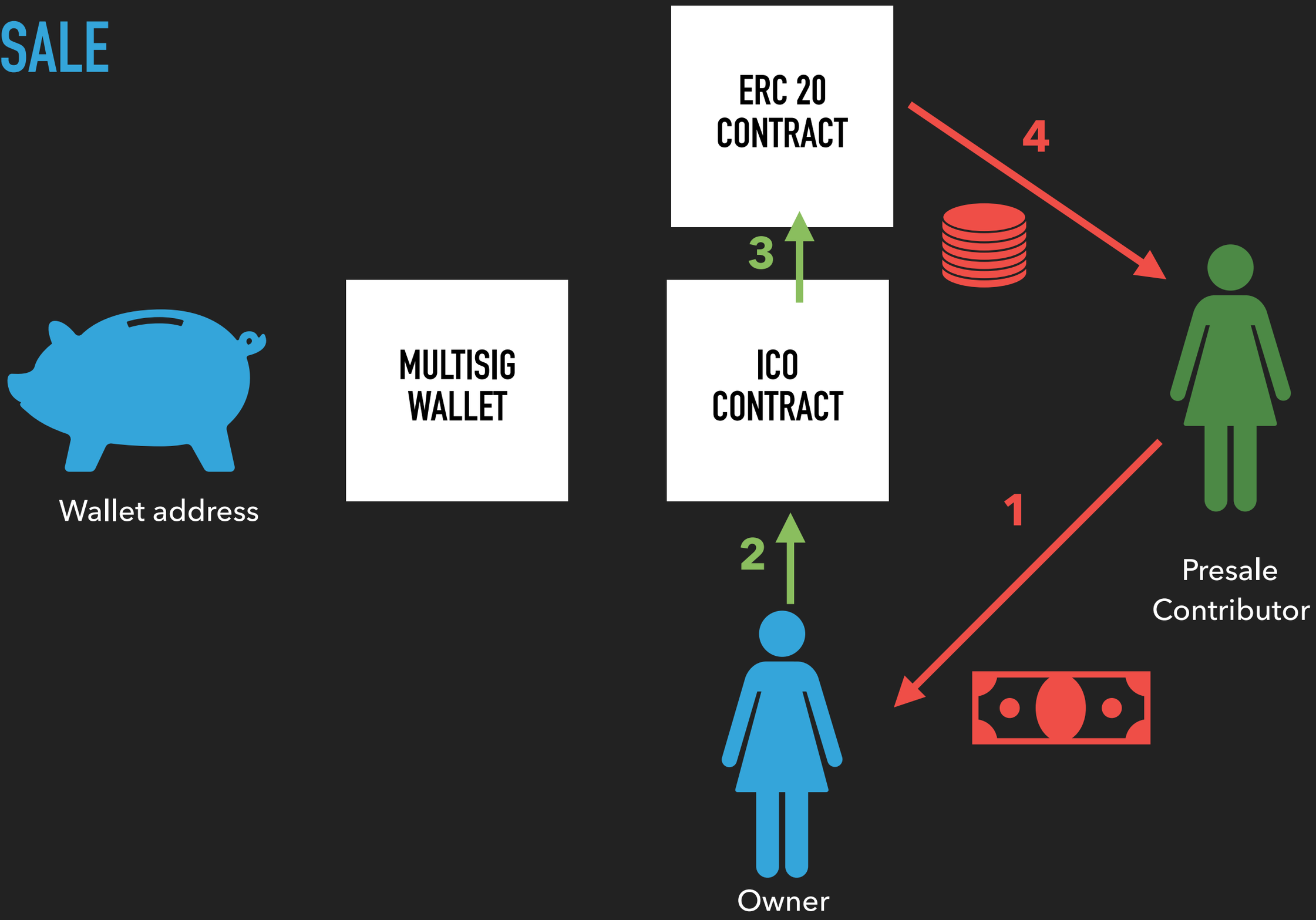
1

2

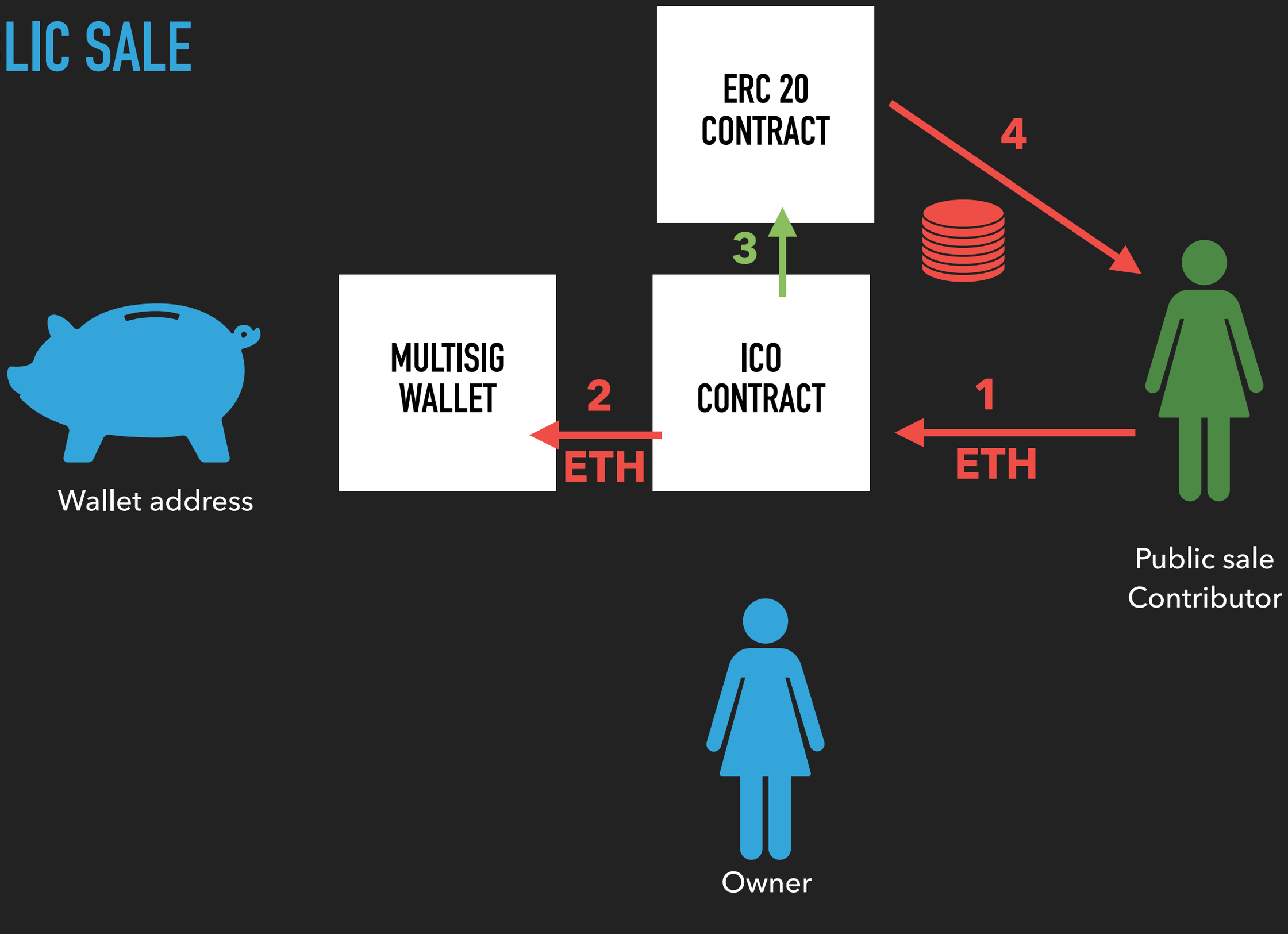


Owner

PRESALE


ERC 20
CONTRACT
4
3
MULTISIG
WALLET
ICO
CONTRACT
Wallet address
2
1
Presale
Contributor
Owner

PUBLIC SALE


ERC 20
CONTRACT
4
3
MULTISIG
WALLET
2
ETH
ICO
CONTRACT
1
ETH
Wallet address
Public sale
Contributor
Owner

TOKEN DISTRIBUTION STRATEGIES

Different way to distribute the tokens to contributors:

- Simple ratio
- Time-based tiers
- Amount-based tiers
- Capped or uncapped sales
- Dutch Auction
- Interactive Coin Offering

THE CONTRIBUTION PHASE

SIMPLE RATIO

- During the sale, every contributor gets X amount of ICO tokens for every ether.
- Rarely used alone, usually used together with tiers

TIME BASED TIERS

ICO is divided to tiers by dates. If – let's say – the ICO is open for 4 weeks, then during the first week contributors get 25% more, then 15, 5 and 0 % more, every week.

AMOUNT BASED TIERS

Similar to time - based tiers, but the tiers work based on how much of the hard cap is sold off.

With amount based tiers, the first tiers might get sold out in minutes.

CAPPED VS UNCAPPED SALE

- Decision needs to be made before the ICO
- Capped sale potentially prevents everyone from participating
- Uncapped sale makes it difficult to account with money

DUTCH AUCTION

- Price starts high and are dropped successively until all the tokens are sold.
- In principle, it helps that both big investors and small investors can participate as well
- In practice, it depends on the demand

INTERACTIVE COIN OFFERING

No token crowdsale satisfies that both: (i) a fixed amount of currency buys at least a fixed fraction of the total tokens, and (ii) everyone can participate.

fixed valuation scheme cannot guarantee universal participation

aims to establish an equilibrium of purchase amounts whose sum is satisfactory to all buyers at some uniform valuation.

1. buyers can withdraw their contributions after committing them to the sale (within certain limits), and

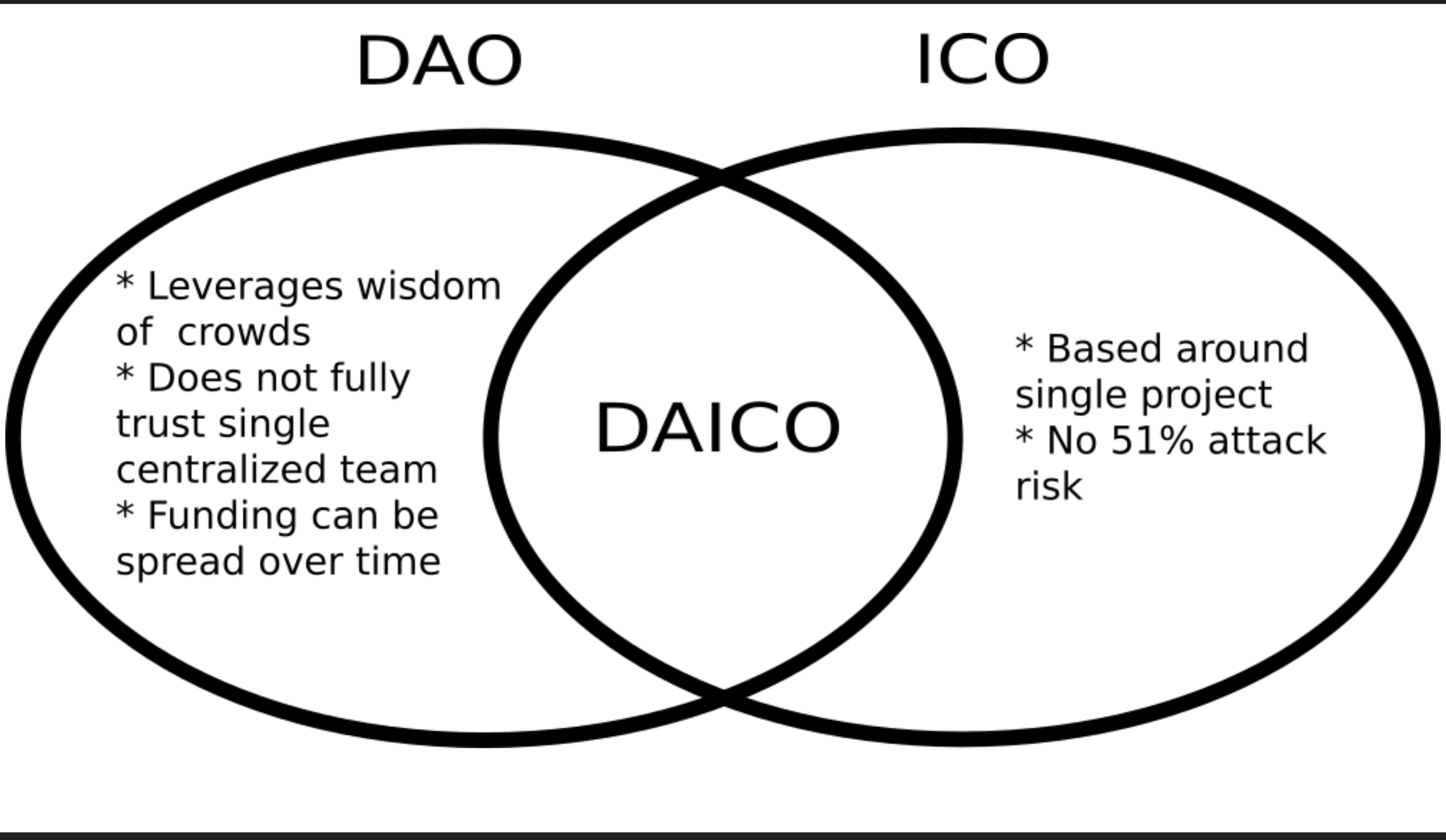
2. the protocol exploits sophisticated bookkeeping capabilities of smart contracts.

INTERACTIVE COIN OFFERING

- Basic step: In each block epoch, buyers can either purchase tokens or voluntarily withdraw funds from the crowdsale. Buyers specify a maximum sale valuation at which they are willing to participate, and if the sale amount ever reaches this personal threshold, the buyer's bid is canceled and she receives a refund. In Section 7, we add support for bid activation triggered by sale lower bounds.
- Withdrawal lock: After a certain number of blocks, voluntary withdrawals are no longer permitted. In a 30-day crowdsale, for example, the smart contract might permit voluntary withdrawals during the first 20 days, but during the last 10 days, only automatic withdrawals are allowed.
- Inflation ramp: Buyers who purchase tokens early receive a discounted price. The maximum bonus might be 20% (a typical amount for crowdsales today). The bonus decreases smoothly down to 10% at the beginning of the withdrawal lock, and then disappears to nothing by the end of the crowdsale.

THE DEVELOPMENT PHASE

DAICO — ACCOUNTABLE DEVELOPMENT



THANK YOU

TWITTER, MEDIUM: @AKOMBA, EMAIL: A@AKOMBA.COM