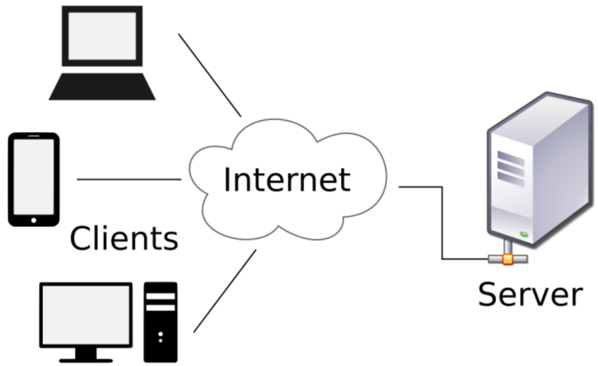
DEPARTAMENTO
DE INFORMÁTICA
PUC·RIO

PUC
RIO

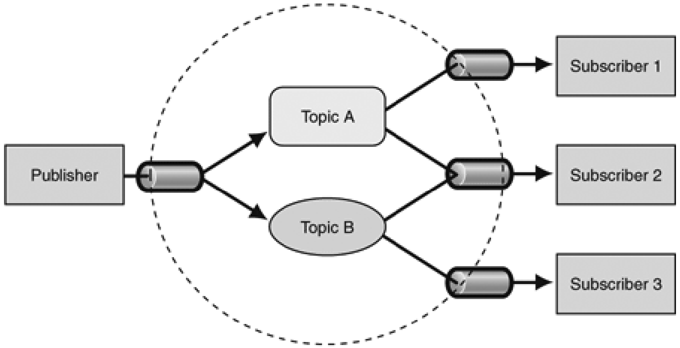
Alexandre Meslin

Gerenciando Dispositivos IoT Utilizando Plataforma de Blockchain

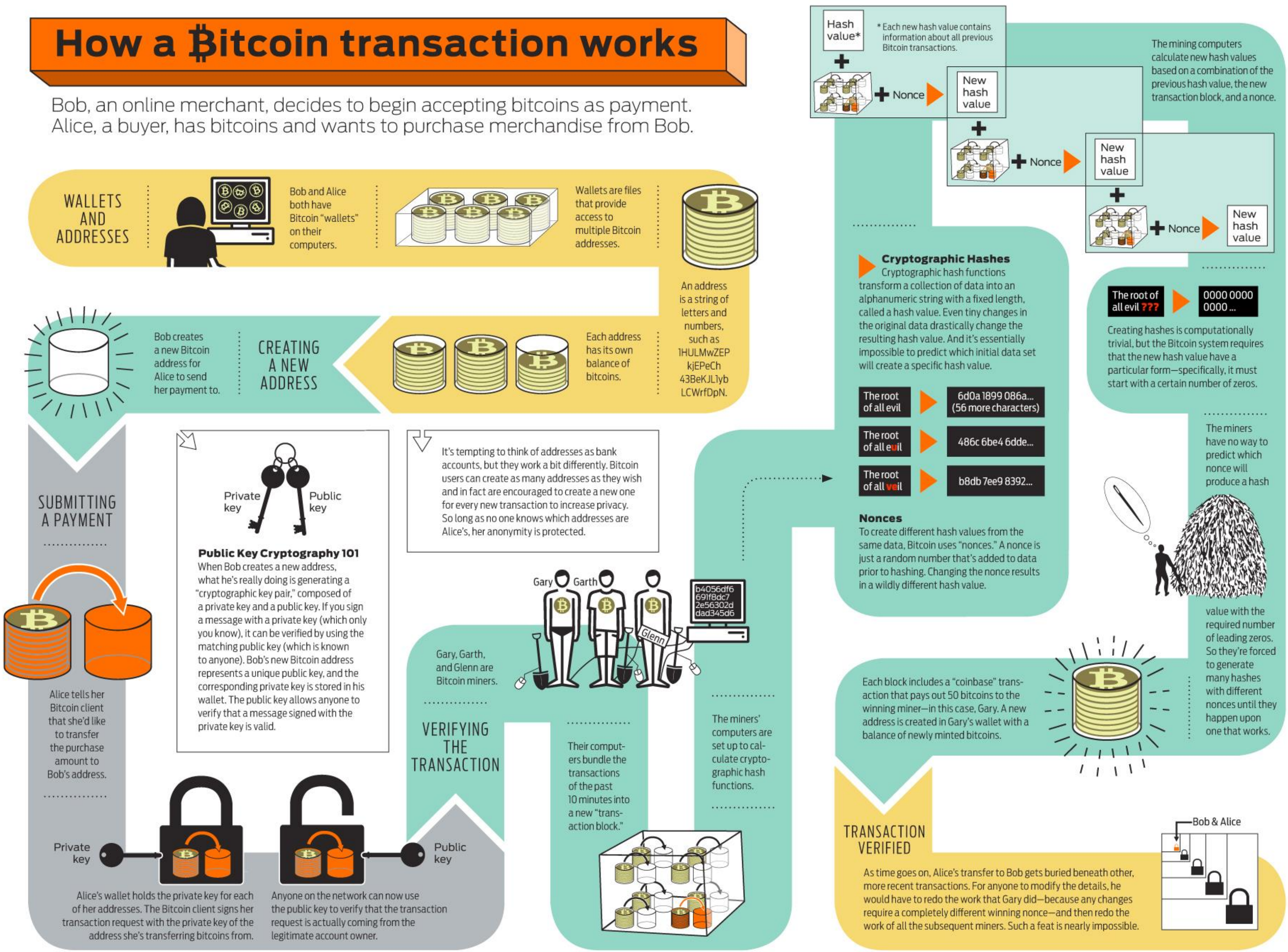
Problemas Abordados



- Cliente-Servidor
- Publisher-Subscriber



- Escalabilidade
- Segurança
- Redundância
- Resiliência
- Tolerância a falha
- Disponibilidade
- Descentralização



http://www.zerohedge.com/sites/default/files/images/user3303/imageroot/2013/05/20130512_BTC.jpg

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

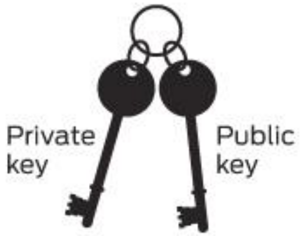
Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.



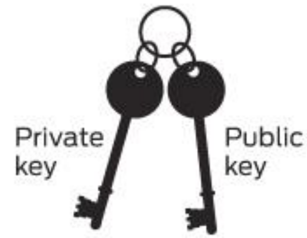
Public Key Cryptography 101

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

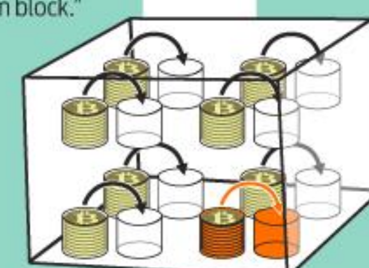
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.

Blockchain

- Livro-razão distribuído
- Armazena registro de todas as transações digitais
- Base de dados replicada e sincronizada
- Visível para todos na rede (pode ser implementado de forma privada)

Livro Razão - Escrituração

RAZÃO ANALÍTICO

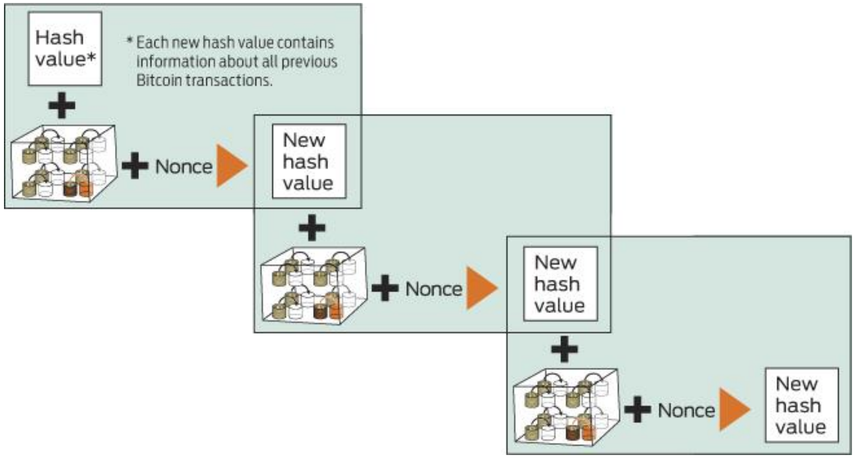
WRA Comércio Ltda. — **Data: 02.01.2012**
PJ: 01.342.575/0001-87 — **Período: 01 a 02.01.2012**

Conta: Bancos C/ Movimento - CEF

Data	Histórico	Débito	Crédito	Saldo
01.01.2012	Saldo Inicial			1.000,00 D
02.01.2012	Depósito	500,00		1.500,00 D
02.01.2012	Cheque nº 050070		200,00	1.300,00 D
Totais		**500,00**	**200,00**	**1.300,00 D**

Blockchain

- Livro-razão distribuído
- Armazena registro de todas as transações digitais
- Base de dados replicada e sincronizada
- Visível para todos na rede (pode ser implementado de forma privada)
- **Não pode ser adulterado!**



Ethereum

- Plataforma de software aberto
- Baseado em blockchain
- Blockchain semelhante ao do Bitcoin usado para armazenar informações financeira
- Blockchain do Ethereum pode ser utilizado para executar código descentralizado
- Mineradores ganham Ether (cripto-token)
- Ether utilizado para pagar taxas e serviços Ethereum

Vantagens do Ethereum

- Imutabilidade – terceiros não podem mudar dados ou códigos
- A prova de adulteração
- Incorruptível
- Seguro
- Downtime ZERO – sistema distribuído
- Período de bloco de 12 segundos (10 minutos com Bitcoin)

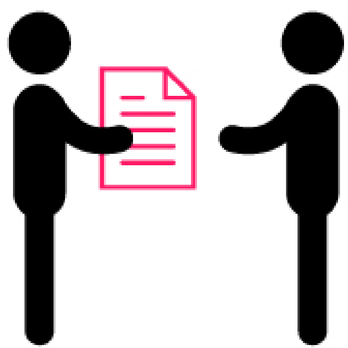
Smart Contrat

- Código executável
- Executa no blockchain quando ocorrem condições especiais
- Sem possibilidade de fraude ou interferência externa
- Código executado no Ethereum Virtual Machine (EVM)

- SZABO, Nick. Smart contracts. **Unpublished manuscript**, 1994.
- SZABO, Nick. Formalizing and securing relationships on public networks. **First Monday**, v. 2, n. 9, 1997.

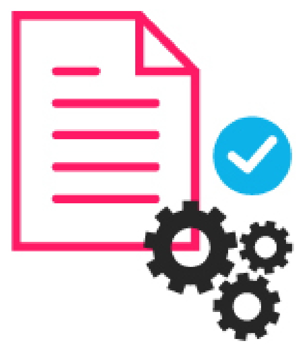
Smart Contract

1



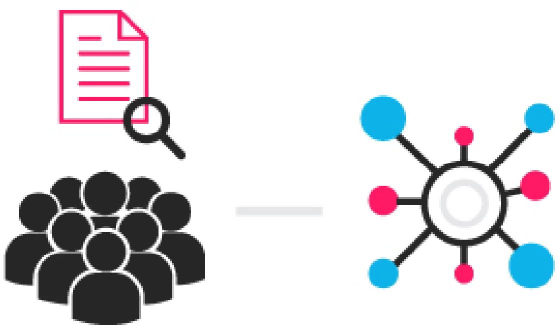
An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2



A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3



Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

https://blockgeeks.com/guides/what-is-ethereum/

Smart Contract

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                          // Subtract from the sender
    balanceOf[_to] += _value;                            // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Controlando IoT com Blockchain

- HUH, Seyoung; CHO, Sangrae; KIM, Soohyung. Managing IoT devices using blockchain platform. In: **Advanced Communication Technology (ICACT), 2017 19th International Conference on**. IEEE, 2017. p. 464-467.

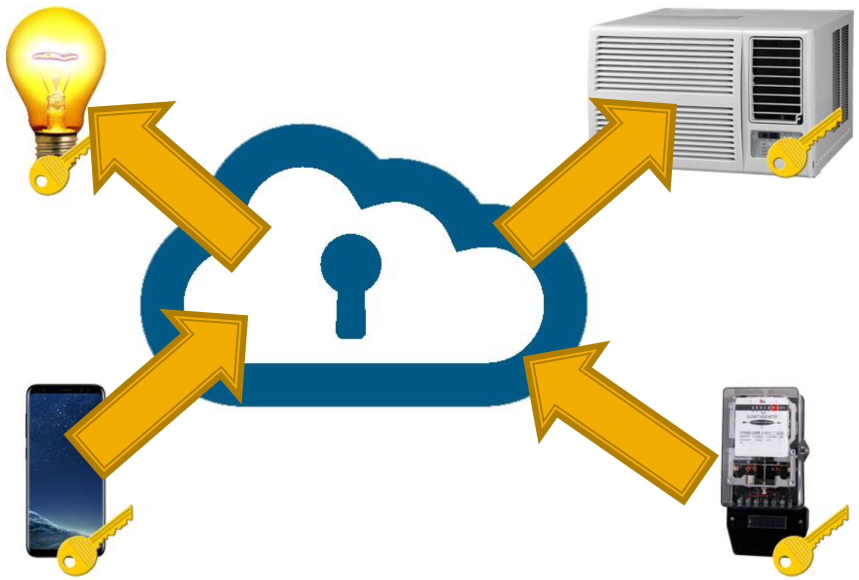
- Autenticação baseada em chave pública
- Configuração de dispositivos IoT usando Ethereum
- Aplicações IoT em geral

Controlando IoT com Blockchain

- Problemas abordados:
  - Centenas de dispositivos conectados
  - Vulnerabilidade do servidor
  - Dados forjados
  - Ataque DoS

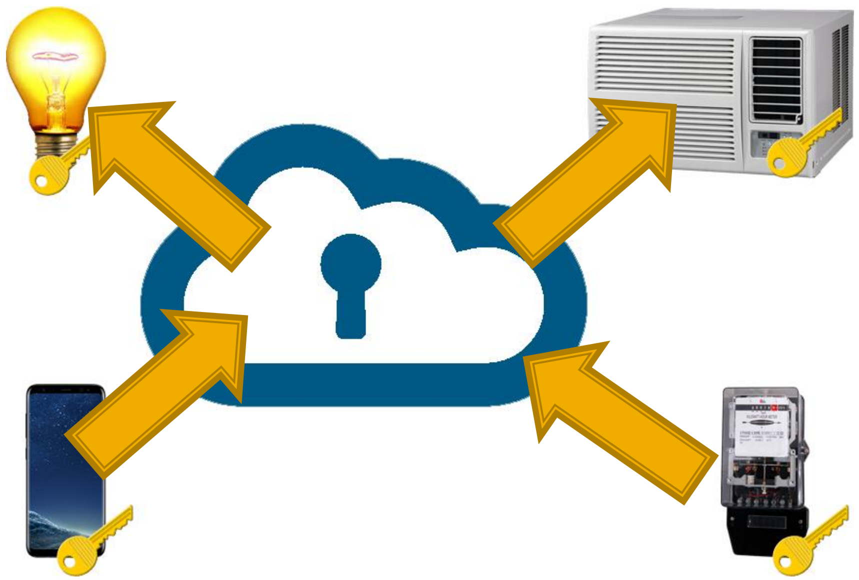
Cenário

- Usuário
- Lâmpada
- Condicionador de ar
- Medidor de consumo de eletricidade



Cenário

- Sistema distribuído
- Cada participante contém parte do blockchain
- Todas as transações são executadas em consenso
- Smart contract com byte code



Contratos

```
contract Meter{
  int value;
  bytes publicKey;
  bytes signature;
  update(int _value, bytes _publicKey, bytes _signature){
    value = _value;
    publicKey = _publicKey;
    signature = _signature;
  }
}
```

```
update(300, "deadbeef", "babebabe");
```

- Keccak-256
- 4 primeiros bytes

```
f1de8ccb000000000000000000000000000000000000000000
000000000000000000012c00000000000000000000000000000
000000000000000000000000000000000600000000000000000
0000000000000000000000000000000000000000000000a0000
000000000000000000000000000000000000000000000000000
0000000004deadbeef000000000000000000000000000000000
000000000000000000000000000000000000000000000000000
000000000000000000000000000000000004babebabe0000000
0000000000000000000000000000000000000000000000000
```

Contratos

- Celular envia os dados para o smart contract

- Lâmpada e condicionador de ar recebem dados via Ethereum

- Obs.: autores utilizaram infraestrutura personalizada de gerenciamento de chaves públicas

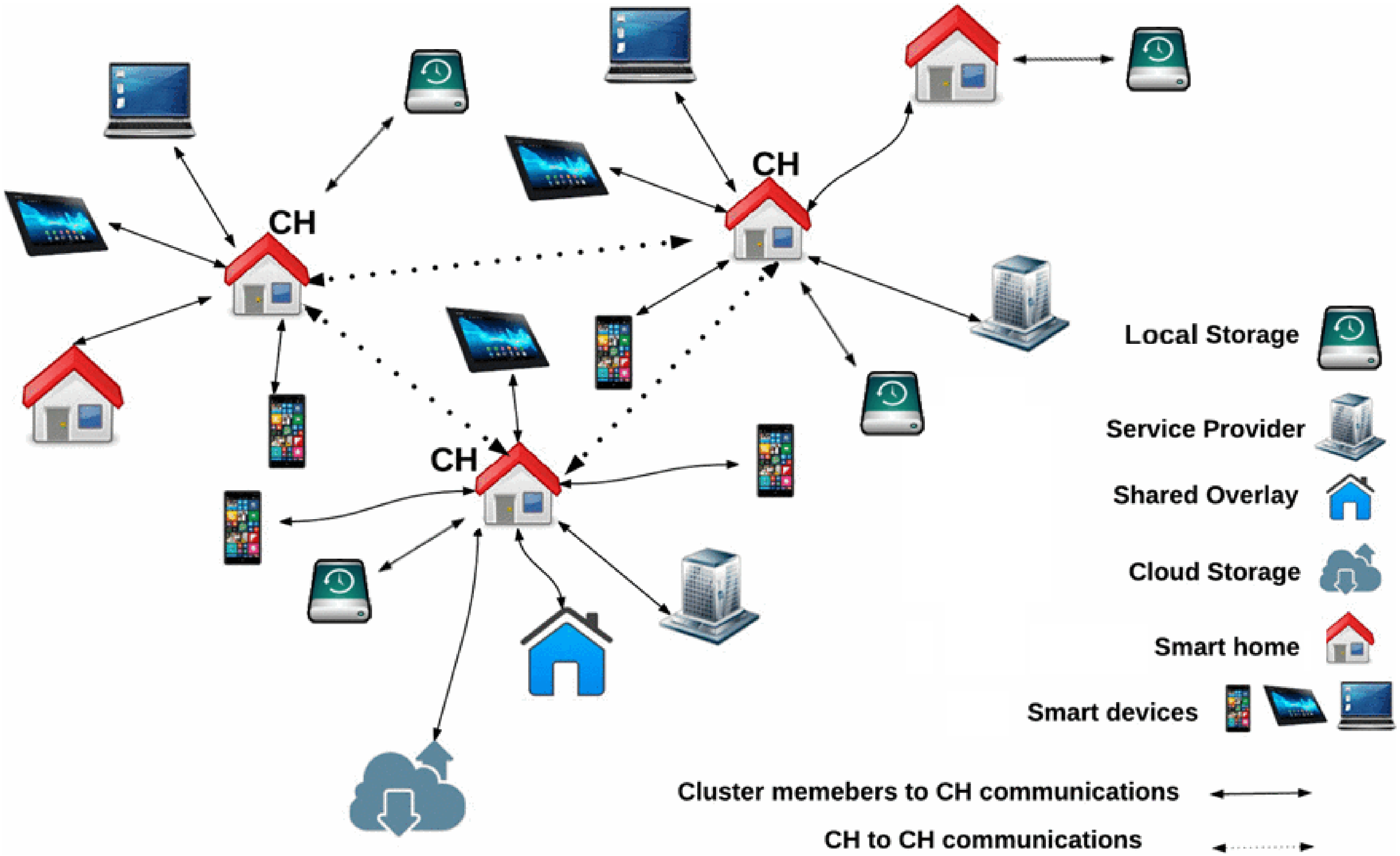
```
contract ACPolicy{
  int acLimit;
  bytes publicKey;
  bytes signature;
  update(int _acLimit, bytes _publicKey, bytes _signature){
    acLimit=_acLimit;
    publicKey=_publicKey;
    signature=_signature;
  }
}
```

Blockchain e Smart Homes

- DORRI, Ali; KANHERE, Salil S.; JURDAK, Raja. Blockchain in internet of things: Challenges and Solutions. **arXiv preprint arXiv:1608.05187**, 2016.

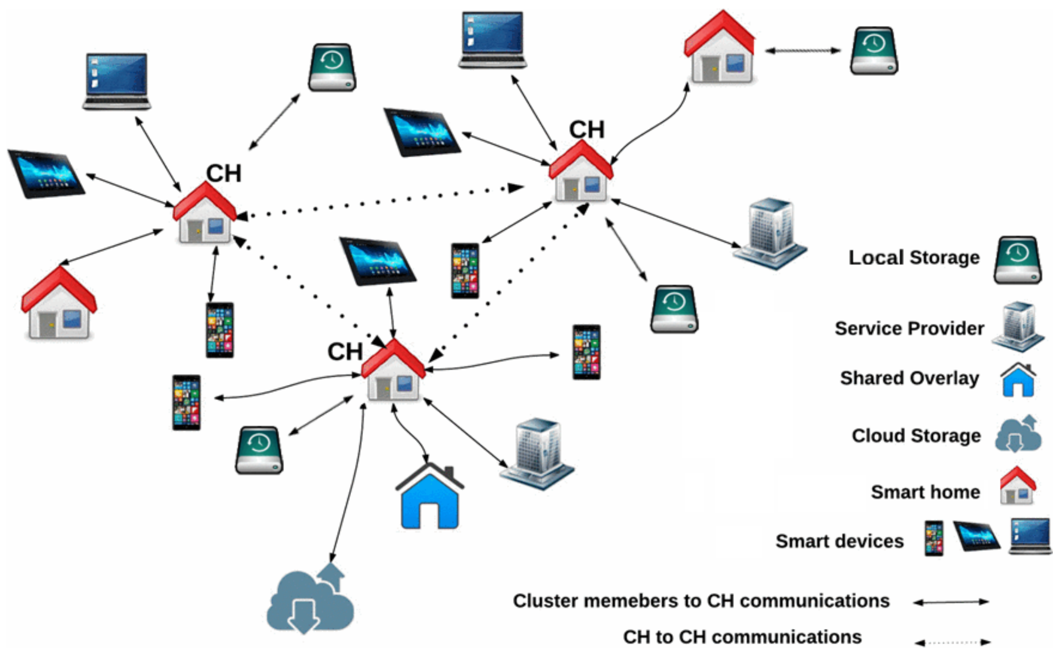
- DORRI, Ali et al. Blockchain for IoT security and privacy: The case study of a smart home. In: **Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on**. IEEE, 2017. p. 618-623.

Blockchain e Smart Homes



Blockchain e Smart Homes

- Eliminação de PoW – aumento de velocidade
- Criação de Cluster Head – diminuição de tráfego de dados
- Uso de chave simétrica – simplificação
- Armazenamento local
- Armazenamento na nuvem



Conclusões

- 12 segundos pode ser muito tempo
- Muitos dados para serem armazenados em um dispositivo IoT
- Ethereum não prevê o uso de *light client*
- Necessário o uso de um proxy para armazenar o blockchain
  - Armazenamento externo
  - Armazenamento na nuvem

Bibliografia

- SZABO, Nick. Smart contracts. **Unpublished manuscript**, 1994.
- SZABO, Nick. Formalizing and securing relationships on public networks. **First Monday**, v. 2, n. 9, 1997.
- S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Disponível em **<https://bitcoin.org/bitcoin.pdf>**. Último acesso em 2017-06-20. 2008.
- HUH, Seyoung; CHO, Sangrae; KIM, Soohyung. Managing IoT devices using blockchain platform. In: **Advanced Communication Technology (ICACT), 2017 19th International Conference on**. IEEE, 2017. p. 464-467.
- DORRI, Ali et al. Blockchain for IoT security and privacy: The case study of a smart home. In: **Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on**. IEEE, 2017. p. 618-623.

Alexandre Meslin

Managing IoT Devices using Blockchain Platform