OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

DAOs – Decentralized Autonomous Organizations

Thomas Bocek

22.10.2023

What is a DAO?

- A Decentralized Autonomous Organization (DAO) is a community-led entity with no central authority
  - Autonomous and transparent
  - Smart contracts define rules
  - Smart contracts execute rules
  - Anyone can audit proposals, voting
- DAO is governed entirely by its individual members
  - Technical upgrades
  - Project funding / treasury allocations

- Simplified: Members create proposals, member vote on the proposal, proposal gets executed
  - Characteristics: decentralized, transparent, autonomous, open source [link]

Decentralized autonomous organizations (DAOs)

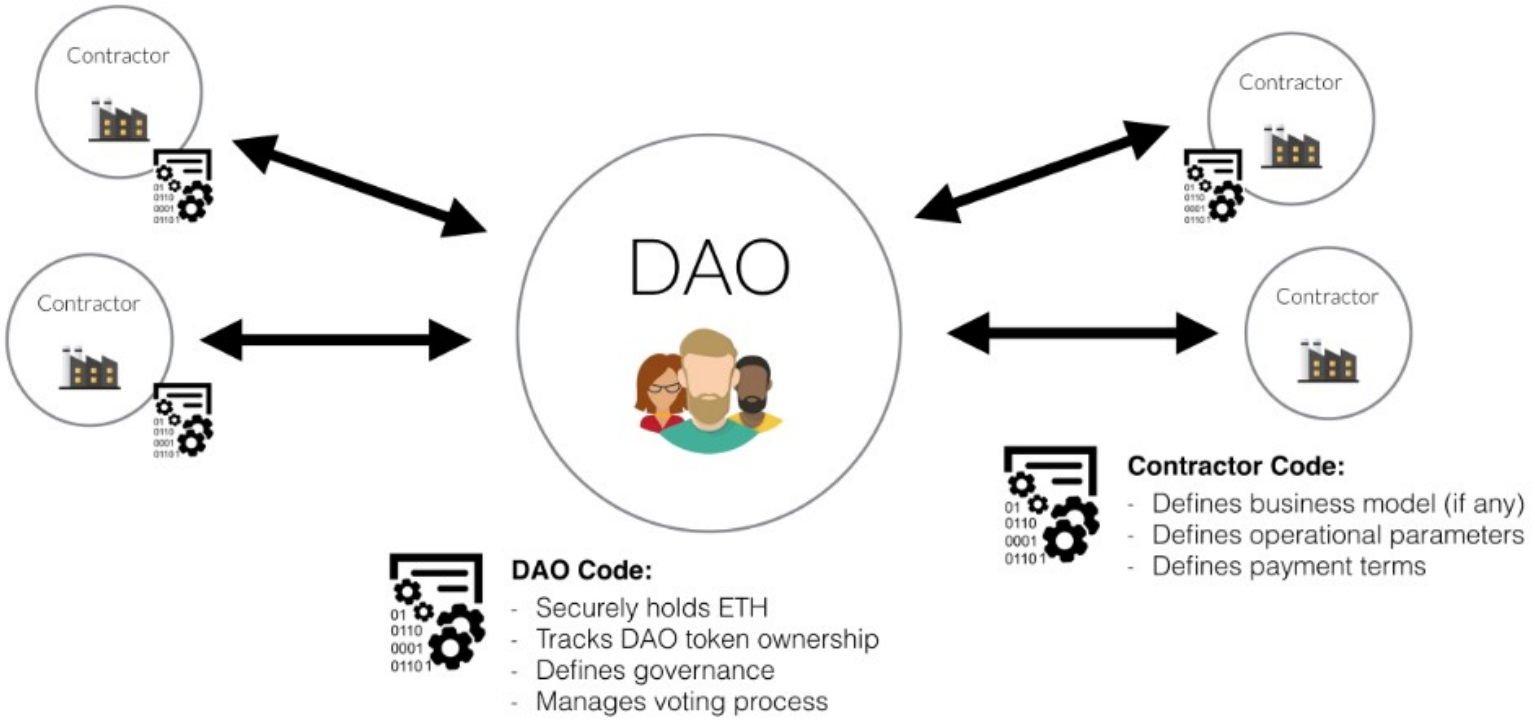
- Member-owned communities without centralized leadership.
- A safe way to collaborate with internet strangers.
- A safe place to commit funds to a specific cause.

https://ethereum.org/en/dao/

OST

History: The DAO

- The first DAO was a disaster (from an economic point of view). It was a success (from an experimental point of view)
- Launched April 2016
  - More than 10’000 investors, more them $150 mio funds raised

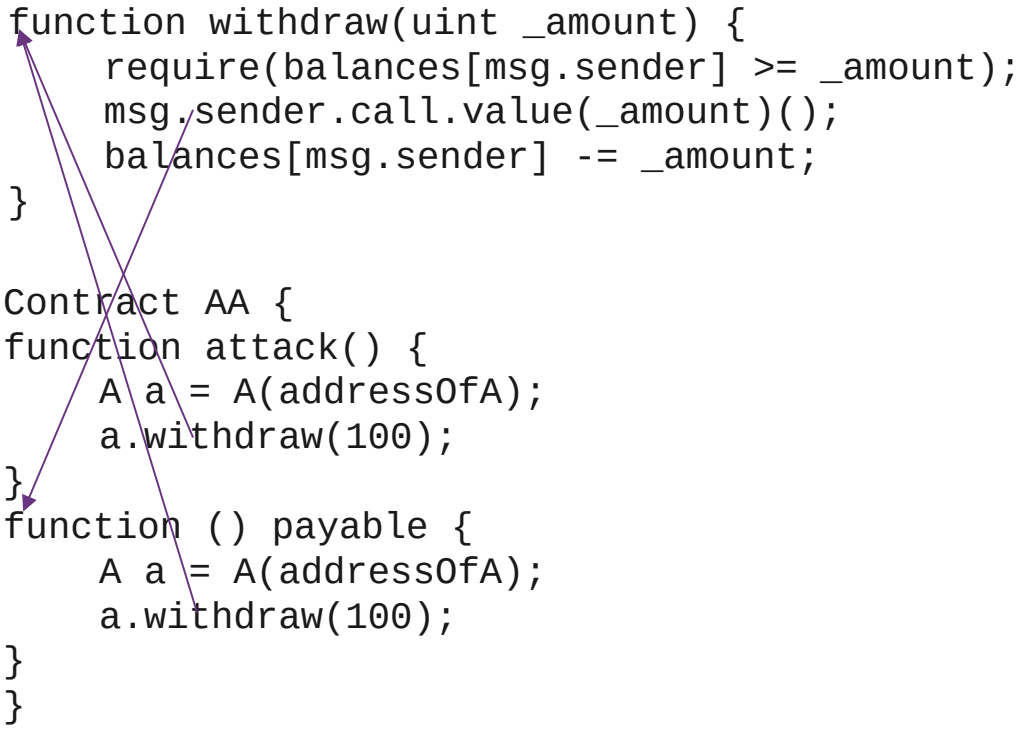


http://www.unine.ch/files/live/sites/ccfi/files/Colloques/Conf%C3%A9rence%204%20oct%202016/Pr%C3%A9sentations/Alexis%20Roussel%20pr%C3%A9sentation%204102016.pdf

OST

History: The DAO

- Smart contract had flaws
  - Investors invested 15m ETH, attacker could drain 3.6m ETH (worth $70 mio at that time)
- What happened?
  - Reentrancy attack: call a function again, before the state is updated
  - Small mistake, huge consequences
  - OpenZeppelin ReentrancyGuard
- Many discussion how to react
  - ETH price dropped from $20 to $13
  - Attackers said they did nothing wrong, they followed the rules of the smart contract



```
function withdraw(uint _amount) {
    require(balances[msg.sender] >= _amount);
    msg.sender.call.value(_amount)();
    balances[msg.sender] -= _amount;
}

Contract AA {
function attack() {
    A a = A(addressOfA);
    a.withdraw(100);
}
function () payable {
    A a = A(addressOfA);
    a.withdraw(100);
}
}
```


OST

History: The DAO

- Still controversial: Vitalik Buterin (co-founder of Ethereum) proposed fork to blacklist the hacker
  - Many agreed, so fork was implemented
  - History of Ethereum was altered (immutability!)
  - Smart contract security is super important
    - No contract on mainnet without external review
- Ethereum fork with the blacklist: Ethereum Classic [link]
  - On this chain the attacker still has access to the funds
- The DAO hack address were blacklisted with a hard fork on the 20. July 2016
- **Rumors** about the DAO hacker
  - Toby Hoenisch [link]
  - Demixer from Chainalysis used to demix CoinJoin (mixer) transaction [link]

https://en.wikipedia.org/wiki/The_DAO_(organization)

OST

DAO vs. Regular Organizations

- Advantages
  - Decisions by individuals rather than central authority
  - Encourages participation
  - Public: everything is transparent and visible
  - Minimum requirement to join, is an Internet connection
- Disadvantages
  - Decisions and voting takes time
  - Currently only tech-savy people participate
  - Bridging blockchain with real world
  - Security considerations

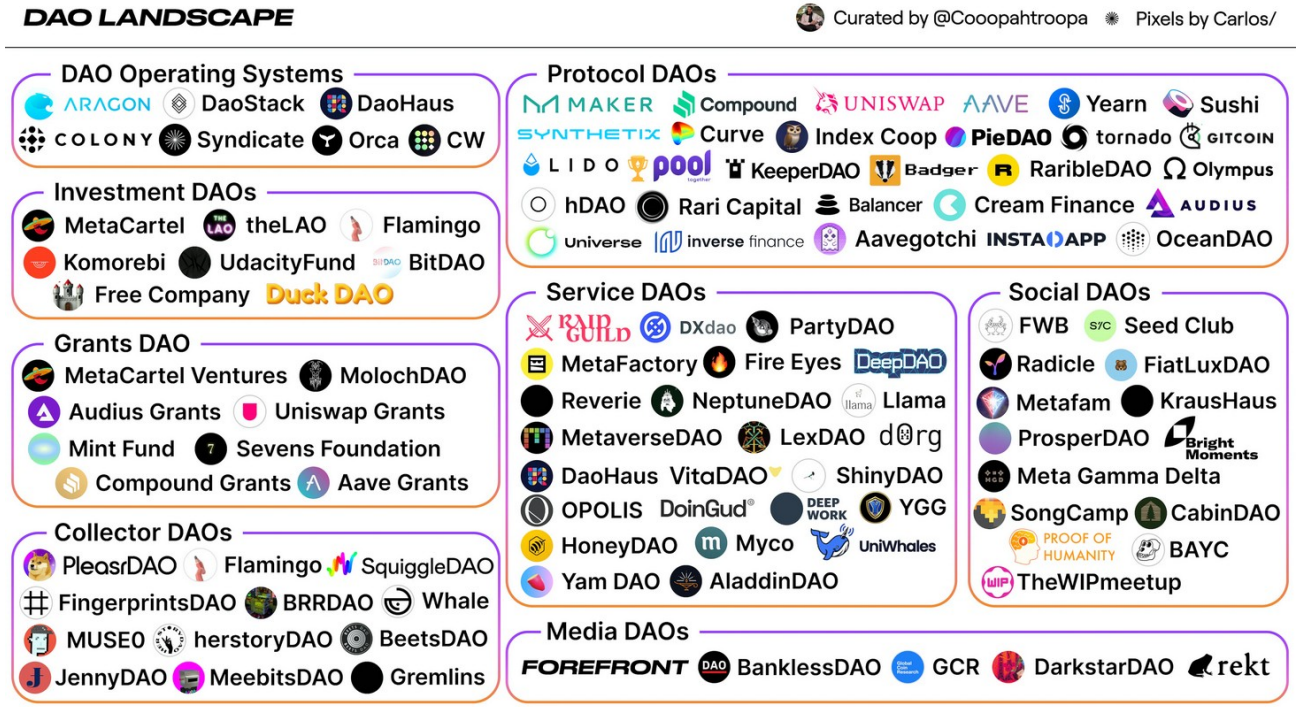
	Corporation	Cooperative	DAO
Management	Board of directors	Board of members	Token holders
Ownership	Shareholders	Members	Token holders
Supervision	Supervisory board	Supervisory board team	Curators
Workforce	Employees	Members	Contractors

https://www.slideshare.net/jbrejcha/decentralized-autonomous-organizations-concept-practical-examples

OST

DAO Examples

- Grants DAOs
  - Communities donate funds and use a DAO to vote on how that capital is allocated
- Protocol DAOs
  - Chains use DAO to let community vote on direction of protocol
- Investment DAOs
  - Investment clubs for generating returns
- Service DAOs
  - Service DAOs create funnels to contract web3 talents
- Social DAOs
  - Focus on social capital over financial capital
- Collector DAOs
  - Collectors club to collect NFTs



https://coopahtroopa.mirror.xyz/_EDyn4cs9tDoOxNGZLfKL7JjLo5rGkkEfRa_a-6VEWw

OST

DAO Examples

- Uniswap, popular decentralized exchange (DEX), since 2020, organized as DAO
- MakerDAO, the DAO that supports the crypto stablecoin DAI
- The Bored Ape Yacht Club, enter social club if you own bored ape [link]
- Curve DAO, a blockchain-based decentralized exchange and automated market maker [link]
- ConstitutionDAO, experiment of a single-purpose DAO, tried to purchase an original copy of the United States Constitution, but lost the bid [link]

UNISWAP
Governance

1Ð ≈ $1

BORED APE
BA YC
YACHT CLUB

Curve

OST

DAO Implementation

- OpenZeppelins Governor contract
  - Customizable, wizard
  - Flexible

```
propose(address[] targets, uint256[] values, bytes[] calldatas, string description) → uint256 proposalId
```

public #

Create a new proposal. Vote start `IGovernor.votingDelay` blocks after the proposal is created and ends `IGovernor.votingPeriod` blocks after the voting starts.

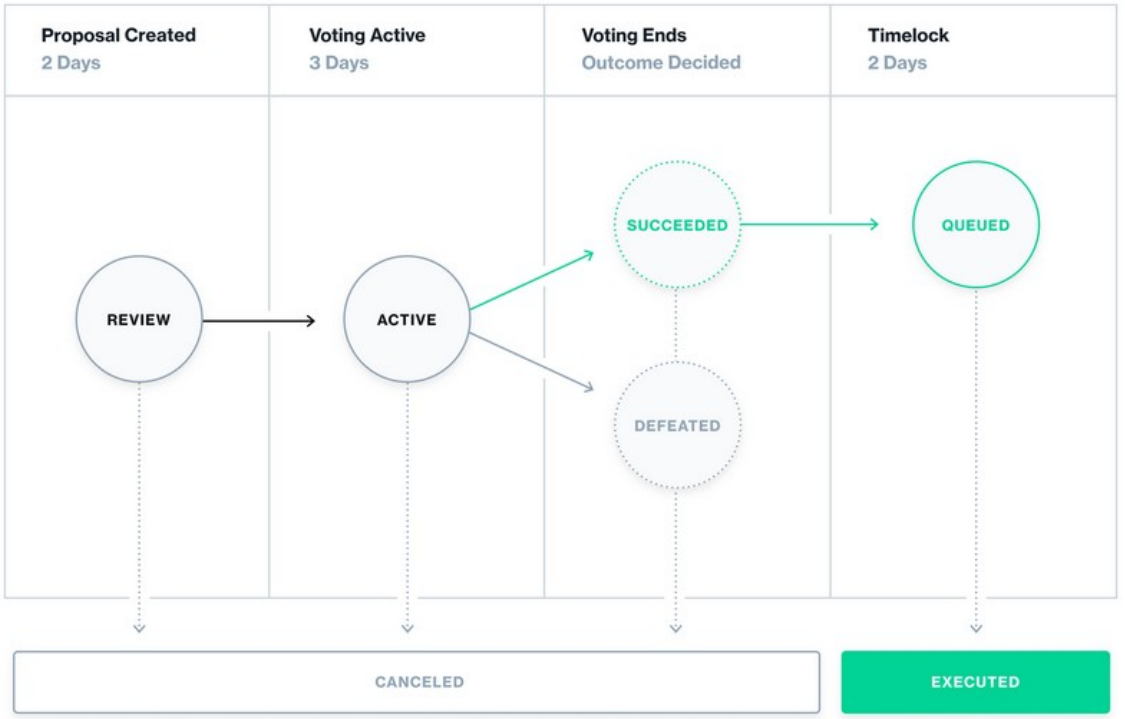
Emits a `ProposalCreated` event.

```
castVote(uint256 proposalId, uint8 support) → uint256 balance
```

public #

Cast a vote

Emits a `VoteCast` event.



https://docs.compound.finance/v2/governance/

OST