SECUREWORLD™

Surviving the Siege:
Medieval Lessons in Modern Security

Blockchain + IoT = <3

By: Hudson Jameson | Co-Founder, Oaken Innovations

Let's cut through the hype and explore the use of blockchain technology to secure IoT devices.

Play CyberHunt, the game within the SecureWorld app!
Have fun, network and win great prizes.

Don't forget to take the survey on the SecureWorld App.
It will also be emailed to you at the conclusion of the conference.

After this presentation, view the slides on the SecureWorld App.

Hudson Jameson

Involved in cryptocurrency/blockchain space since 2011.

USAA: 2014-2016

Ethereum Foundation: 2016-current

Oaken Innovations: 2016-current

1 Wife & 3 Cats

Who We Are

Oaken Innovations made up of a team of professionals working to build-out practical solutions within the blockchain space.

Oaken is an IoT blockchain platform for smart cities with hardware and software for automated machine-to-machine transactions over a secure and decentralized network.

Welcome to the intersection of Blockchain and IoT.

John Gerryts

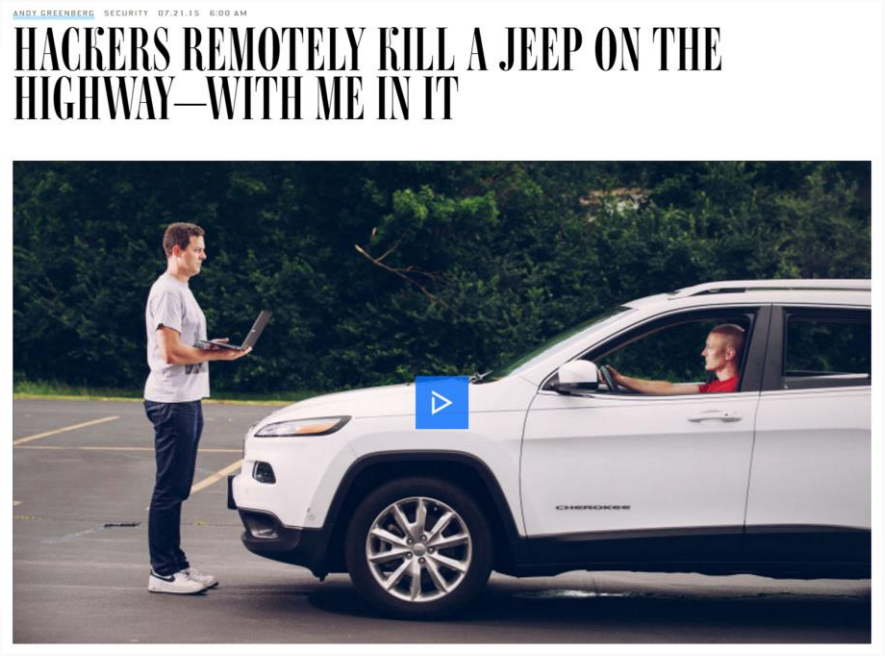
Laney Fisher

Hudson Jameson

Shuang “Lex” Liang

James Johnson

Why IoT Needs Blockchain



BLOCKCHAIN

Identity

Trust

Value

What is a Blockchain?

Definition

Decentralized, **distributed ledger** (database) that keeps a permanent, **tamper-resistant** record of all previous transactions.

3 Components

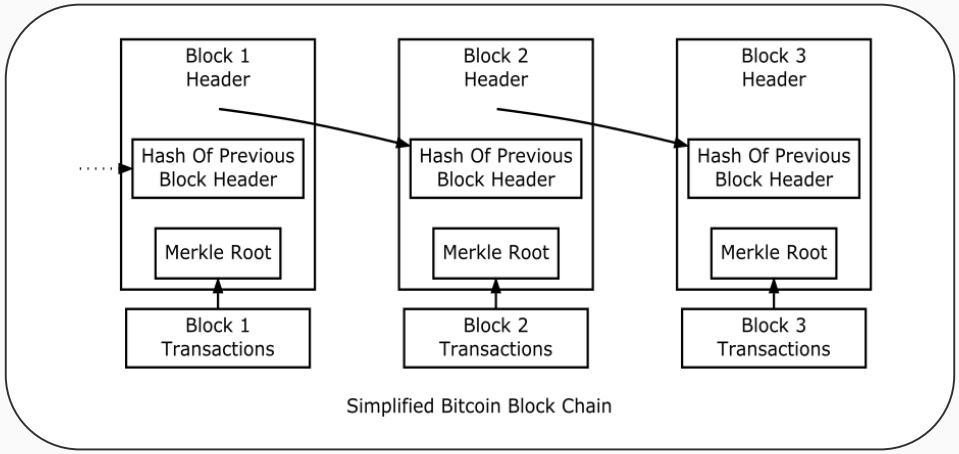
Data Layer

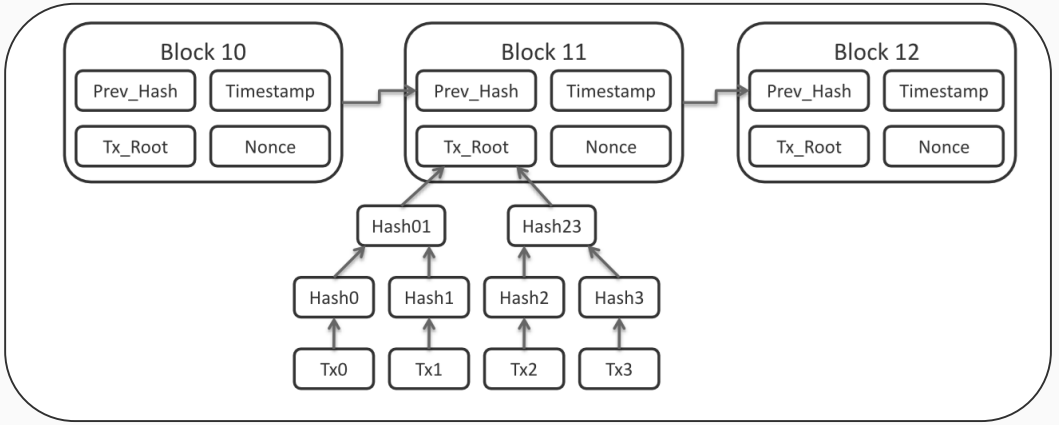
Networking/Gossip Layer

Consensus Layer

Data Layer

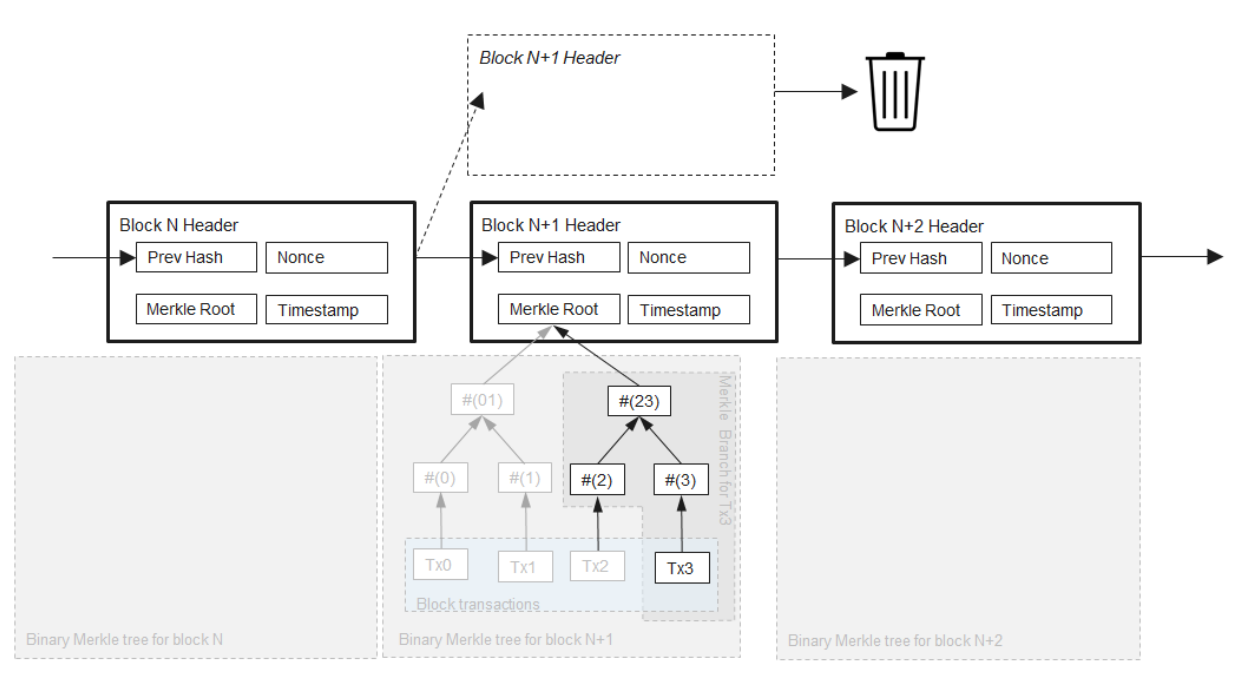
Data is stored in “blocks” where transactions are hashed together to make a transaction root.

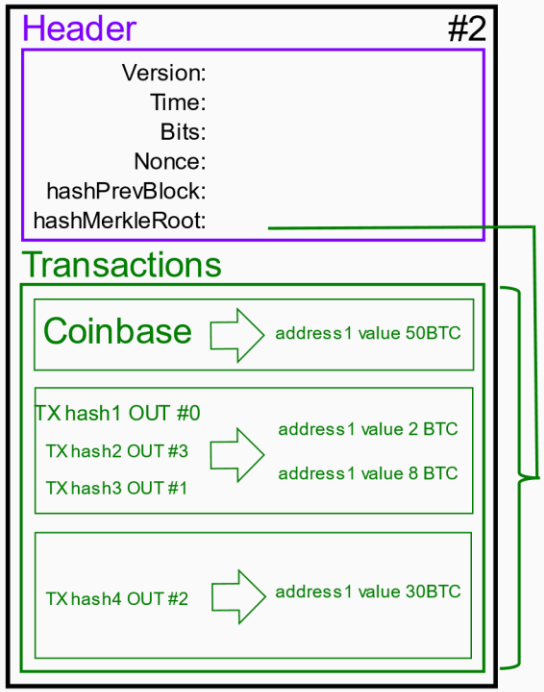




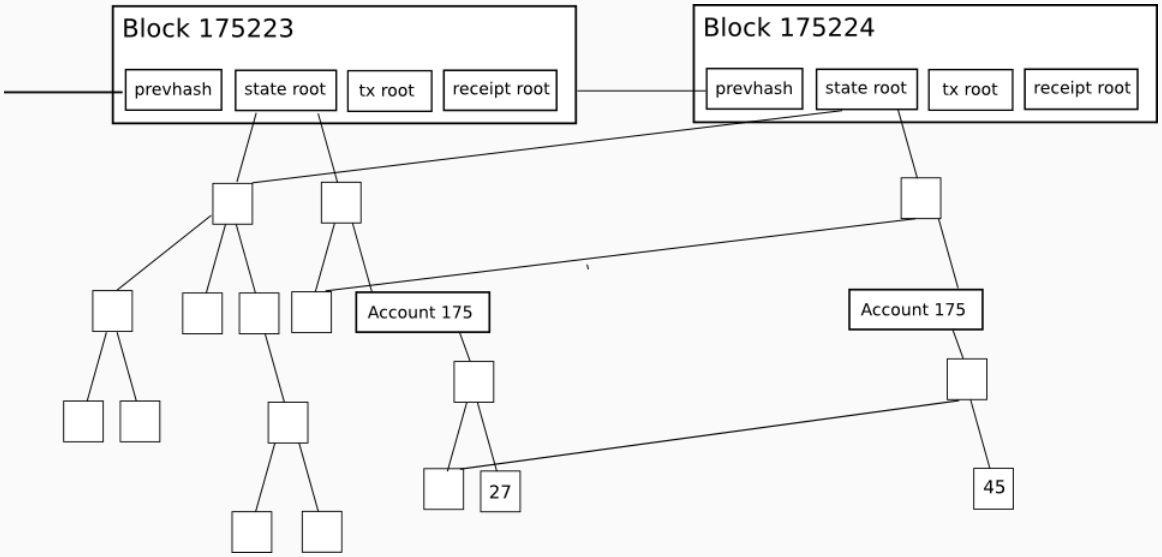
Merkle trees are created from these roots to prove the existence of the transactions in an efficient manner.

Bitcoin: Blocks and Transactions



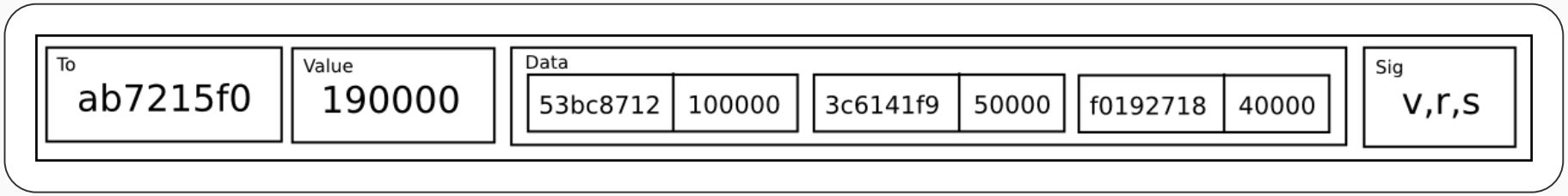


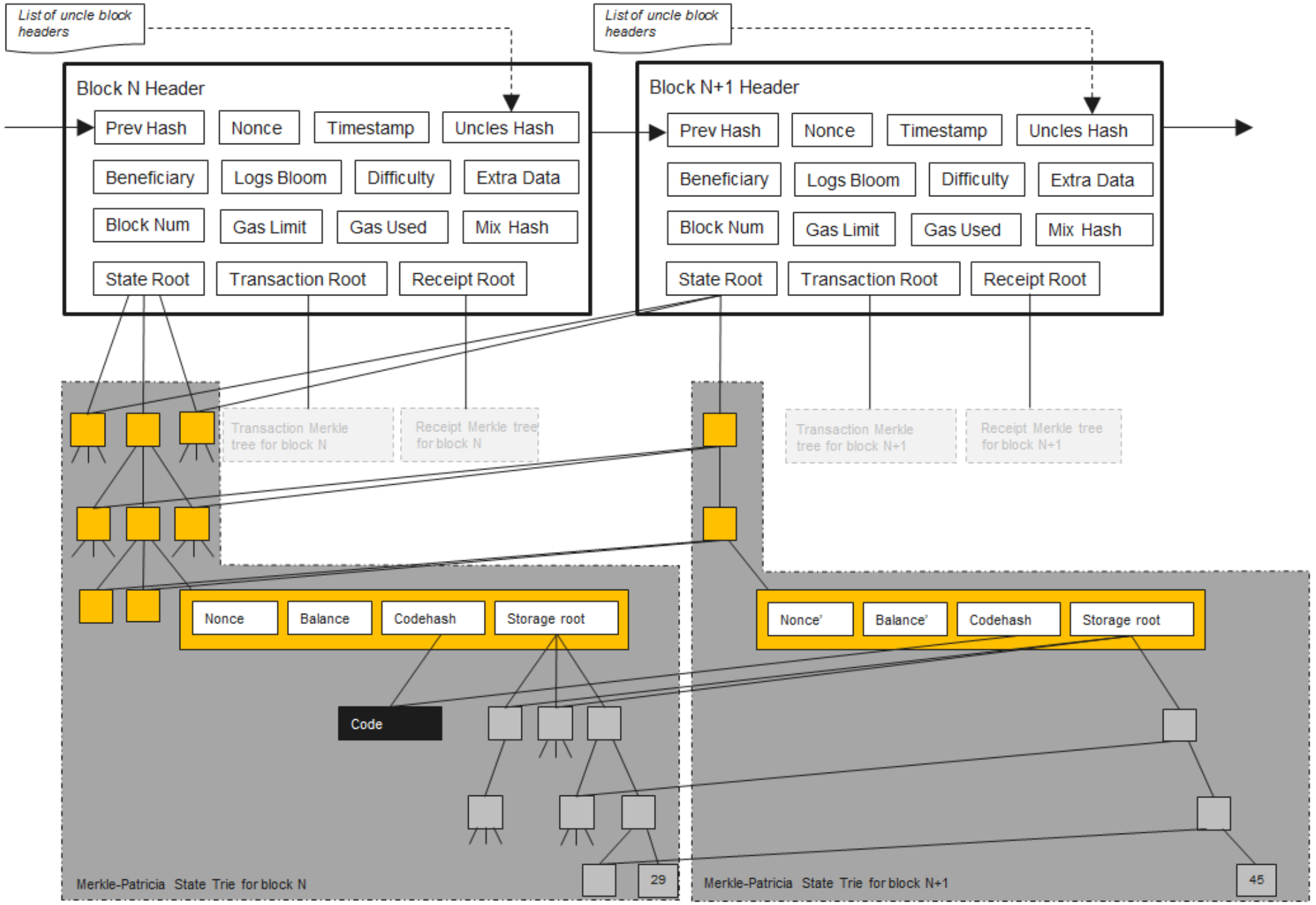
Ethereum: Blocks and Transactions



Ethereum transactions contain:

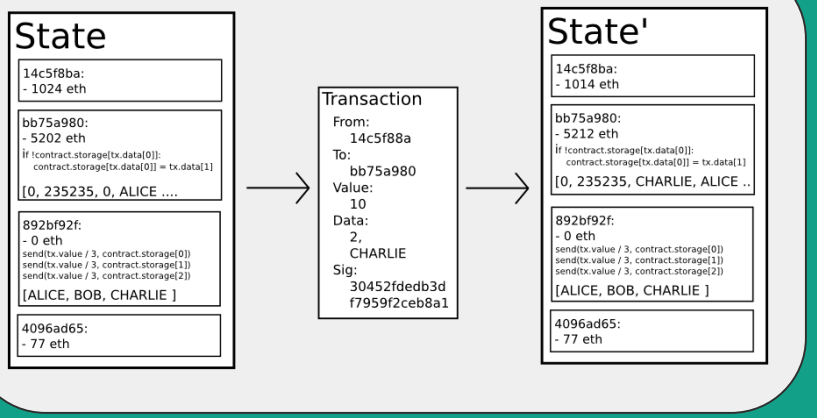
- **nonce** - transaction sequence number for the sending account
- **gasprice** - price you are offering to pay
- **startgas** - maximum amount of gas allowed for the transaction
- **to** - destination address (account or contract address)
- **value** - eth to transfer to the destination, if any
- **data** - all of the interesting stuff goes here
- **v, r, and s values** - along with **r** and **s** makes up the ECDSA signature

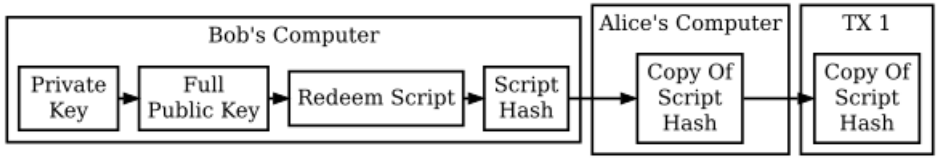



List of uncle block headers
List of uncle block headers
Block N Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Block N+1 Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Transaction Merkle tree for block N
Receipt Merkle tree for block N
Transaction Merkle tree for block N+1
Receipt Merkle tree for block N+1
Nonce
Balance
Codehash
Storage root
Code
Nonce'
Balance'
Codehash
Storage root
Merkle-Patricia State Trie for block N
29
Merkle-Patricia State Trie for block N+1
45

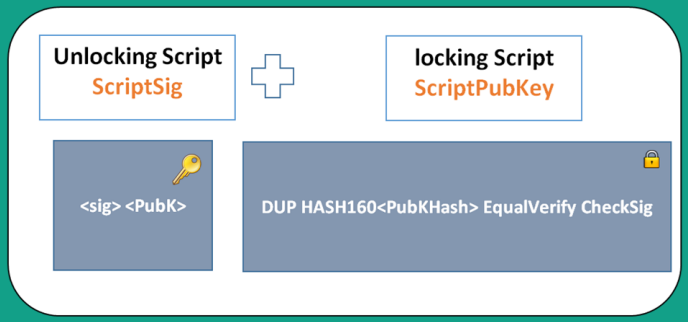
Data Layer: Contracts

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

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

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





Creating A P2SH Redeem Script Hash To Receive Payment

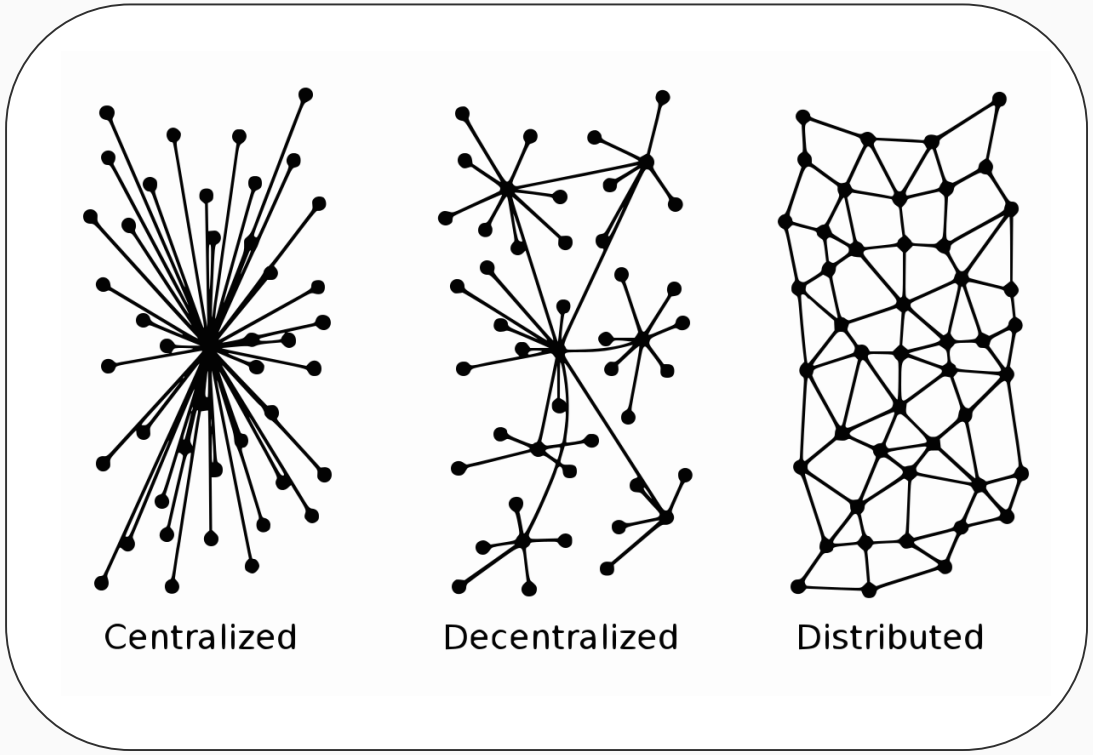


Networking/Gossip Layer

Blockchains are

- Decentralized
- Distributed

If a blockchain does not possess these properties it is either a fully private blockchain or a database that is incorrectly being termed a blockchain.



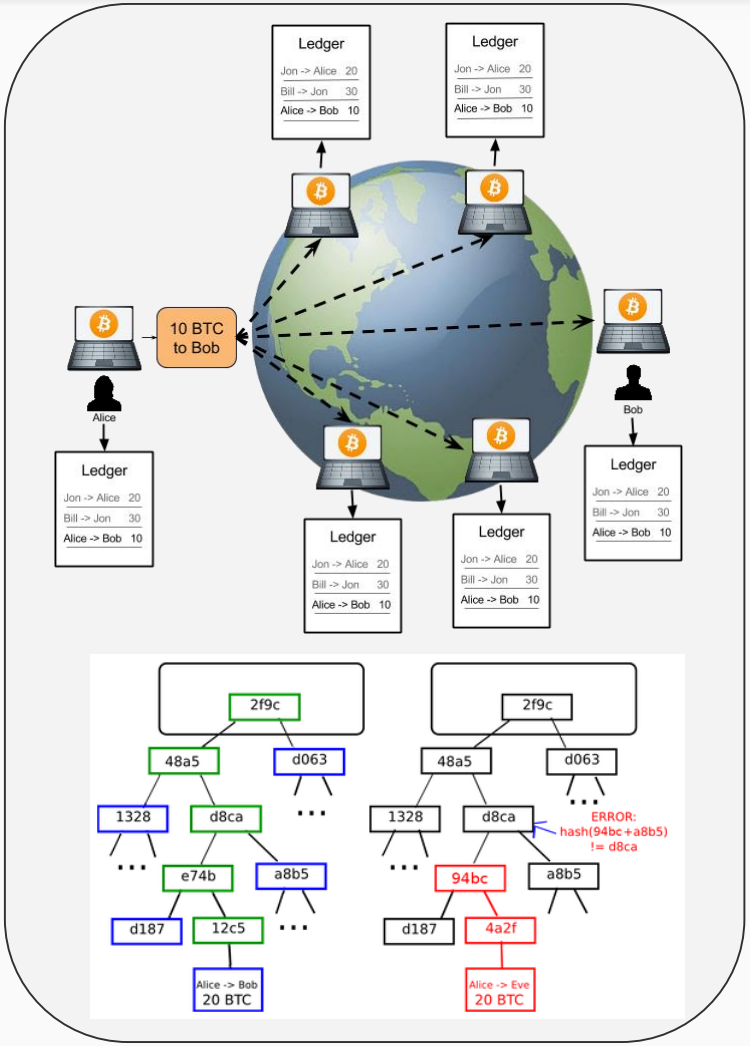
Networking/Gossip Layer

Bitcoin network layer: “Bitcoin network protocol”.

Ethereum network layer: “ĐΞVp2p”.

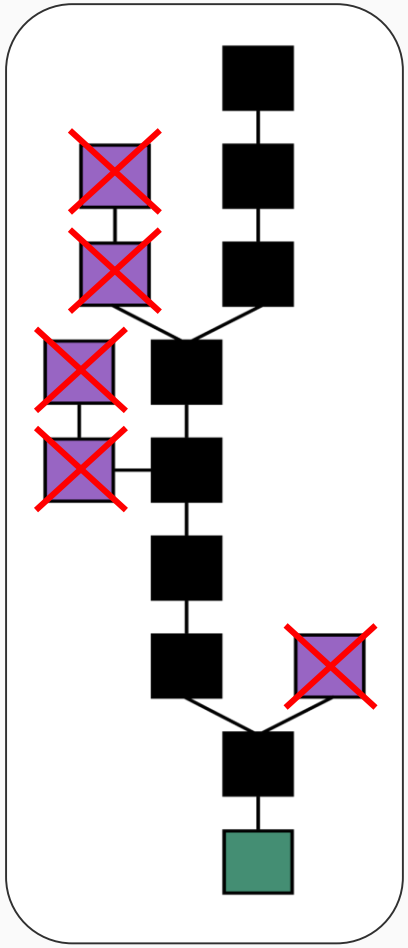
SPV/Light/Thin Clients

- verify only certain information from full nodes, such as block headers.
- Merkle roots make this possible.
- Helps blockchain scalability.



Consensus Layer

- How the nodes in the network come to agreement on which transactions to accept once a transaction is propagated and what the current state of the network is.
- Provides security and immutability to the data in the blockchain.
- Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work.
- Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain. This protects the block chain from tampering.



Consensus Layer: Protocols

Network consensus is achieved through a consensus protocol that the “provers” on the network follow to prove they have contributed to the network. Consensus protocols prevent things that would harm the network, such as duplicate transactions and blockchain forking.

Examples:

- Proof-of-Work: provide a piece of data that is difficult to produce, but easy to verify in order to prove work on the network.
- Proof-of-Stake: block validators take turns validating blocks, putting up a stake that can be taken from them if they try to cheat the network.

Consensus Layer: Proof-of-Work/Stake

Proof-of-Work 

- "Prover" proves they performed a certain amount of work to generate a block.
- Prover gets block reward and transaction fees if they are selected.
- Selection based on combination of how much computing power you contribute and randomness.
- Used in Bitcoin, Ethereum (for now), Litecoin, Dogecoin

Proof-of-Stake 

- "Prover" shows they own a certain amount of money.
- Prover gets block reward and transaction fees if they are selected.
- Selection based on combination of how much stake you have put up and randomness.
- Used in Peercoin, Nxt, Blackcoin, Ethereum (future).

3 Types of Blockchains

- **Public Blockchains** - no central authority, everyone can read/write transactions.
- **Consortium Blockchains** - no central authority, selected participants can write/verify transactions. Read access may be permissioned or public. This type is also called Hybrid Blockchains.
- **Private Blockchains** - write permissions for transactions centralized to one organization. Read permissions may be granted to outside organizations.

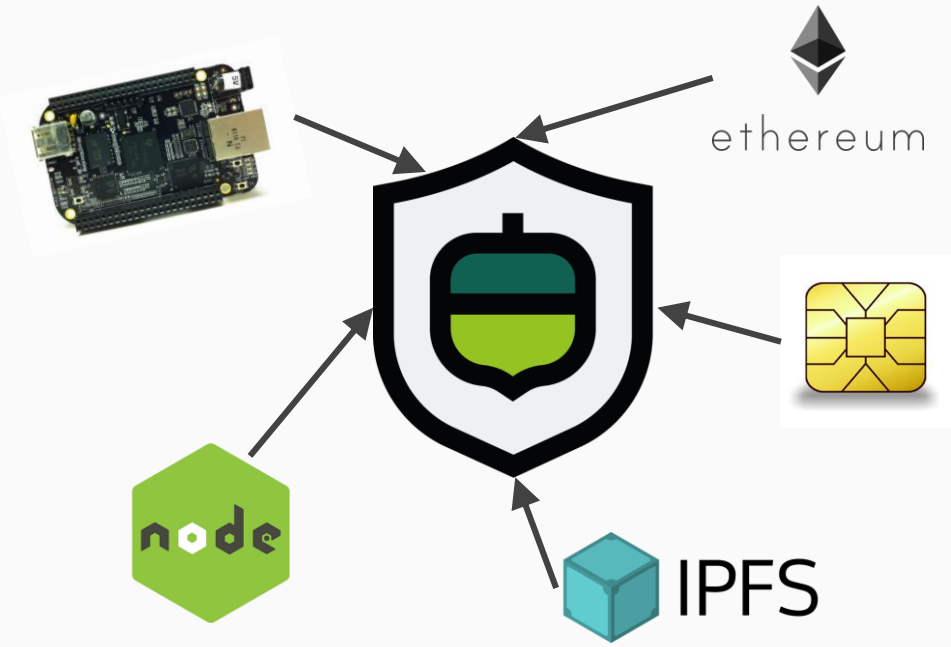
Want more information? Read the blog post "On Public and Private Blockchains" by Vitalik Buterin on the Ethereum blog.

Type	Permissioned?	Decentralized?	Trustless?
Public	No	Yes	Yes
Consortium	Yes	Partially	No
Private	Yes	No	No

The Oaken Platform

The Oaken platform is made of A.C.O.R.N.S (Autonomous Communication Over Redundant Nodes).

ACORNS provide a layer of security to both the hardware and software components of an IoT network.



MQTT-Trusted - trusted messaging framework based on MQTT and crypto signatures.

Sign Message or Verify Message

Message

```
Message from 1/5/17 1:33 PM UTC: Unlock Car
```

Include your nickname and where you use the nickname so someone else cannot use it. Include a specific reason for the message so it cannot be reused for a different purpose.

Sign Message

Signature


```
{
  "address": "0x1bdae8d8c66badc1d02fe9f58e1586fb00d21b87",
  "msg": "Message from 1/5/17 1:33 PM UTC: Unlock Car",
  "sig": "0x07b81d14341624c3b13281ca20845579b35a4d6911bbf0aaaa492486b988e8e908dfc45ab8bf622f2bbd2616a37af76988f58e14001d6a9734088058ffcc2b651c",
  "version": "2"
}
```

Sign Message or Verify Message

Signature

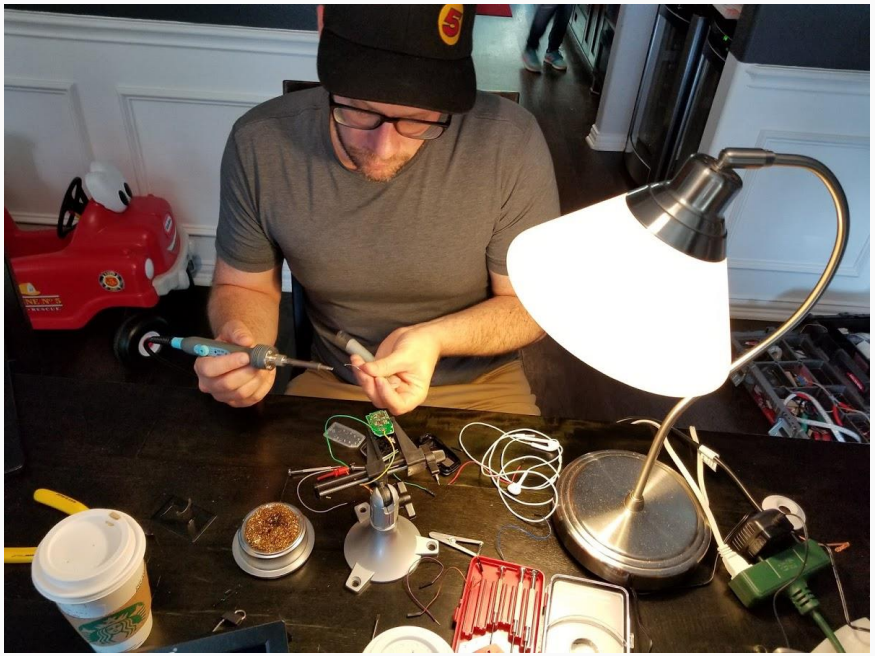

```
{
  "address": "0x1bdae8d8c66badc1d02fe9f58e1586fb00d21b87",
  "msg": "Message from 1/5/17 1:33 PM UTC: Unlock Car",
  "sig":
"0x07b81d14341624c3b13281ca20845579b35a4d6911bbf0aaaa492486b988e8e908dfc45ab8bf622f2bbd2616a37af76988f58e14001
d6a9734088058ffcc2b651c",
  "version": "2"
}
```

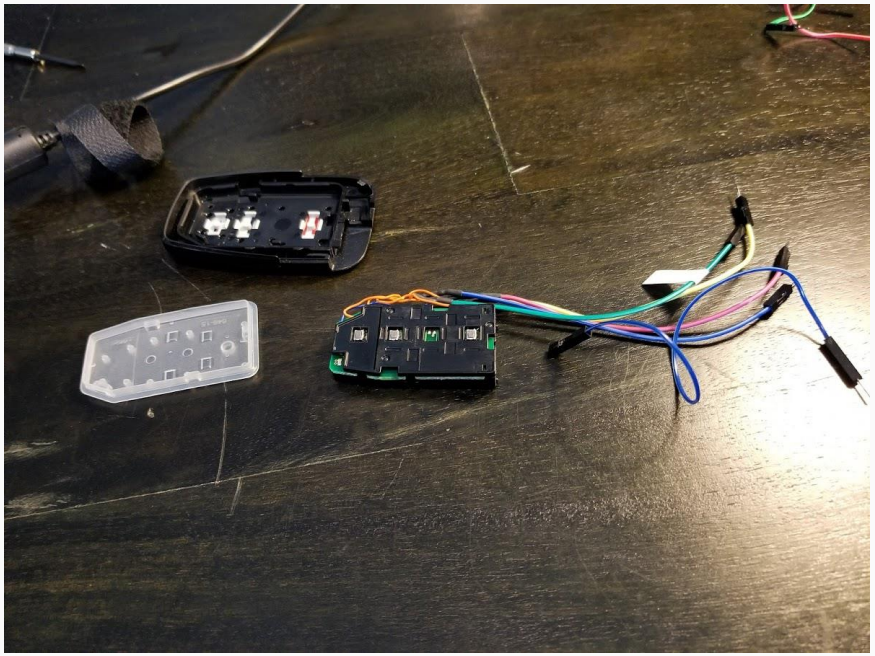

Verify Message

0x1bdae8d8c66badc1d02fe9f58e1586fb00d21b87 did sign the message Message from 1/5/17 1:33 PM UTC: Unlock Car.

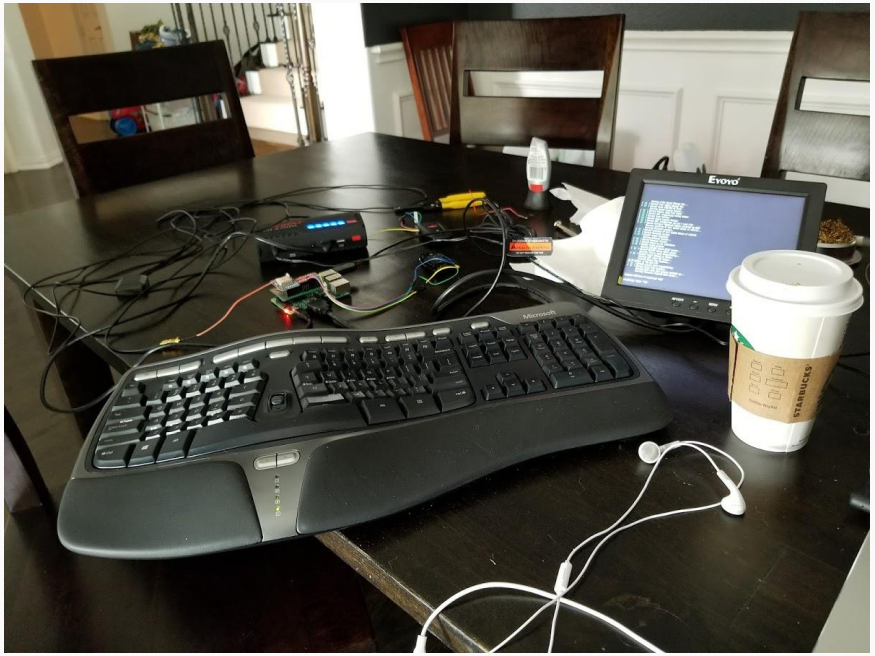
MyEtherWallet

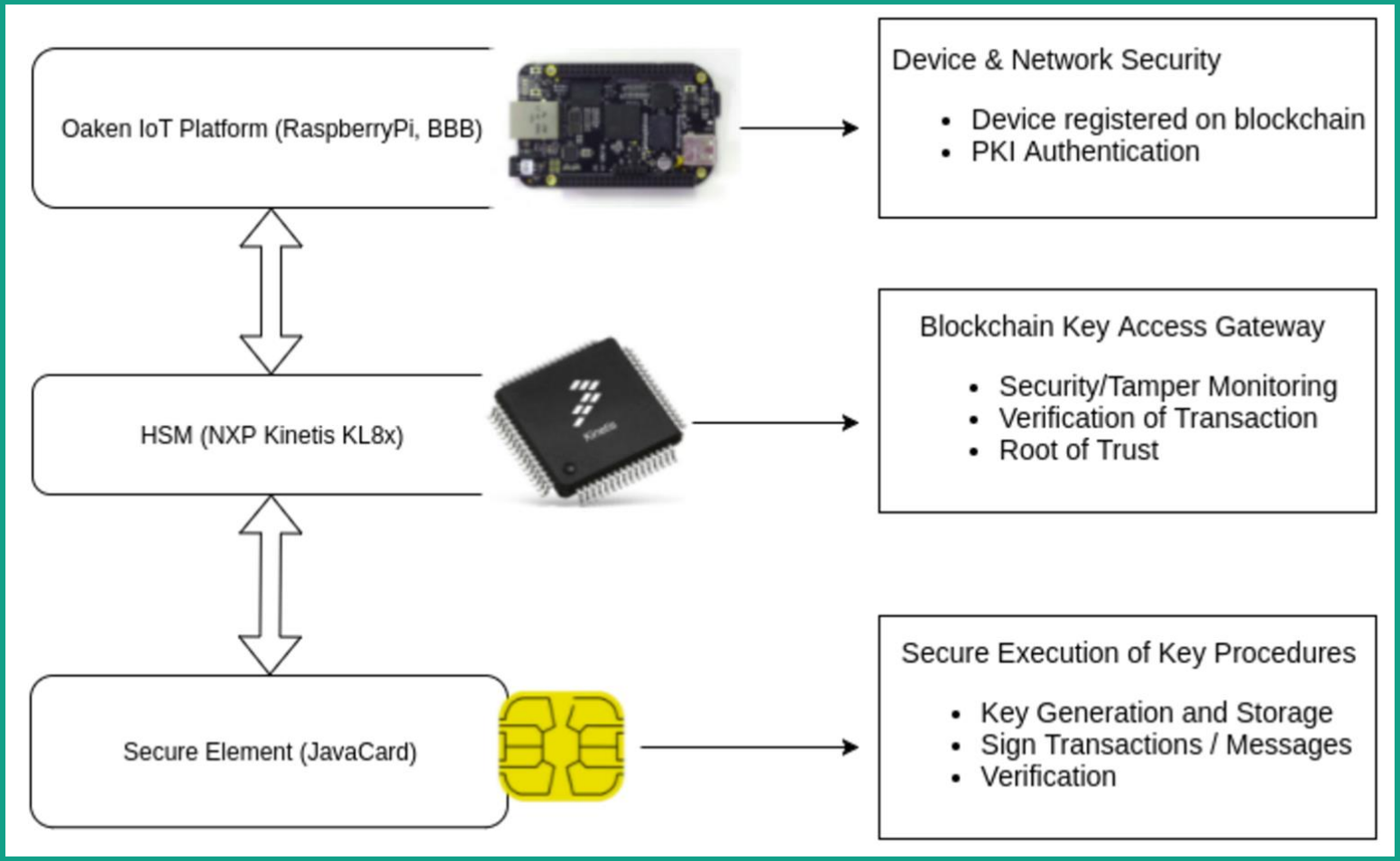
Building an ACORN





Building an ACORN



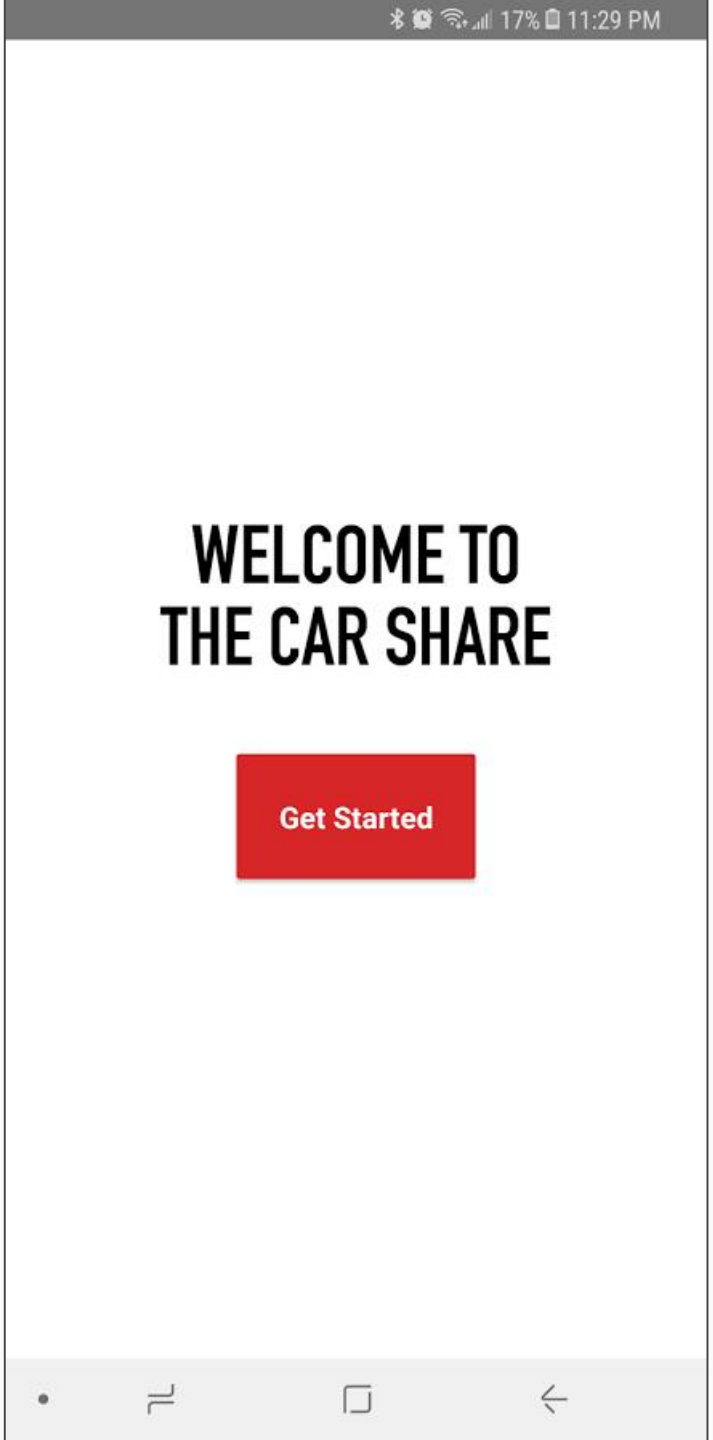

Oaken IoT Platform (RaspberryPi, BBB)
HSM (NXP Kinetis KL8x)
Secure Element (JavaCard)
Device & Network Security
Device registered on blockchain
PKI Authentication
Blockchain Key Access Gateway
Security/Tamper Monitoring
Verification of Transaction
Root of Trust
Secure Execution of Key Procedures
Key Generation and Storage
Sign Transactions / Messages
Verification

Car Share Demo

- Demonstrate disintermediation of Hertz.
- Built in collaboration with Toyota.
- Back-end using almost entirely decentralized tech.
- Debuted at Consensus 2017.

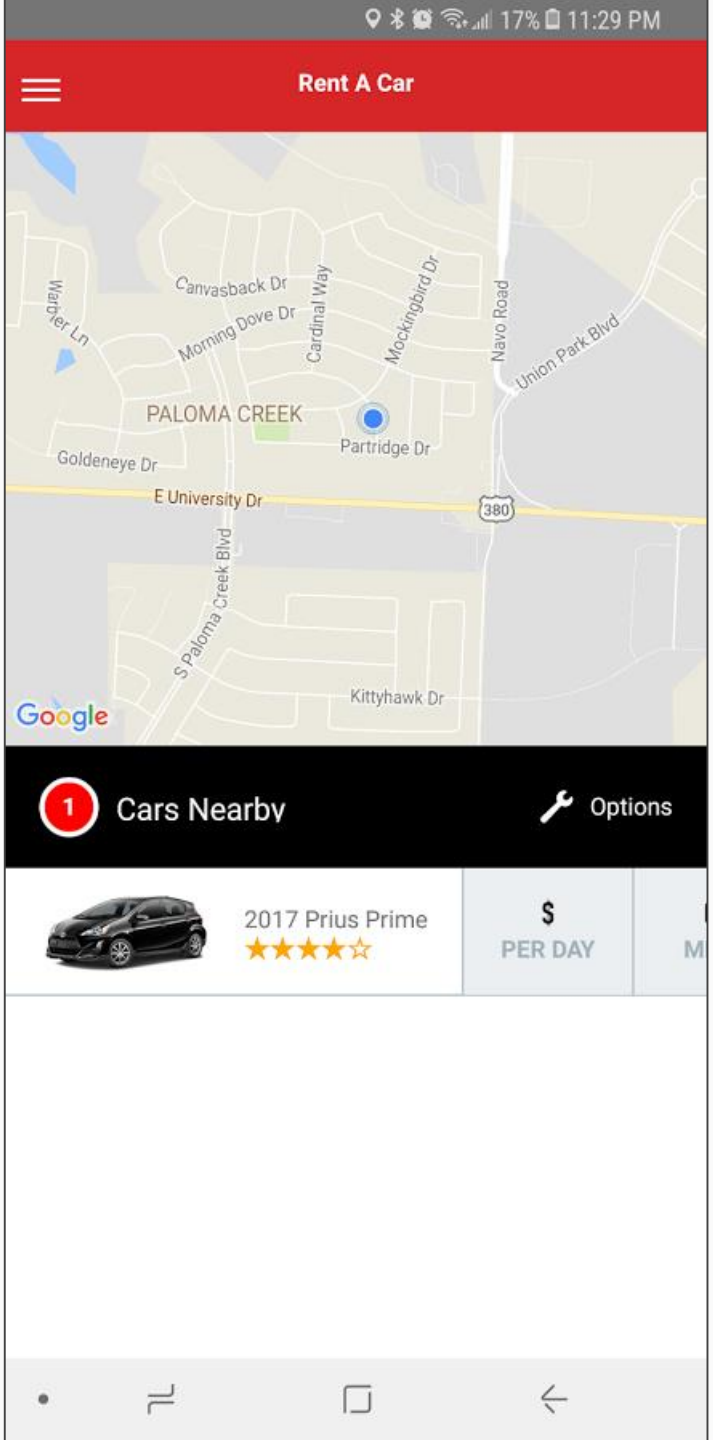
Built Using:

React Native ethereum IPFS MQTT JS INFURA solidity



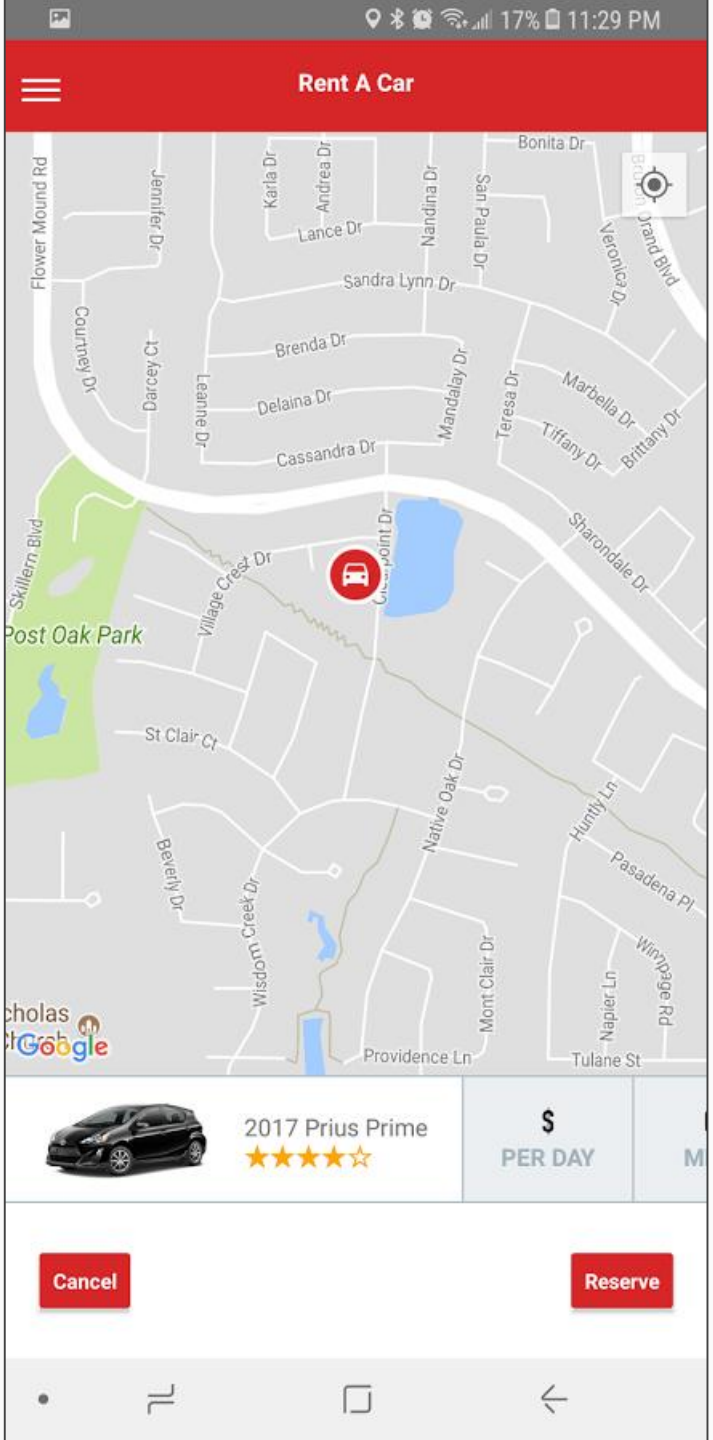
Car Share Demo

- Log in using Ethereum account.
- Public key cryptography
  - Built in identity
  - Client side
  - Self-sovereign
- Hardware
  - Raspberry Pi
  - HSM w/ custom firmware
  - Hacked Toyota Prius key fob
  - GPS antenna



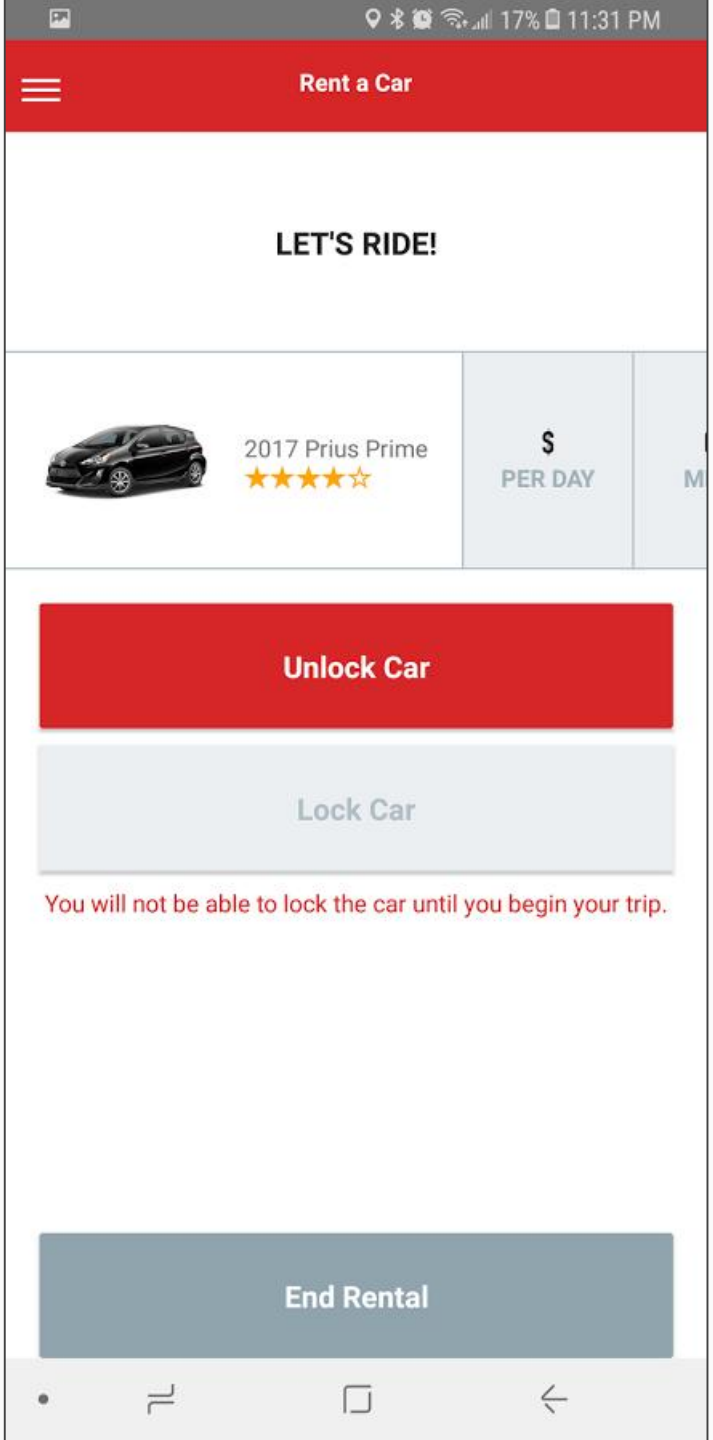
Car Share Demo

- Frontend
  - React Native
  - Custom built IPFS React Native module
  - Displays data stored in nested JSON files
  - Google Maps
- Networks
  - Ethereum connection using Infura
  - Testing using Metamask and Ropsten/Rinkeby testnets
  - MQTTT broker (could be replaced with IPFS pub/sub)



Car Share Demo

- Backend
  - Ethereum
    - Authentication
    - Payment
  - IPFS
    - Ephemeral data store
  - MQTTT
    - Pub-sub platform
    - Modified MQTT for Ethereum key signing
    - Secure car locking/unlocking



Car Share Demo

- Security
  - Software
    - Smart contract on a blockchain allows only specific addresses to unlock the car.
    - No way to spoof it
- Hardware
  - Tamper resistant HSM
- Uses
  - Car owners to monetize excess capacity
  - Common data platform framework market
  - Car history

Contact

Hudson Jameson

Twitter: @hudsonjameson
Website: hudsonjameson.com

Oaken Innovations

Twitter: @projectoaken
Website: oakeninnovations.com