

A black and white photograph of the MIT Great Dome at night. The dome is brightly lit from within, casting a glow on the surrounding trees and the building's facade. The sky is dark.

Smart Contracts

Abel Sanchez, John R Williams

MIT

MIT Campus | Cambridge, MA



CONTRACTS

Sumerian contract
Selling field & house
Circa 2600 BCE



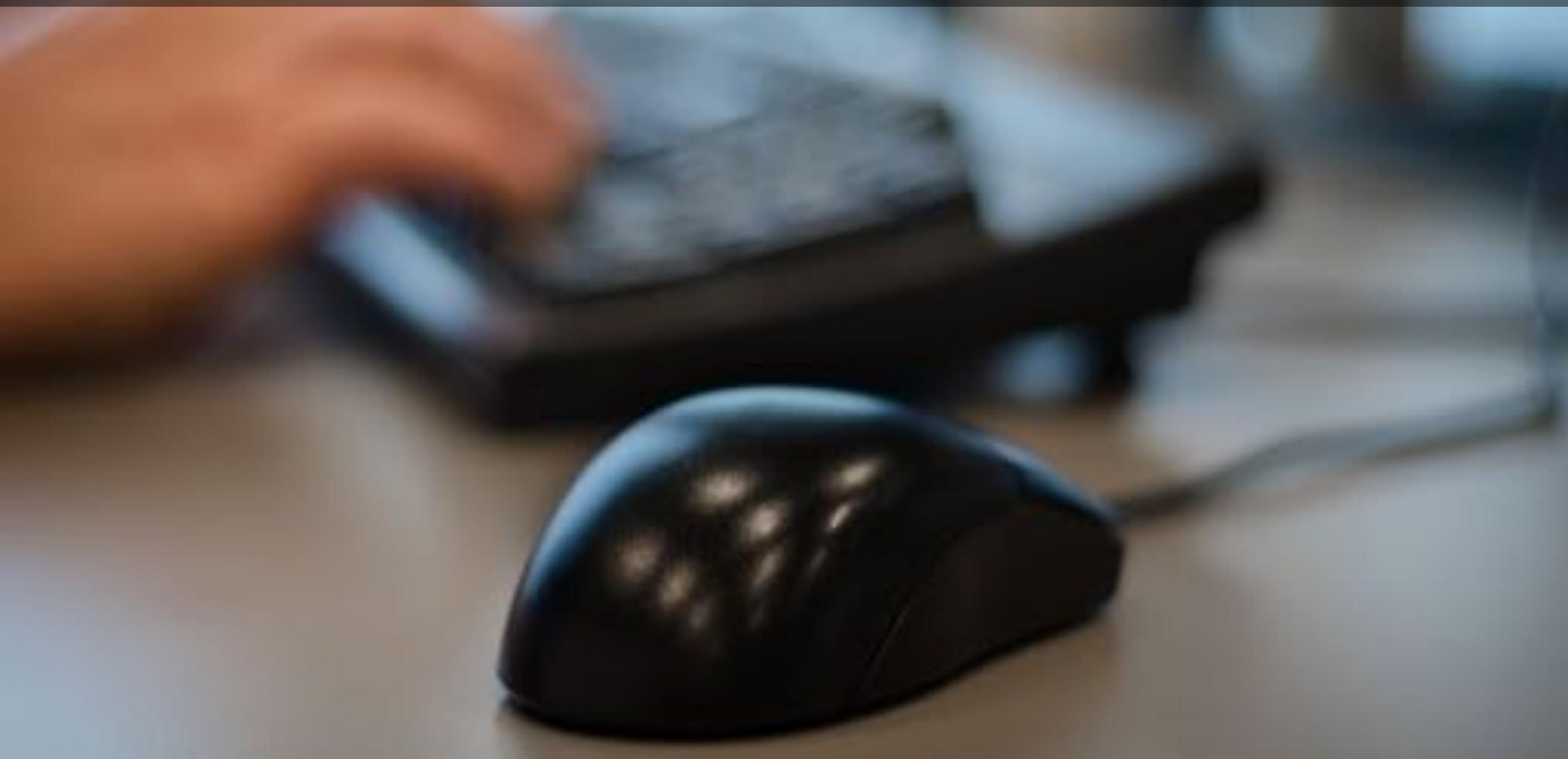
Papyrus Contract Marriage 4th BCE





A contract is an agreement between two or more parties that is enforceable by law

Building Block of Market Economy



We Live in a World of Paper

A photograph showing a massive, sprawling pile of papers and files on a desk. The papers are stacked high in several places, creating large, undulating hills of paper. Some papers have black clips holding them together. In the background, there's a computer monitor, some office equipment, and a small orange toy figure standing on the desk. The overall impression is one of overwhelming paperwork and clutter.

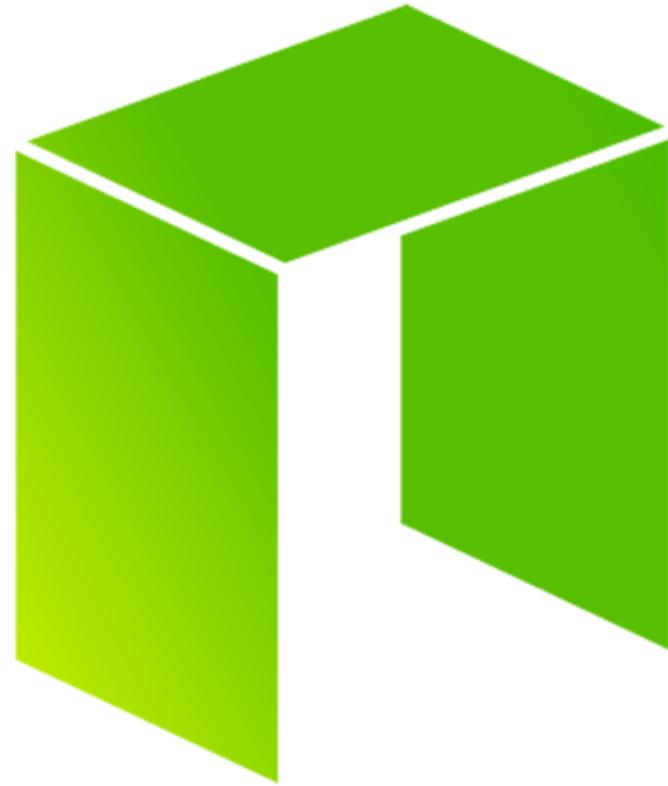
Connecting CONTRACT To Virtual WORLD



SMART CONTRACTS



Smart contract platforms





TWO BIG IDEAS

Nakamoto Blockchains

- First idea
 - Tokens as money
 - Peer-to-Peer
 - Foundation on cryptography
- Second idea
 - Database
 - Multiple writers
 - Absence of trust
 - Disintermediation
 - Chain of custody
 - Validation

Bitcoin – Great at one thing

- Great at one thing
- Forks working on extensions
- Challenging as not a platform

Smart Contract Platforms

- A platform vision
- A redesigned blockchain
- State and transaction separation
- Turing complete programming language

What is a contract?

- Code that lives inside blockchain
- Has an address and a balance
- Executes when it receives a transaction
- You can send money to contracts
- You can send messages to contracts
- On invocation, code executes

Contract Limitations (Implementation Dependent)

- Virtual Machine constraints
- Gas limits
- High costs
- Cannot reuse existing libraries (financial, ML, etc.)
- No confidentiality/privacy
- Scalability



POVERTY

Hernando de Soto



The formal, legal world

- Citizens can prove who they are
- People and businesses have legal addresses and identities
- Property titles and registries allow everyone to know who owns what
- Articles of incorporation enable investors and customers to know who they are buying and selling from
- Legal contracts are binding and enforceable



The CHOOSE.
NETWORK

The poor and extralegals

- The poor's assets cannot be easily represented
- People are not easily held accountable for their commitments
- Assets are not liquid, cannot be used to create credit or capital
- People are not as interconnected across distances
- Transactions cannot easily be tracked from one owner to next
- The poor do not have the means to divide labor and control risks
- Limited liability and corporations out of reach
- People cannot be identified
- Contracts are unable to reach external markets

Core Challenges

- Identity
- Contracts
- Payment

IDENTITY

Plit

Identities Today are Siloed and Vulnerable



Identity Silos Centralized Servers



- Education
- Car Insurance
- Health Care
- Tax Reports
- Social Media



* Within same institution
Multiple accounts



Challenges For Organizations

- Visibility
- Interoperability
- Cybersecurity



For Individuals

- Physical documents
- Management Burden
- Repetition of information
- Personal Information Leaks
- Identity Theft

Identity with blockchain contracts

- Blockchain identity
 - Managed by user
 - Data owned by user
 - Collection of credentials



- Data
 - Verified claims/attestations (citizenship, visa, certificates)
 - Data standards, data schema
 - Granular disclosures
 - Possible to establish multiple identities/reputation

Timestamp
Recipient ID
Claim Data
Issuer ID
Issuer Signature
History
Reputation

Adoption Example - uPort

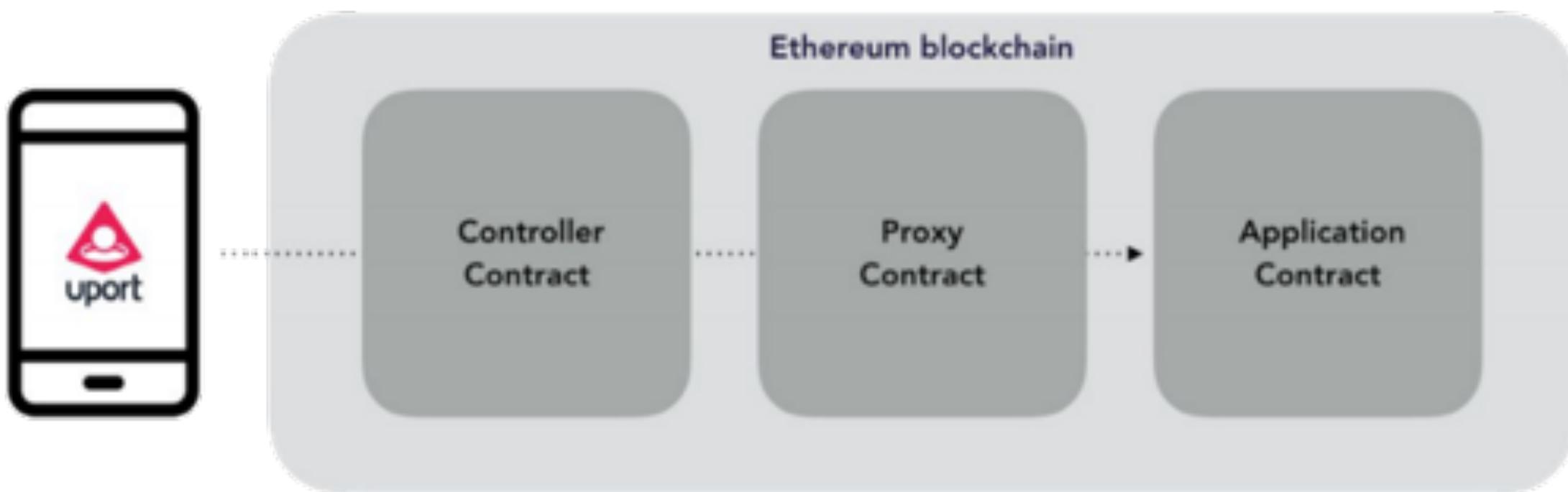
1. End-users
2. Developers
- 3. Dapps**
4. Exchanges
5. Enterprises
6. Governments



Swiss City of Zug, First self-sovereign government issued identity on blockchain



Architecture Overview



Decentralized Identity Foundation (DIF)

DECENTRALIZED IDENTITIES

anchored by

BLOCKCHAIN IDs

linked to

ZERO-TRUST DATASTORES

that are

UNIVERSALLY DISCOVERABLE

<http://identity.foundation>





scn

ASHISH GADNIS - Co-FOUNDER / CEO
BANQU INC.

153015.16 202004061 22.67 13.73
230560.34 579188246 2.18 12.89
102833.56 187796711 20.16 15.76

INITIAL COIN OFFERING (ICO)

Initial Coin Offering (ICO)

- Digital tokens sold in advance to raise money
 - Ethereum \$18M, \$93B
 - Golem \$8.6M, \$367M
 - Qtum \$15.6, \$2B
 - Gnosis \$12.5, \$177M

Breaking records

- Telegram, over \$1 Billion Raised So Far
- XYO, going through the roof

ICO > VC in 2017

- Initial coin offerings and now surpass early stage VC funding

DECENTRALIZED AUTONOMOUS ORGANIZATIONS





Token

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(sender, receiver, amount);

    /* Initializes contract with initial supply tokens to the creator */
    function token(supply) {
        coinBalanceOf[msg.sender] = supply;
    }

    /* Very simple trade function */
    function sendCoin(receiver, amount) returns(sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

Token

- An entrance ticket
- A certificate of ownership
- A share
- A currency
- Advantages
 - Does not need a server
 - Creator defines terms
 - Control of tokens by contract



Crowdsale

```
contract Crowdsale {

    /* data structure to hold information
       about campaign contributors */
    struct Funder {
    }

    /* at initialization, setup the owner */
    function Crowdsale(beneficiary, fundingGoal, duration, price, token _reward) {
    }

    /* default function that is called whenever anyone sends funds to a contract */
    function () {
        uint amount = msg.value;
        funders[funders.length++] = Funder({addr: msg.sender, amount: amount});
        amountRaised += amount;
        tokenReward.sendCoin(msg.sender, amount / price);
        FundTransfer(msg.sender, amount, true);
    }

    /* checks if the goal or time limit has been reached and ends the campaign */
    function checkGoalReached() afterDeadline {
    }
}
```

Decentralized Autonomous Organization

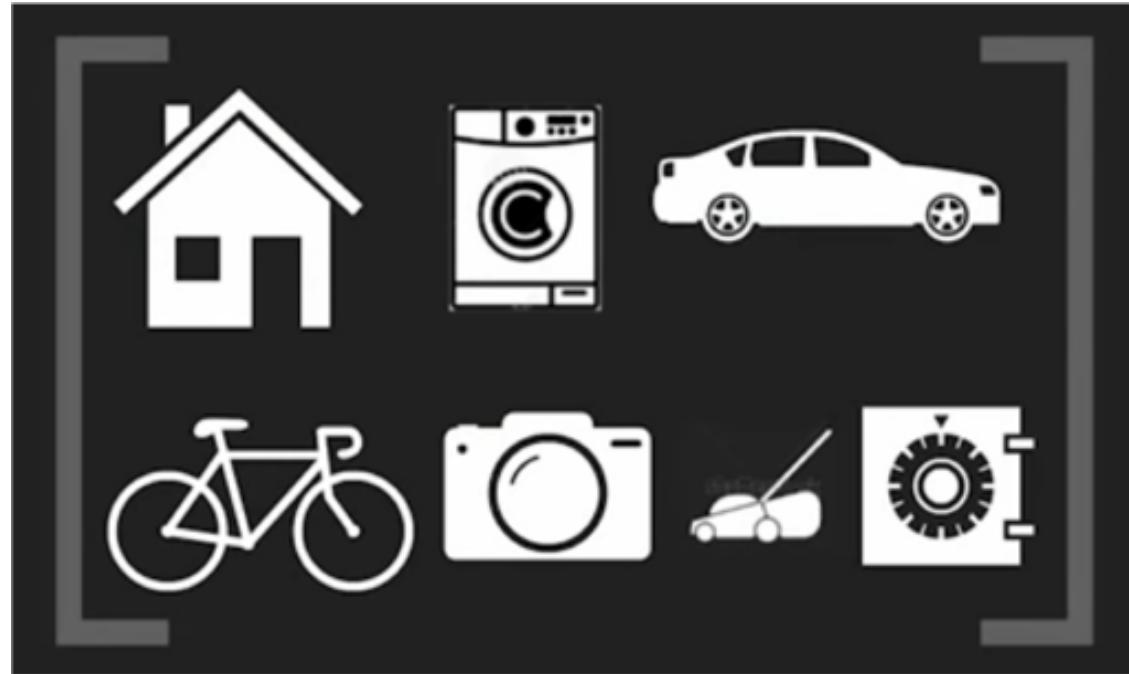


```
contract Democracy {  
  
    public minimumQuorum;  
    public debatingPeriod;  
    public voterShare;  
    public founder;  
    public proposals;  
    public numProposals;  
  
    event ProposalAdded(proposalID, recipient, amount, data, description);  
    event Voted(proposalID, position, voter);  
    event ProposalTallied(proposalID, result, quorum, active);  
  
    function Democracy(voterShareAddress, minimumQuorum, debatingPeriod) {  
    }  
  
    function newProposal(recipient, amount, data, description) returns (proposalID) {  
    }  
  
    function vote(proposalID, position) returns (voteID){  
    }  
  
    function executeProposal(proposalID) returns (result) {  
    }  
}
```

AUTONOMOUS CITIES

Underutilization of resources

- Payment
- Organization
- Matching
- Security
- Etc.

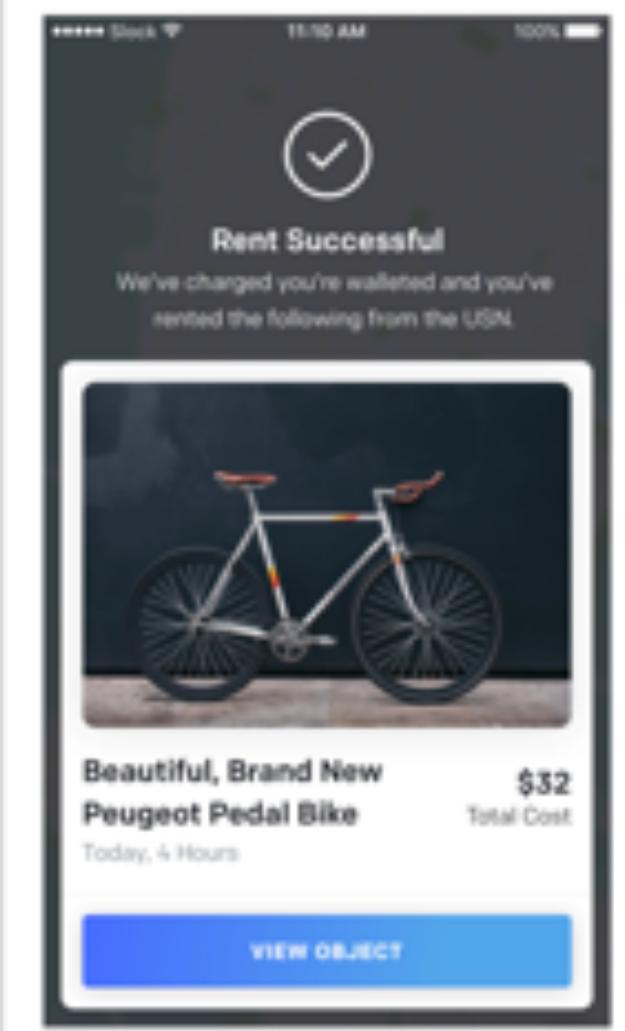
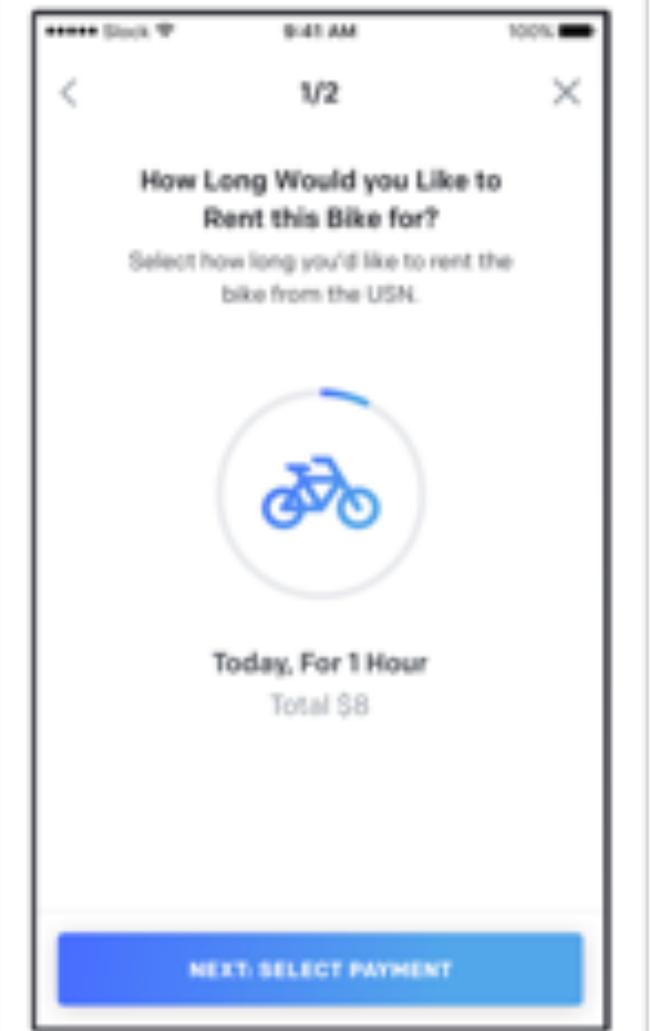
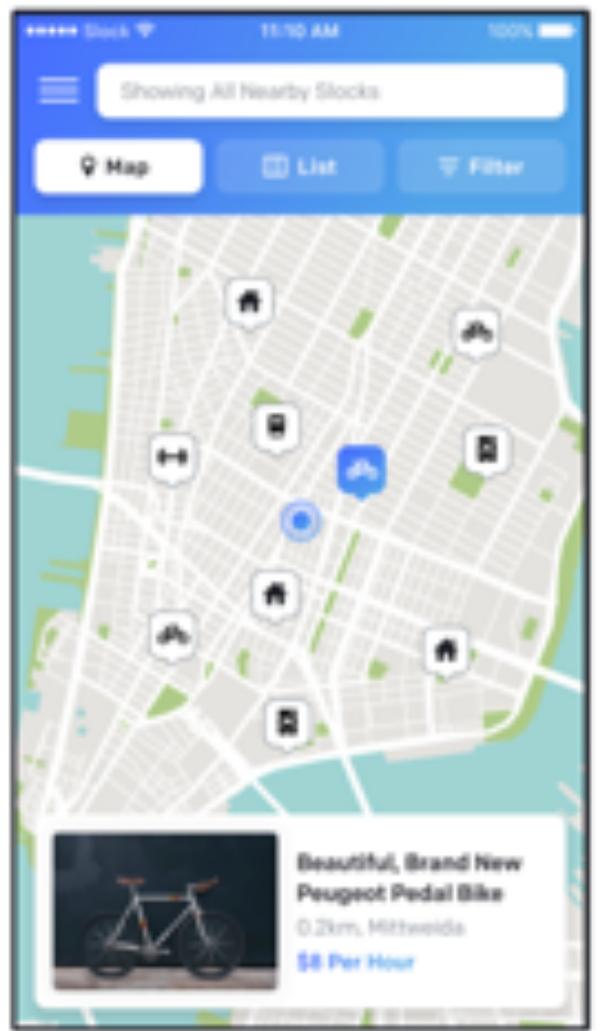


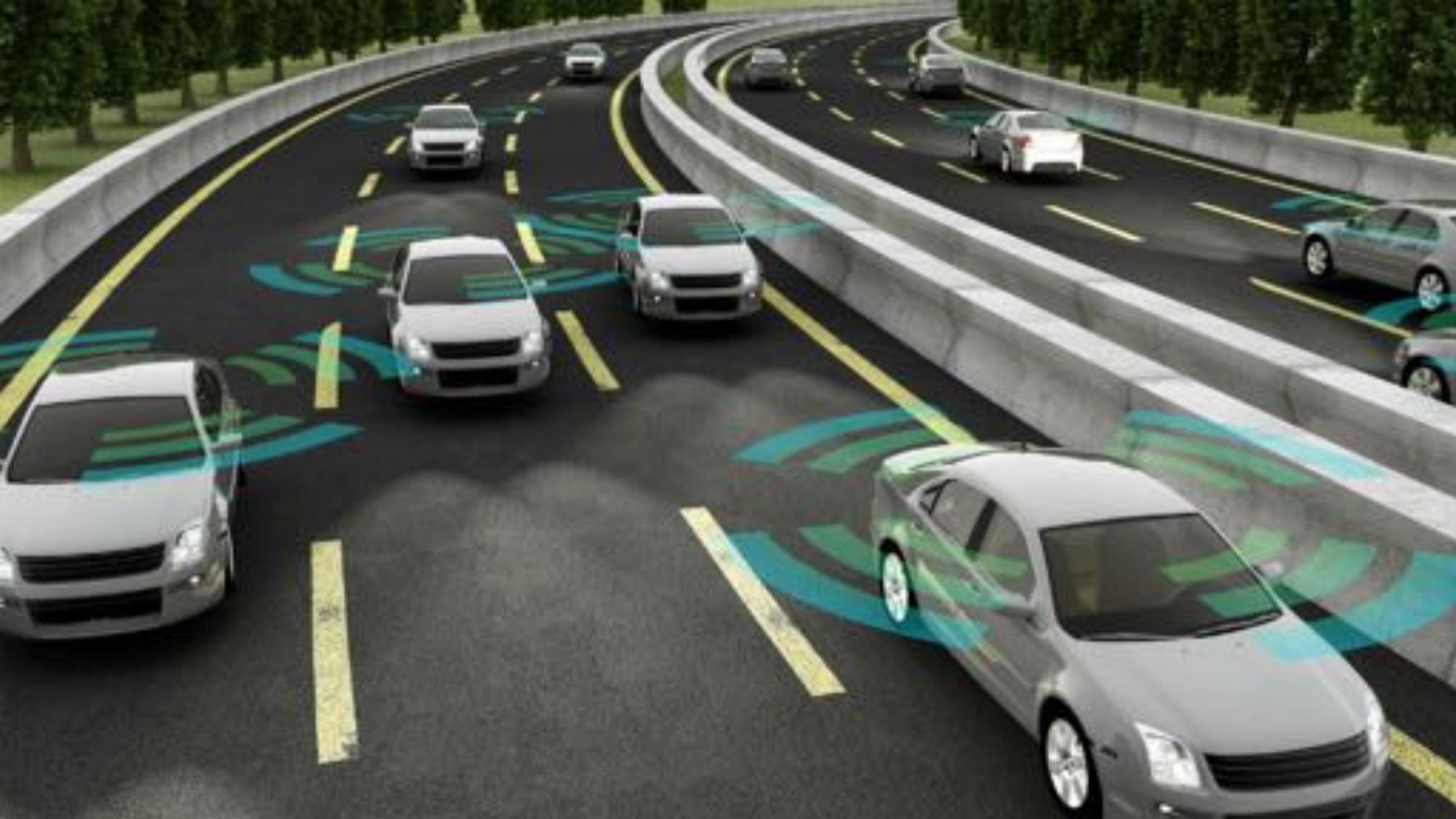
5% Use

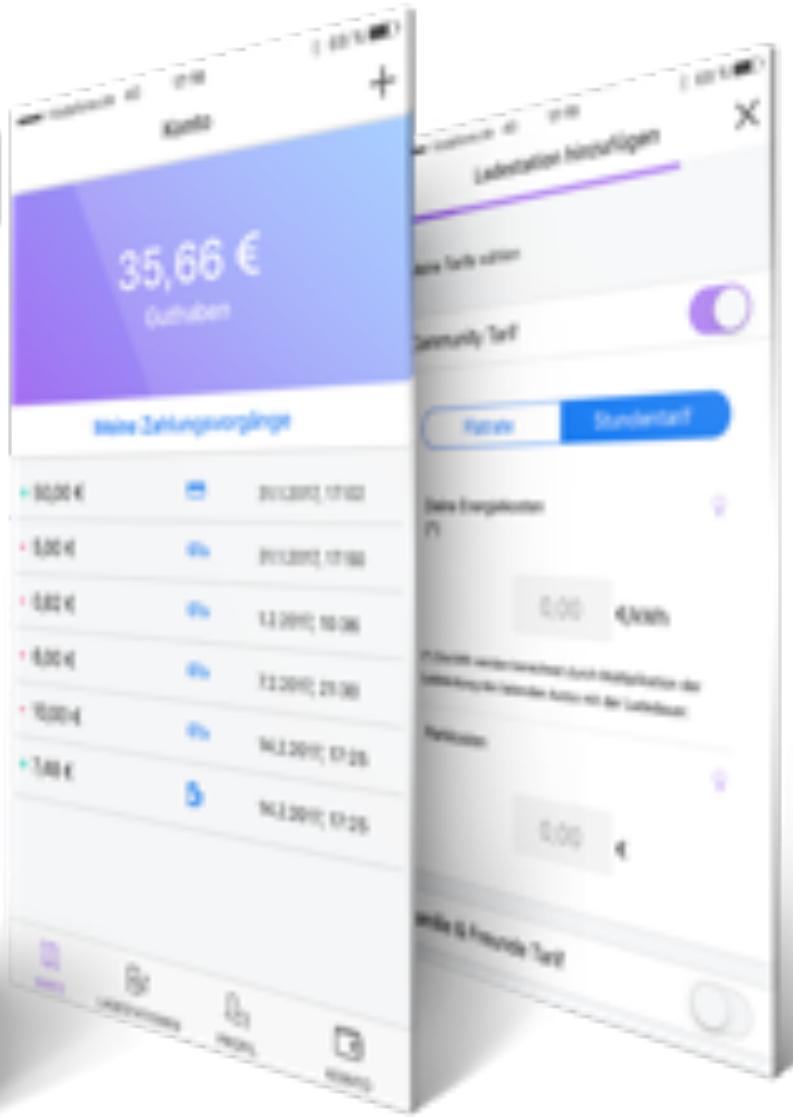
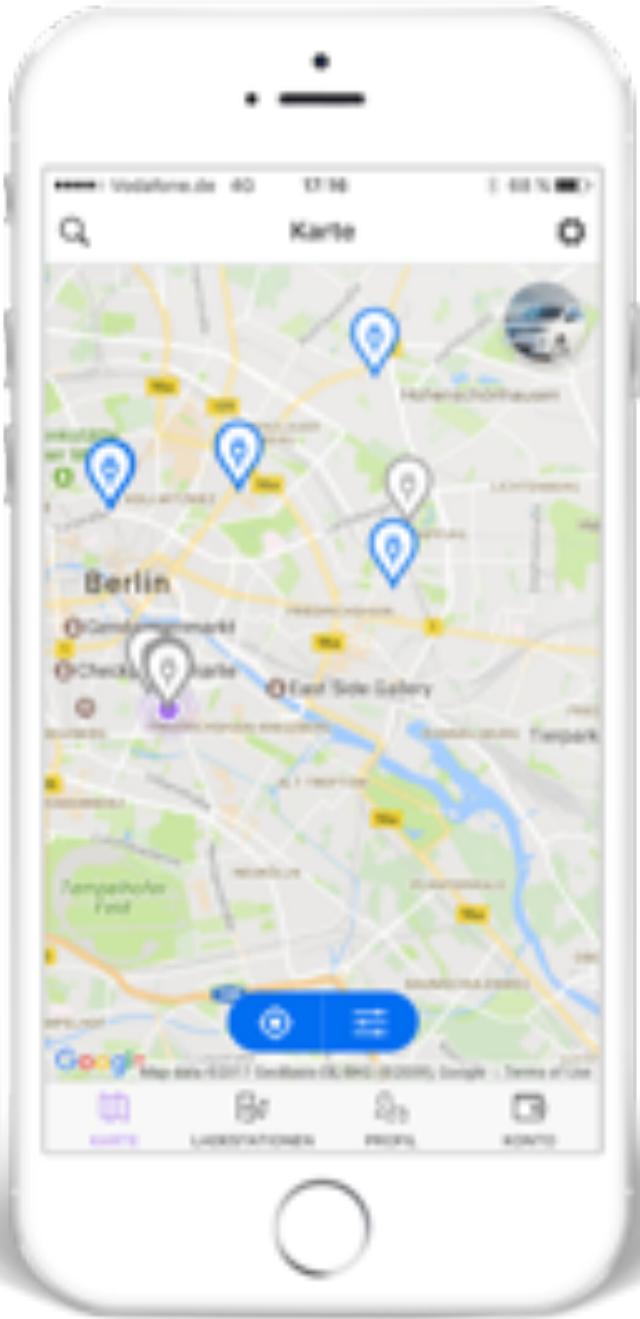
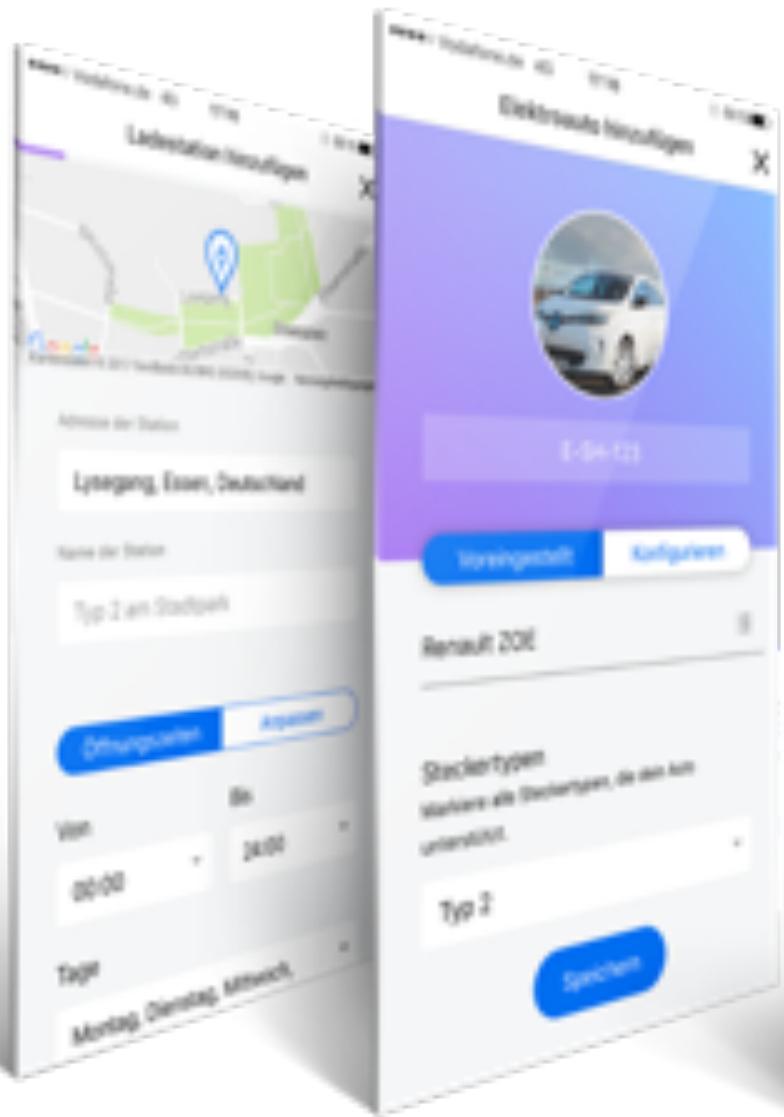
Sharing economy – how?

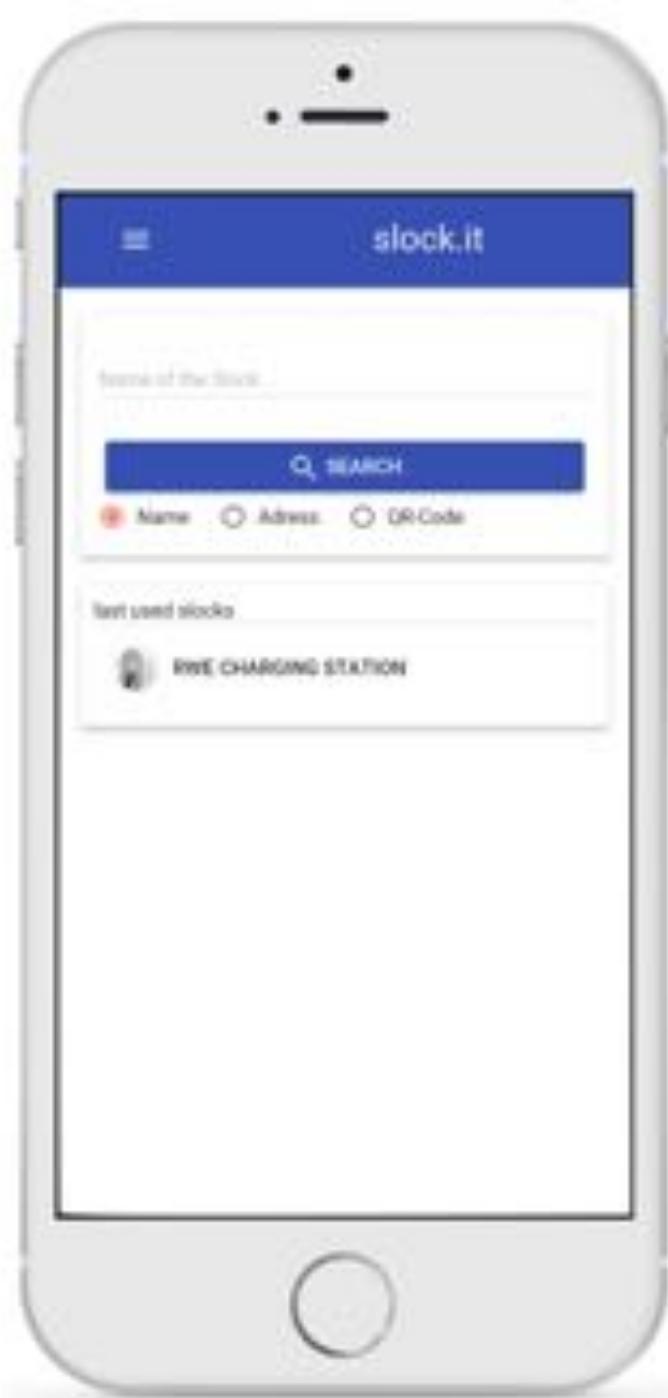
- Payment
- Organization
- Matching
- Security
- Etc.







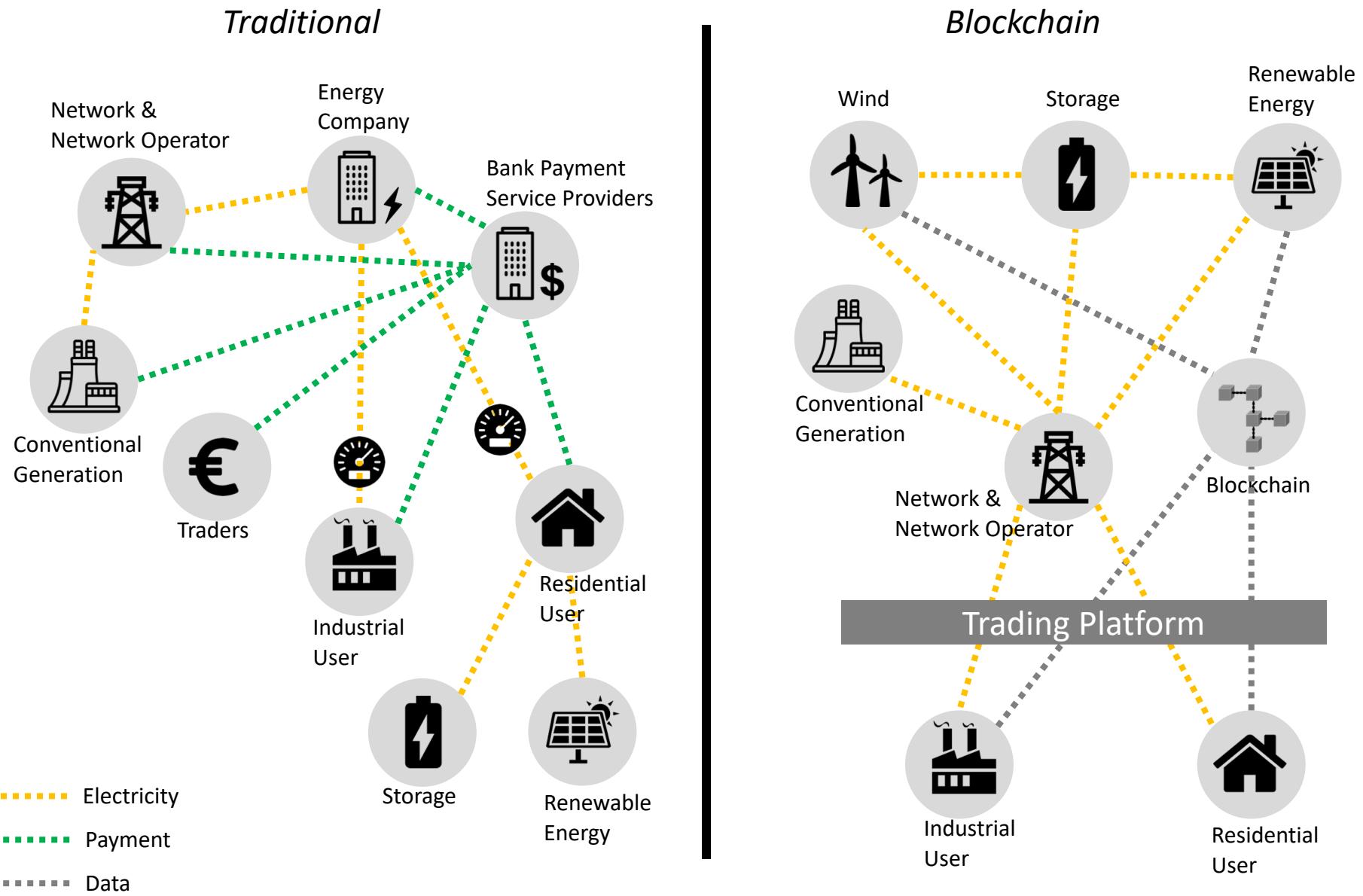




Autonomous vehicles & smart contracts



Decentralized Energy & Supply

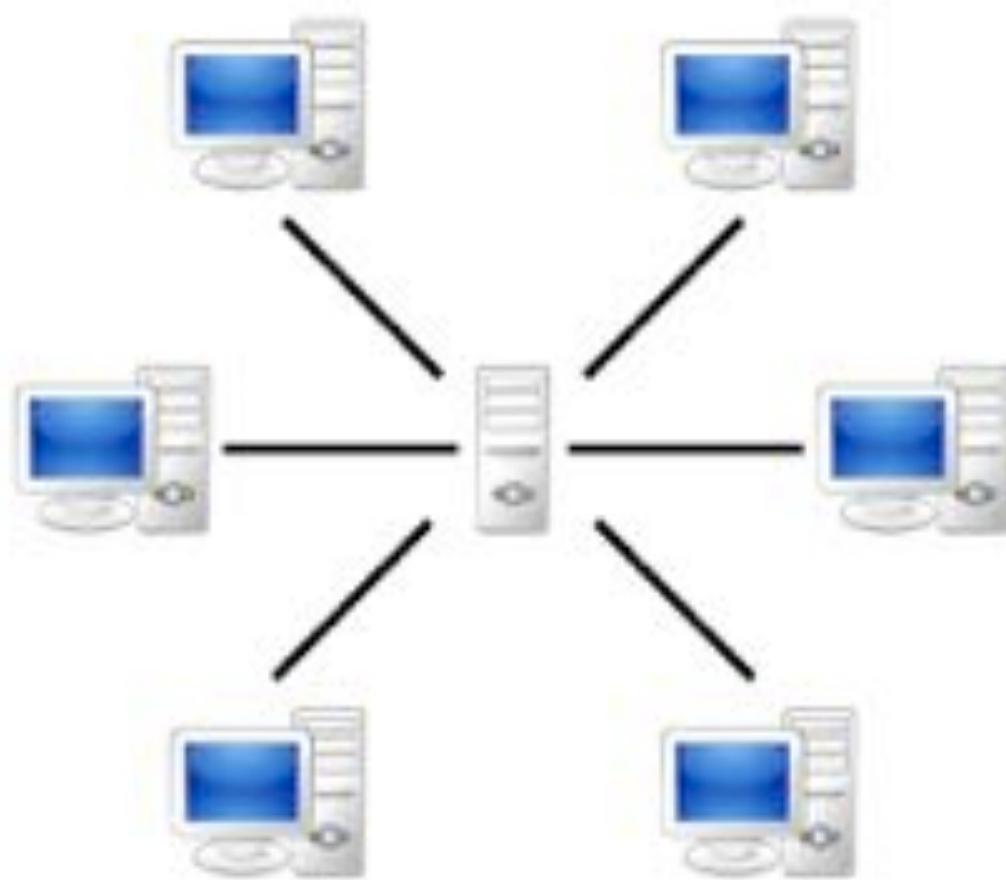




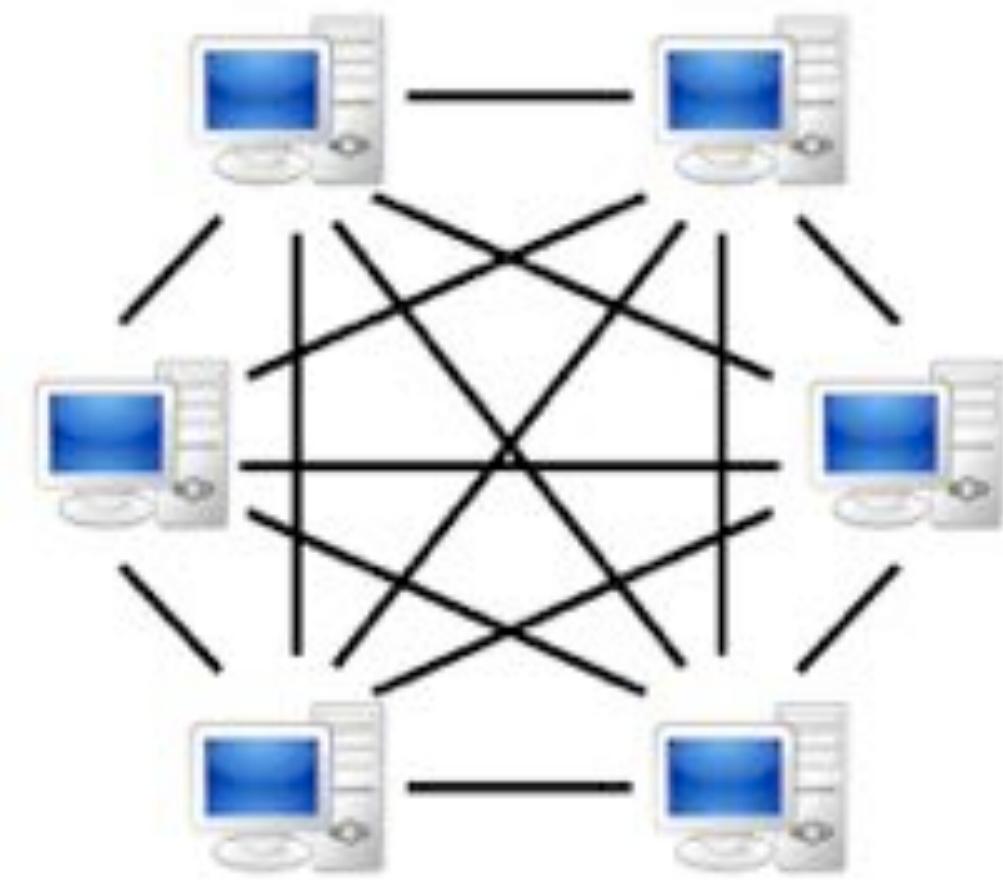


ARCHITECTURE

MIT



Server-based

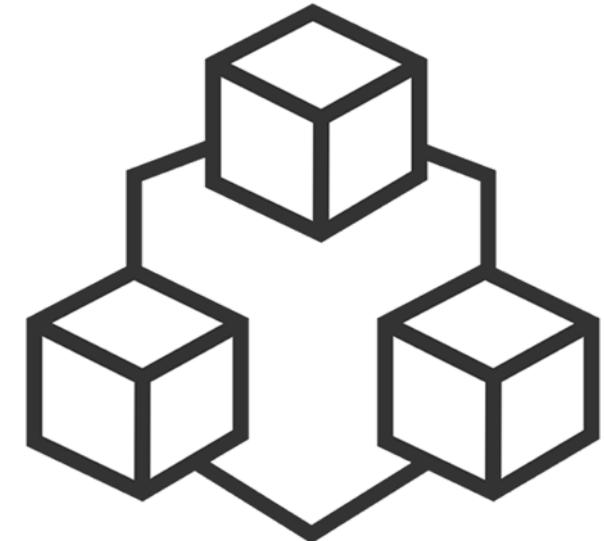
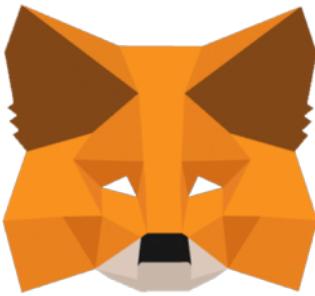


P2P-network

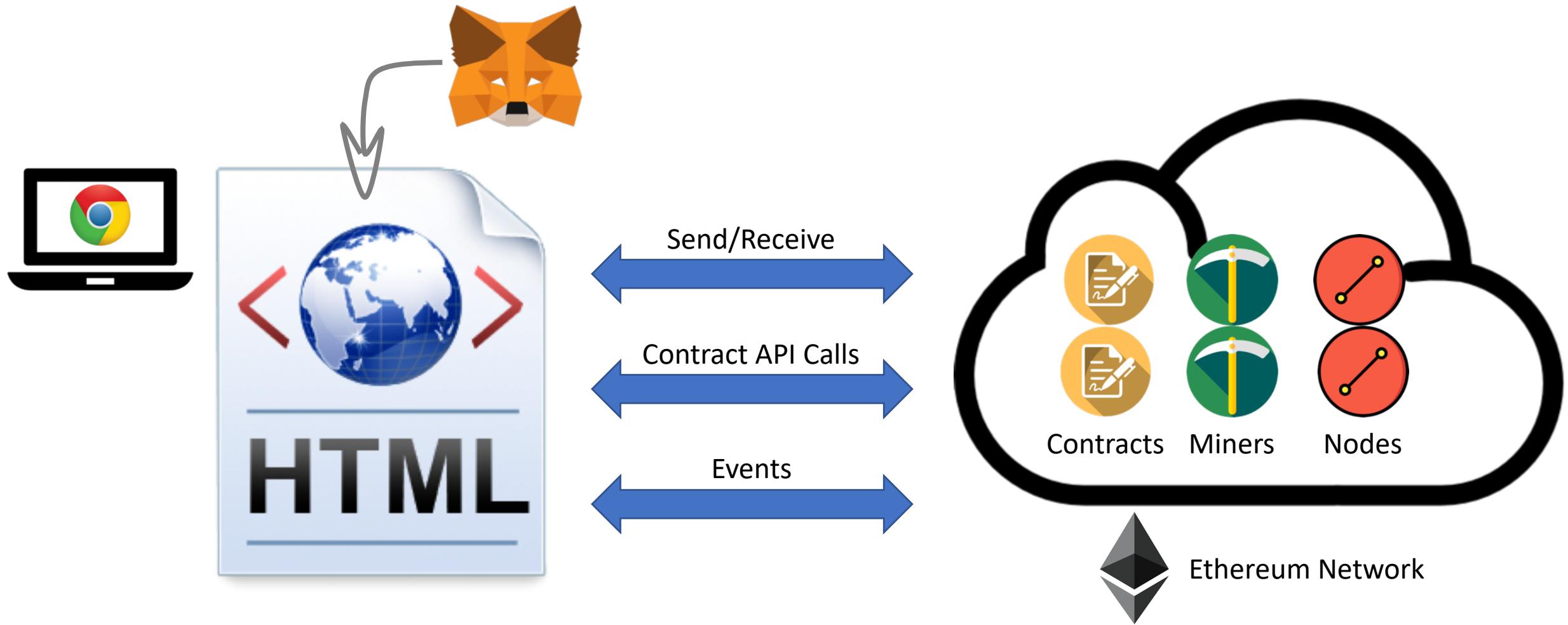


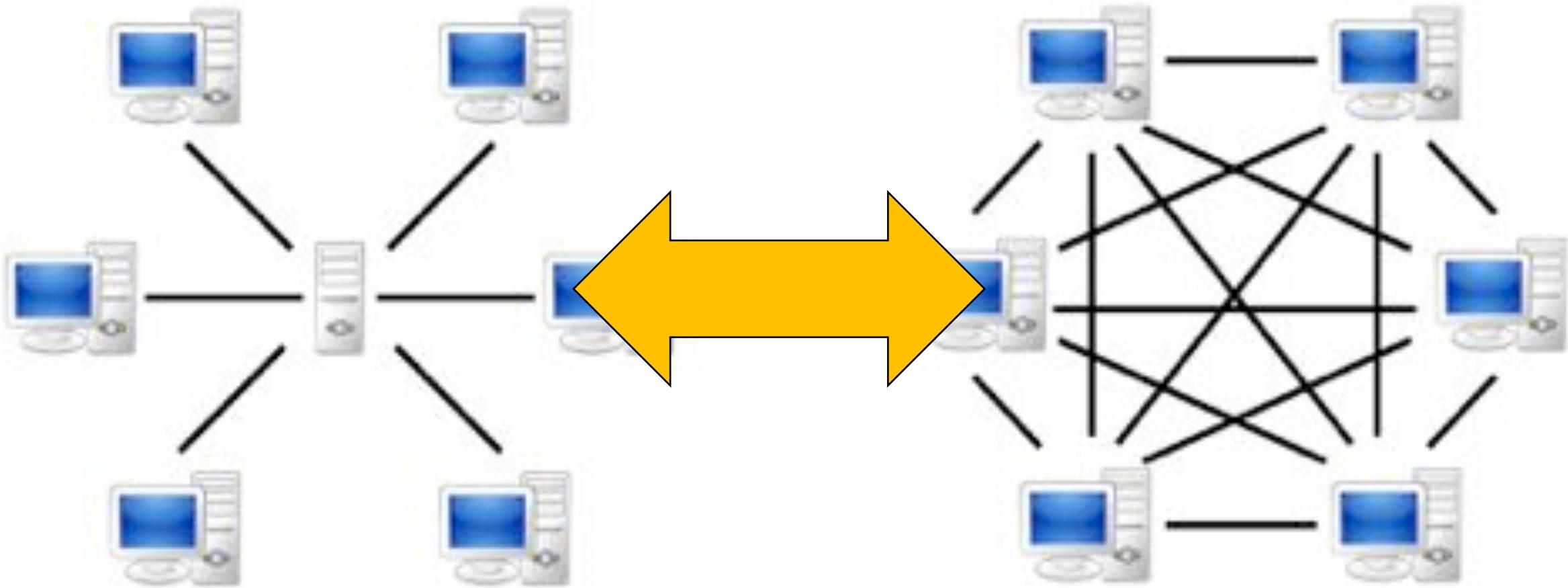


WEB



BLOCKCHAIN





Server-based

P2P-network

CONCLUSION



Buy

Sell

Phone

TV

Car

Microwave

Refrigerator

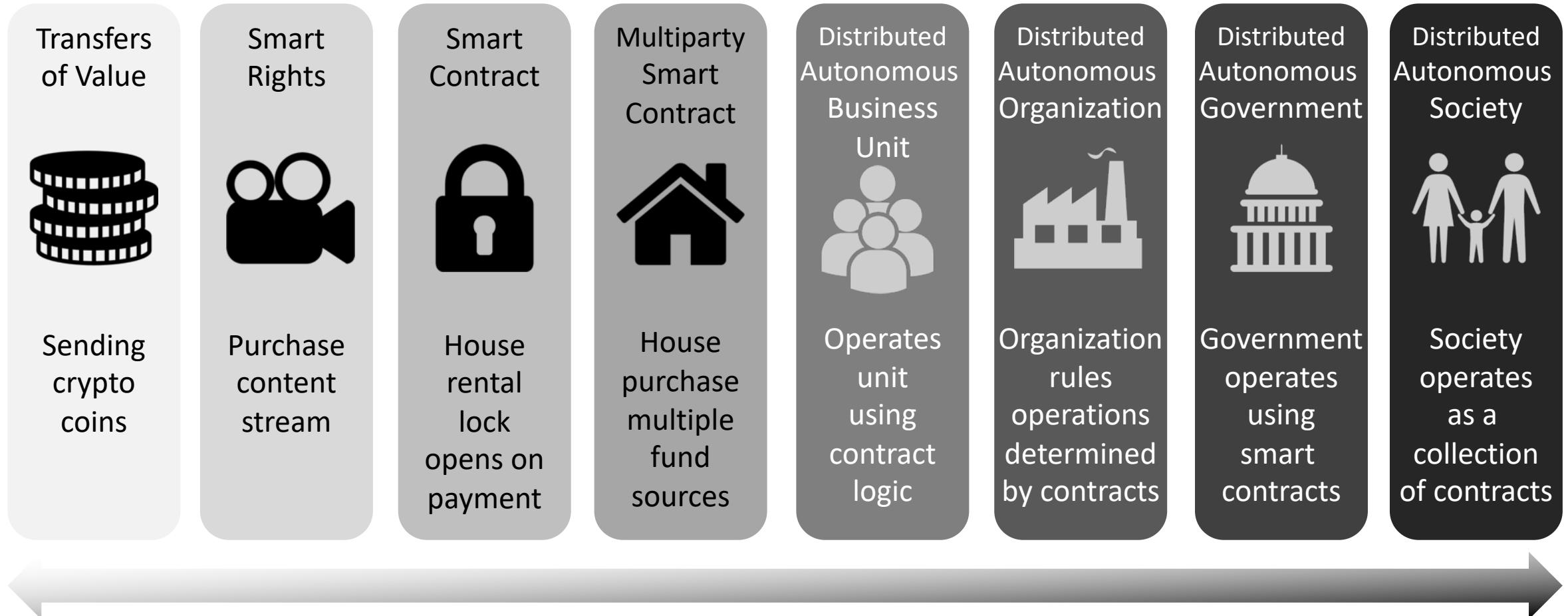
Washing Machine

Library

Blockchain Properties

- Database
- Multiple writers
- Absence of trust
- Disintermediation
- Chain of custody
- Validation
- Identity
- Contracts
- Payment

Smart Contracts



Simple

Complex

Q & A