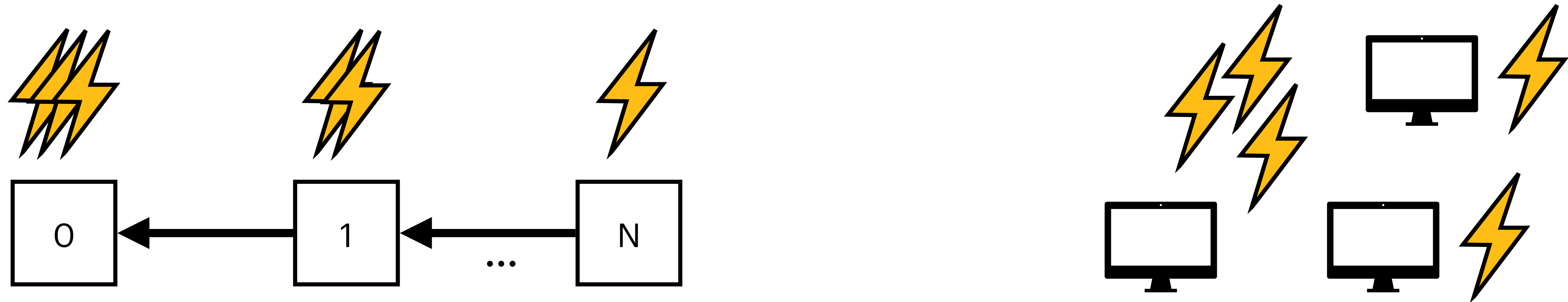


A Different Form of Consensus

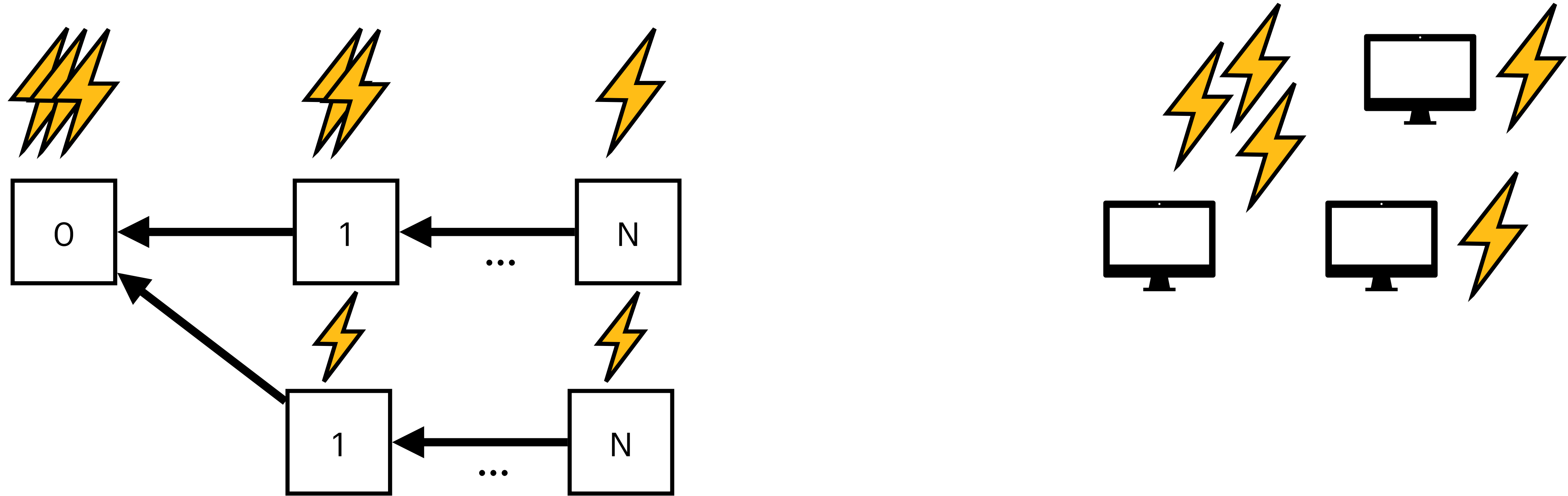
Proof of Work & Proof of Stake

Proof of Work (PoW)



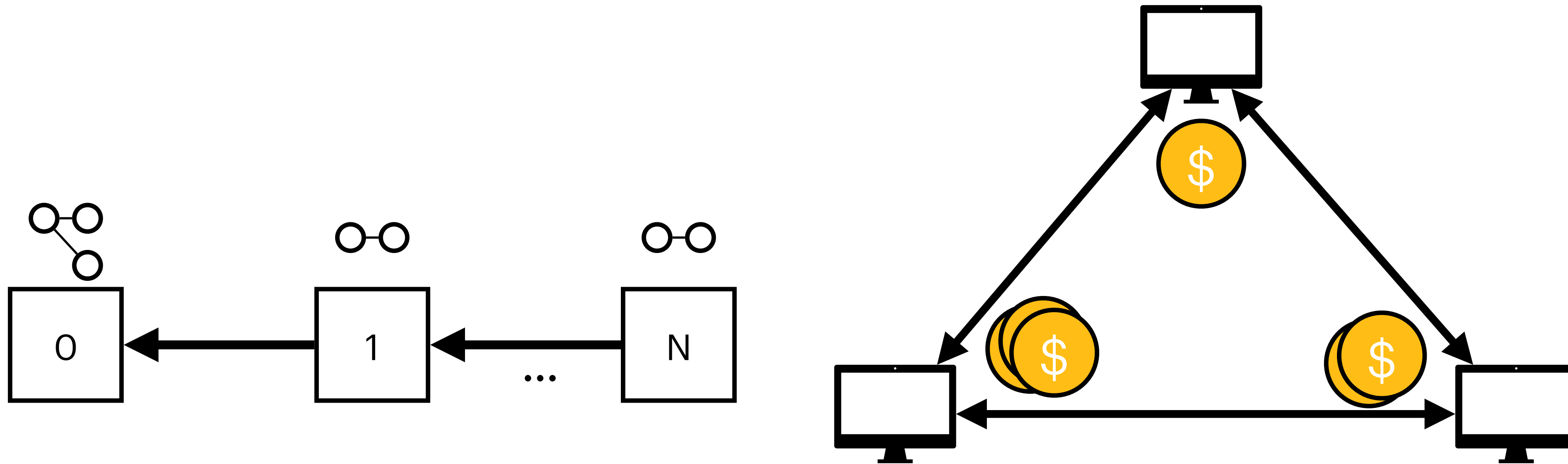
- Mineradores competem uns com os outros para produzir blocos.
- Dificuldade $< x$ para produzir 1 bloco a cada 10 minutos.
- Alto custo energético.
- Quantidade de membros escalável.
- Ex. Bitcoin.

Forks & 51% Attack



- Chain com mais energia (mais pesada) ganha
- Esperar um tempo até algum Fork ganhar.

Proof of Stake (PoS)



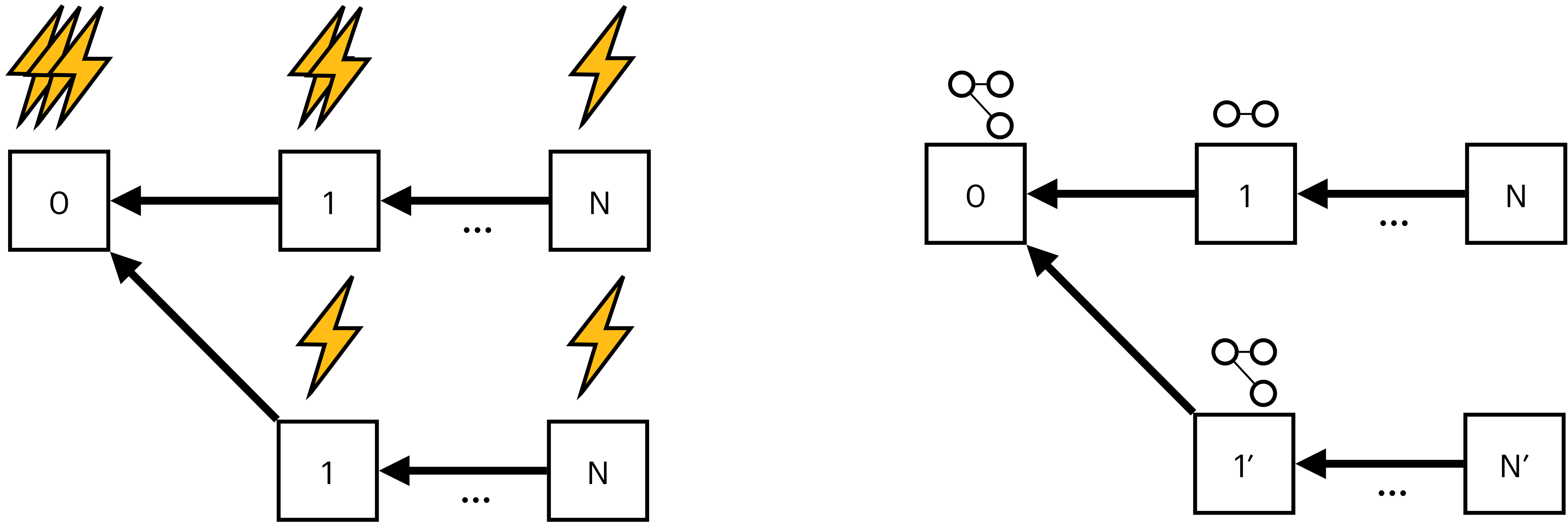
- Stakers fazem um consenso sobre o próximo bloco a ser produzido.
- Difícil escalar quantidade de membros (alto custo de mensagens).
- Baixo custo energético.
- Alta subjetividade.
- Ex. Ethereum, Solana, Avalanche

Always have been

So it was Paxos all along?

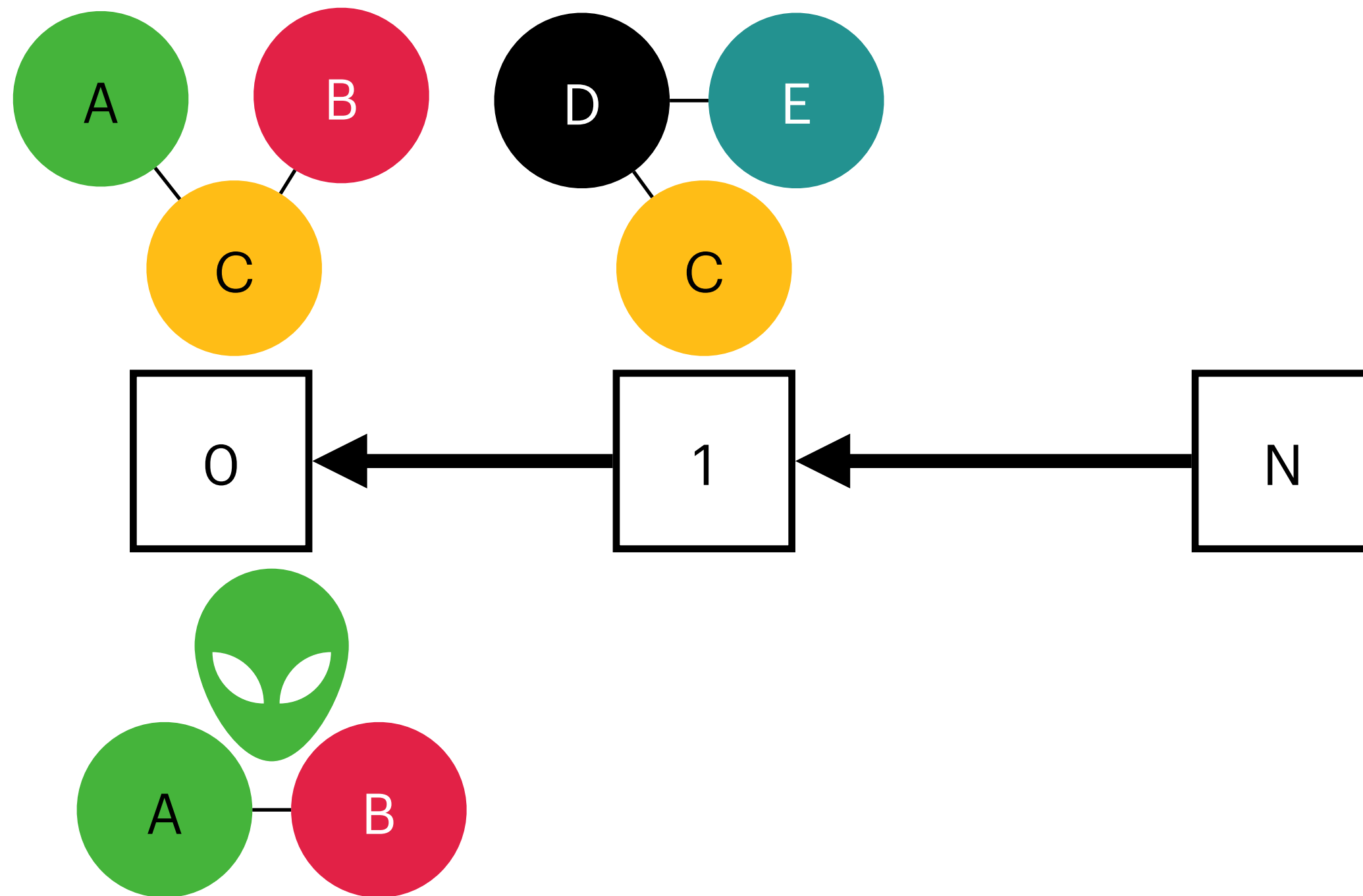


Subjetividade



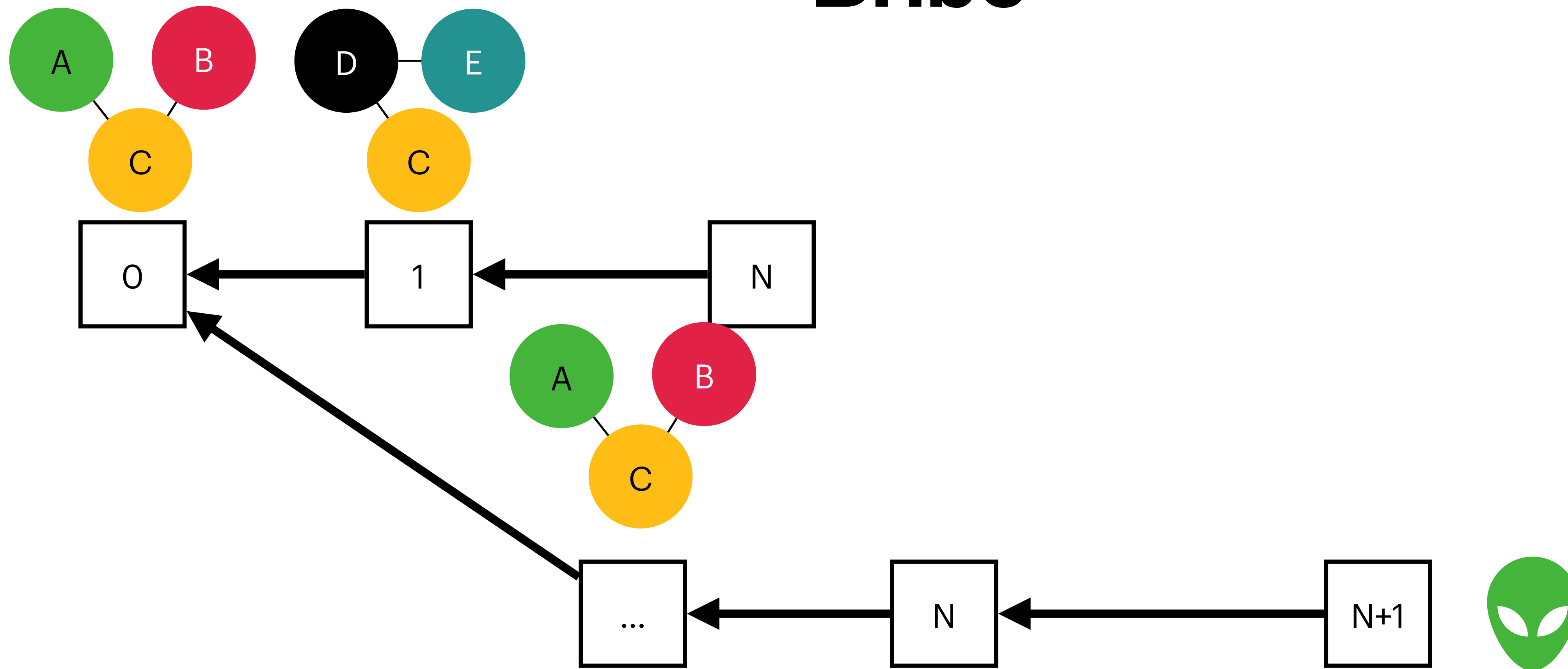
- Olhando cada dificuldade, podemos relacionar PoW com consumo.
- Olhando somente a chain PoS não se pode dizer nada.

Bribe



- Olhando cada dificuldade, podemos relacionar PoW com consumo.
- Olhando somente a chain PoS não se pode dizer nada.

Bribe



- Olhando cada dificuldade, podemos relacionar PoW com consumo.
- Olhando somente a chain PoS não se pode dizer nada.

Smart Contracts

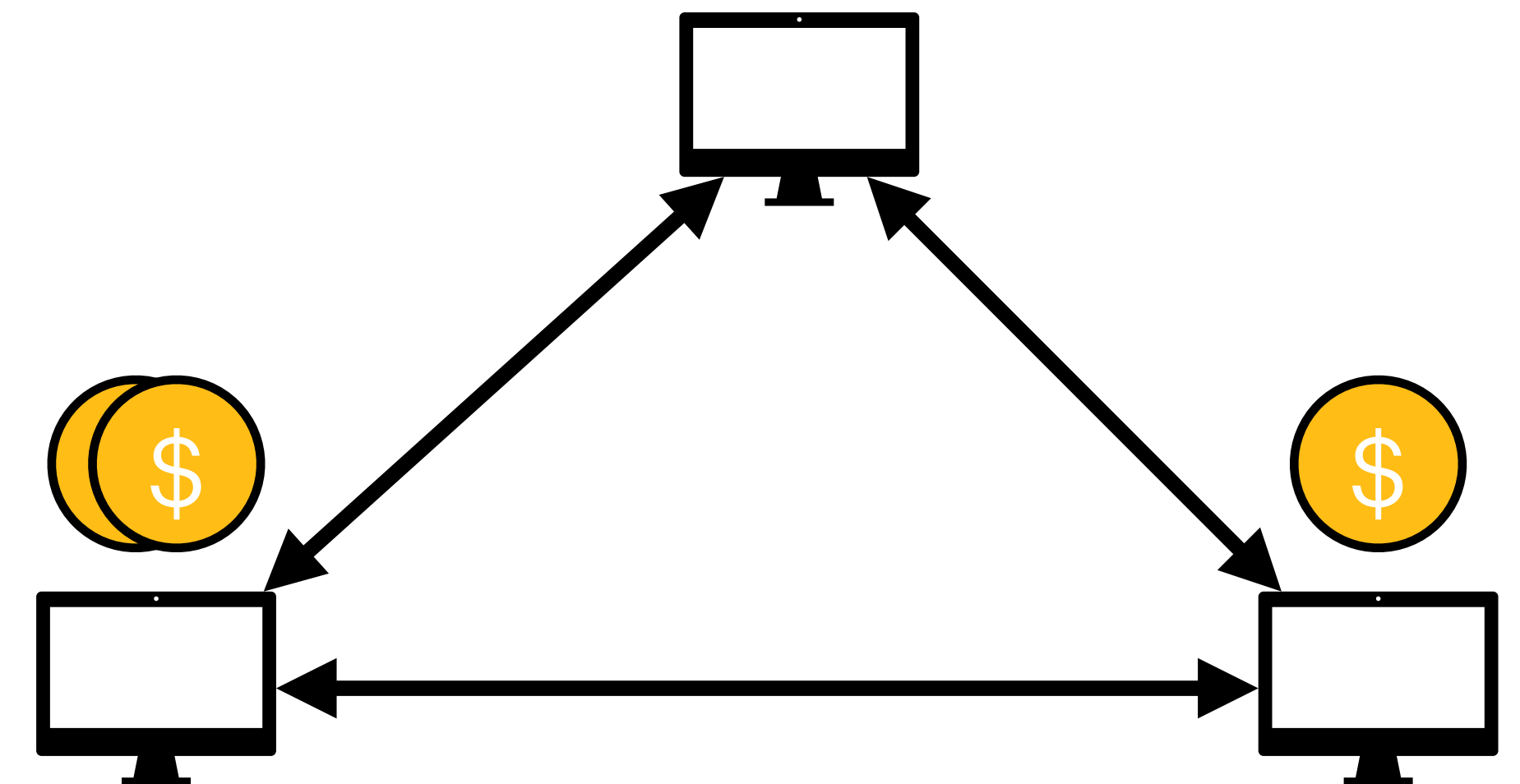
- Programação em Blockchains.
- Aproveitar **interface** de consenso.
- Um banco de dados programável distribuído tolerante a falhas.
- Programas agora podem ter uma noção de **valor**.

Vulnerabilidades

- Transações irreversíveis.
- Contratos sem upgrade.
- DAO Hack: 3.6 milhões Eth = \$5.76 bilhões
- Mais que qualquer outro roubo à época.

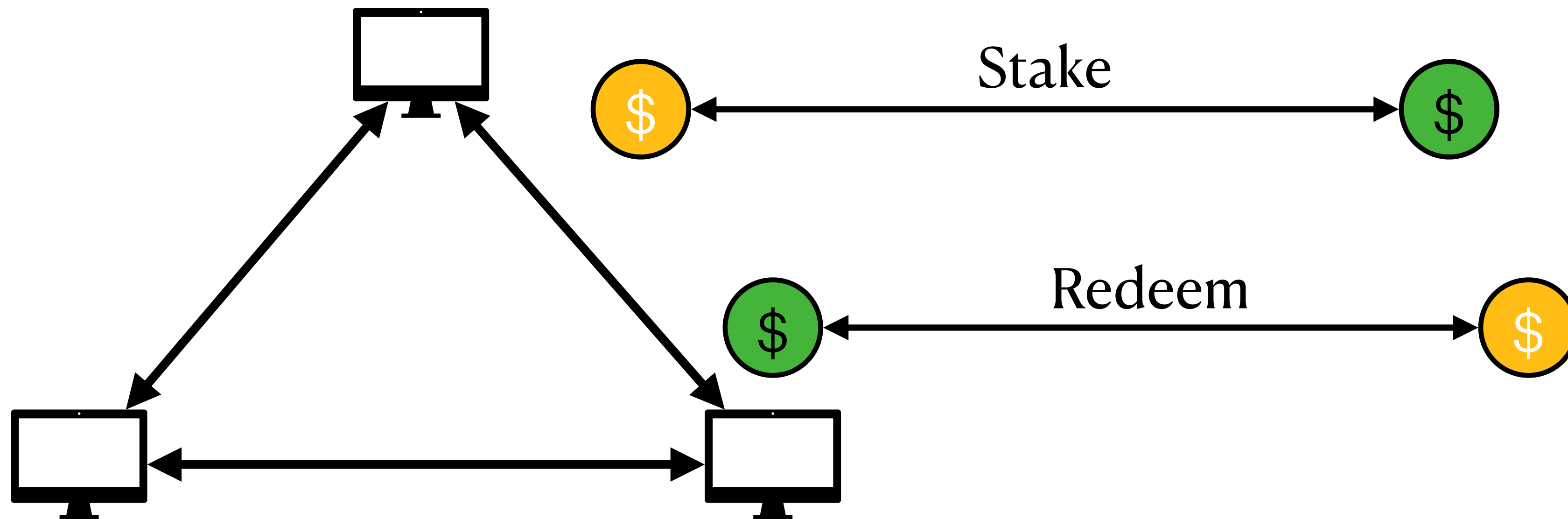
Solido - Solana

Chorus-one



- Stakers fazem stake em contas
- Os depósitos são feitos travando o stake por um interesse futuro (similar a um título)
- Os fundos não podem ser movidos por um certo tempo.

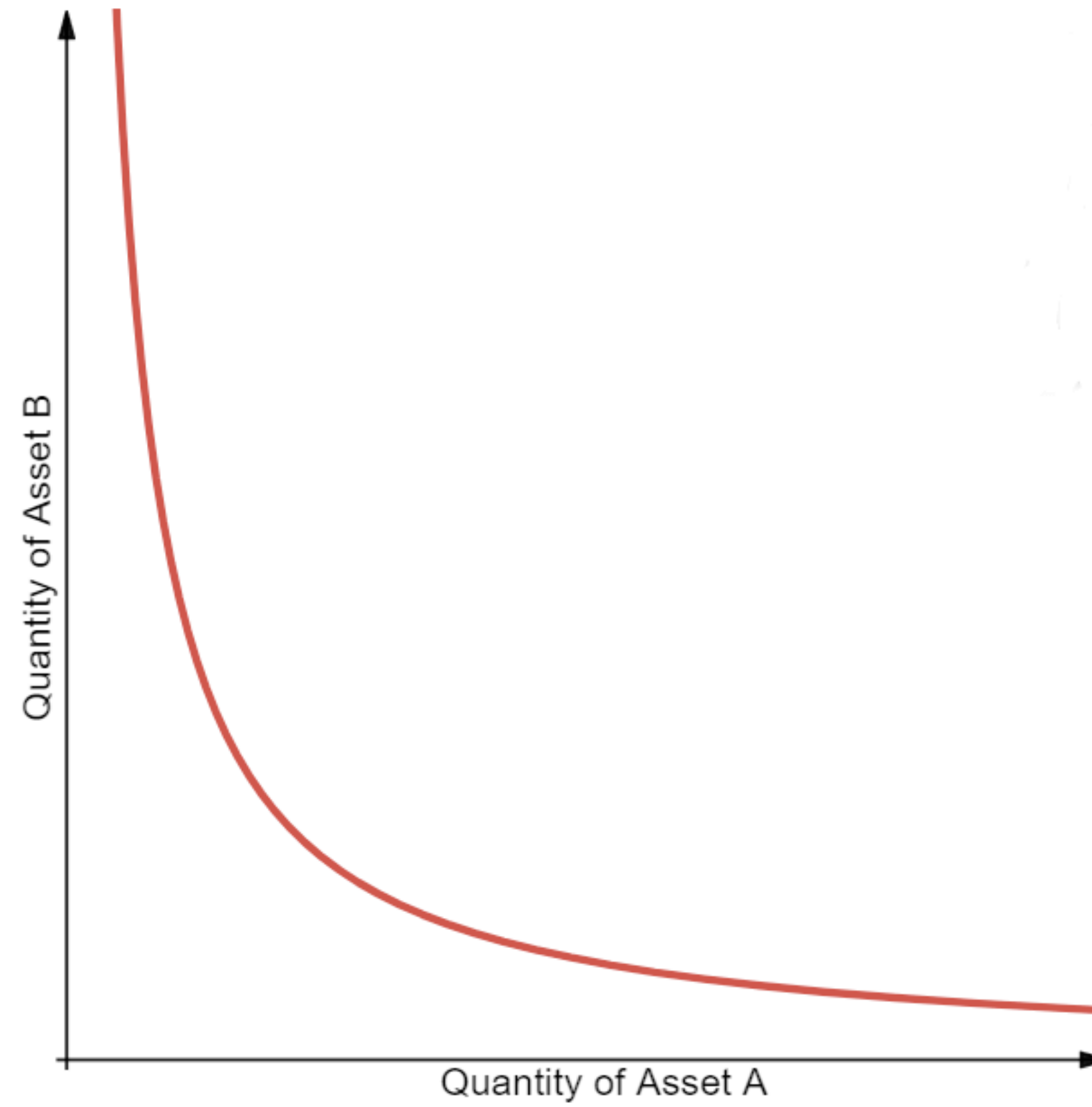
Solido (Chorus One)



Stake com liquidez

- O stake que estaria bloqueado agora pode ser utilizado em outras coisas como:
 - Uso em outros protocolos.
 - Empréstimos.
 - Provedor de liquidez.

Mercado: Sol x stSol



- AMM: Automatic Market Maker
- $\text{token}_a * \text{token}_b = \text{constante}$

Exemplo: AMM

A: 45

B: 30

$a \cdot b = 1350$

swap(a)

A: 5

AMM {

reserva_a = 45;

reserva_b = 30;

reserva_a * reserva_b = constante

}

Exemplo: AMM

AMM {

reserva_a = 45;

reserva_b = 30;

reserva_a * reserva_b = constante

}

A: 45

B: 30

$a \cdot b = 1350$

swap(a)

A: 5

$1350 = 50 \cdot b = 27$

$B \leftarrow 3$

Exemplo: AMM

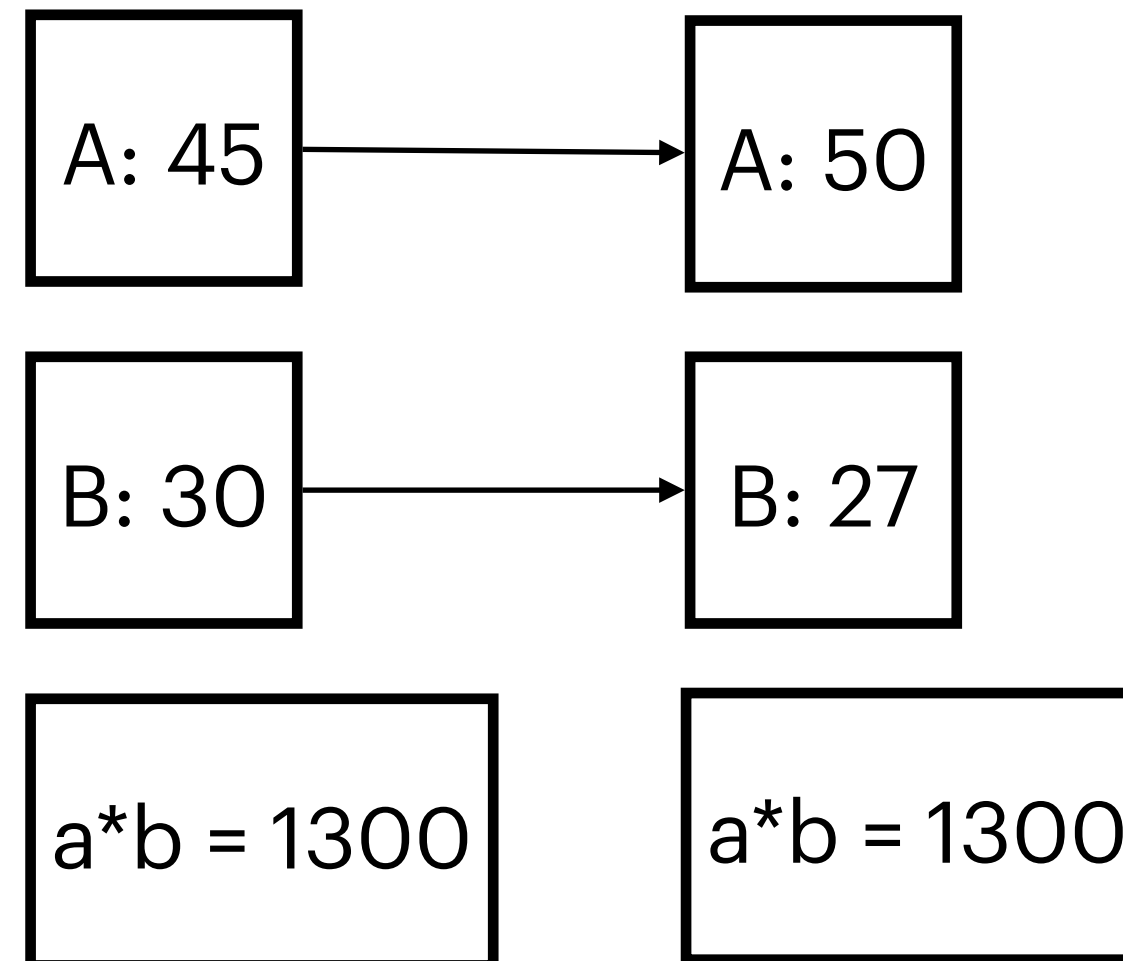
AMM {

 reserva_a = 50;

 reserva_b = 27;

 reserva_a * reserva_b = constante

}



swap(a)

A: 5

$1350 = 50 * b = 30$

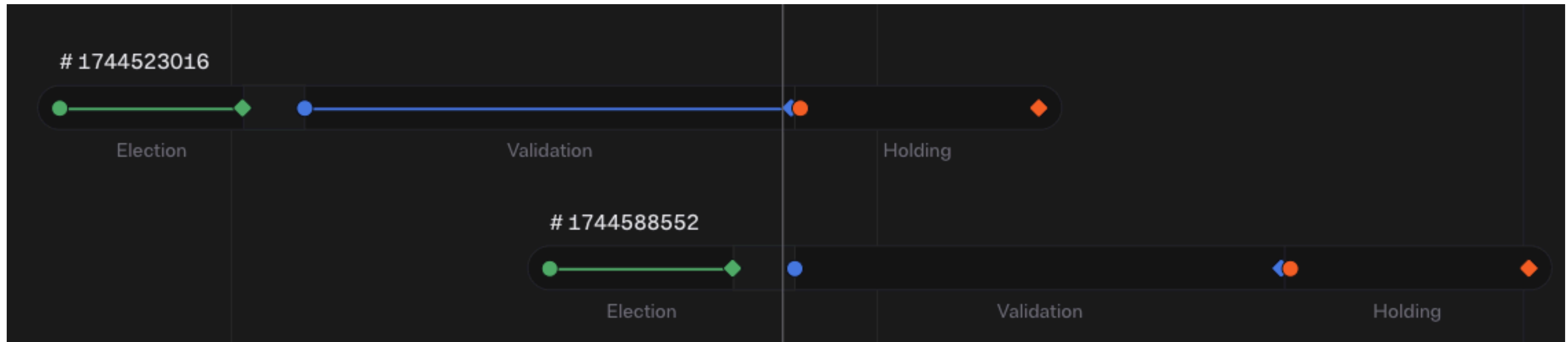
B <- 3

TON

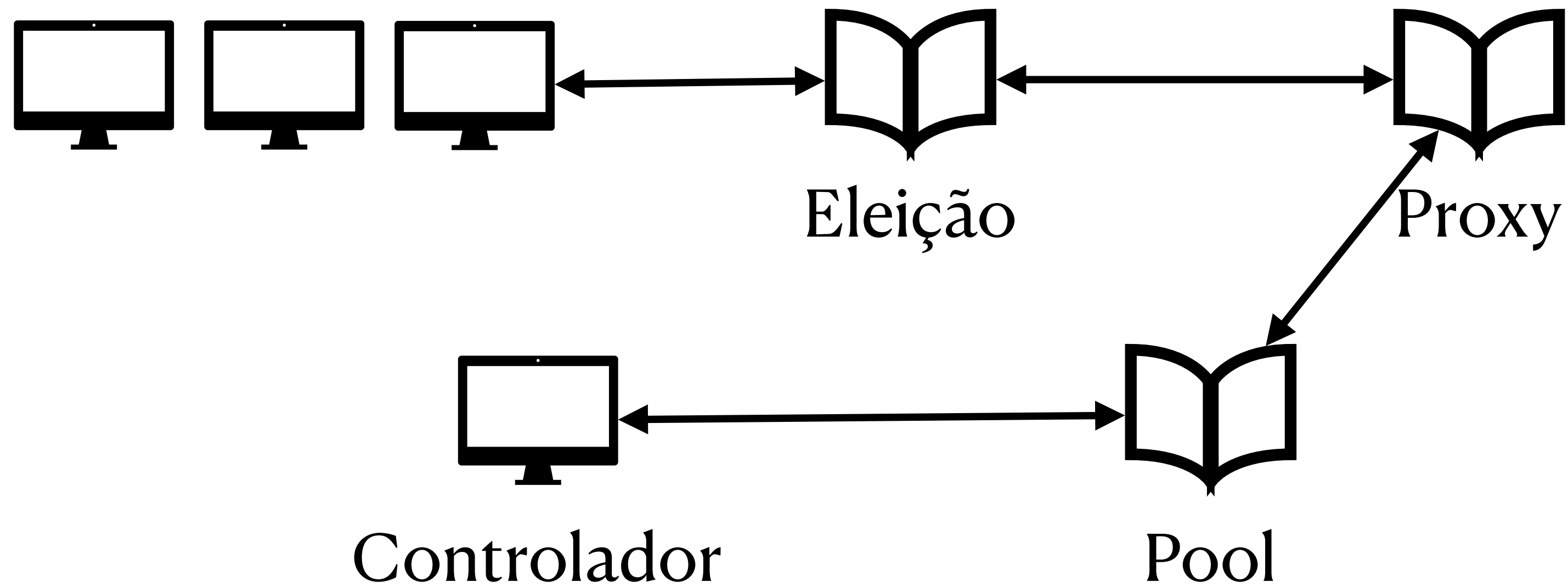
- Cada conta vive em sua própria partição.
- Mensagens podem ser enviadas com uma resposta, não existem transações.
- Diferente design para construção de smart contracts.
- Possibilidade de escalar partições conforme necessário.

TON

Eleições baseadas em stake

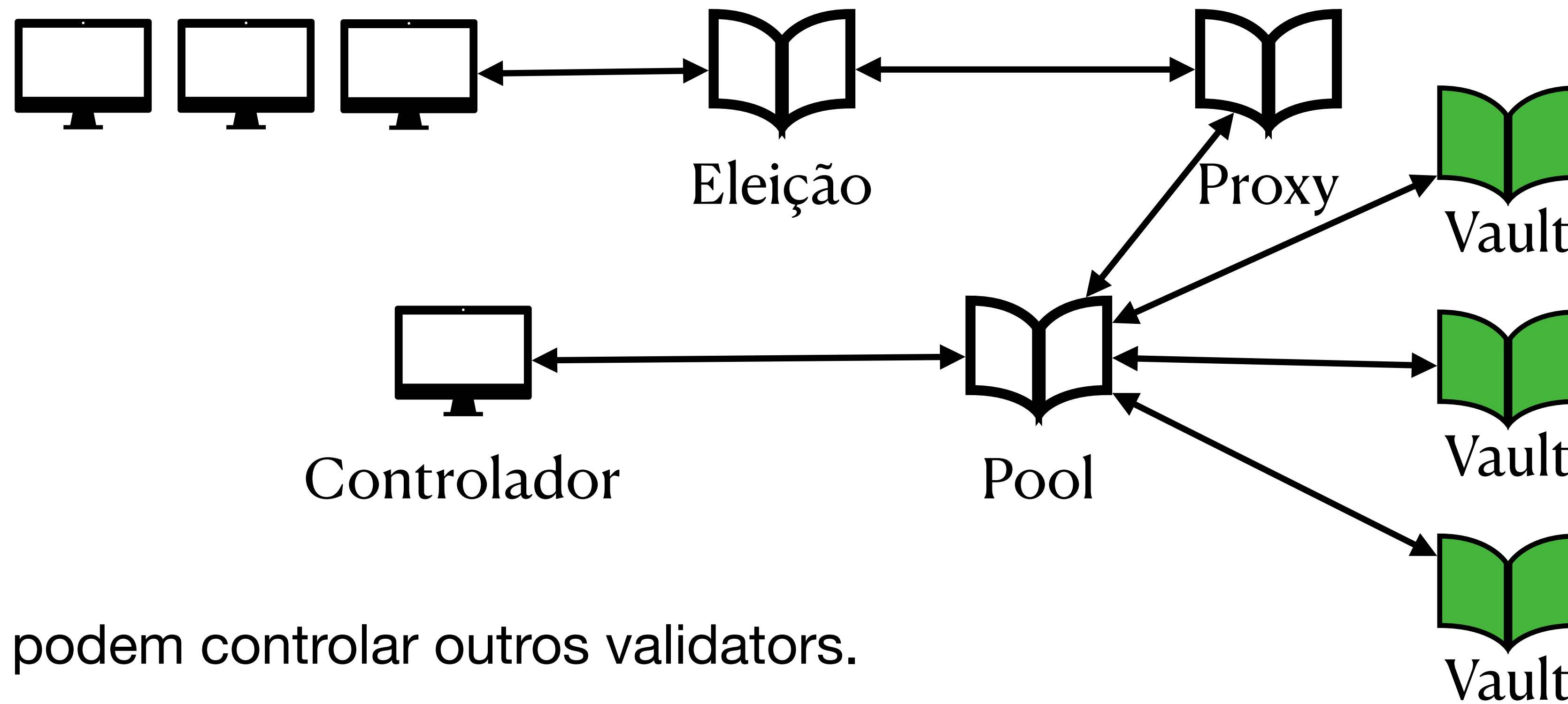


Pool



- Pool podem eleger mais de um validator.
- Contratos podem fazer parte da pool.
- Fácil de manter.

Pool v2

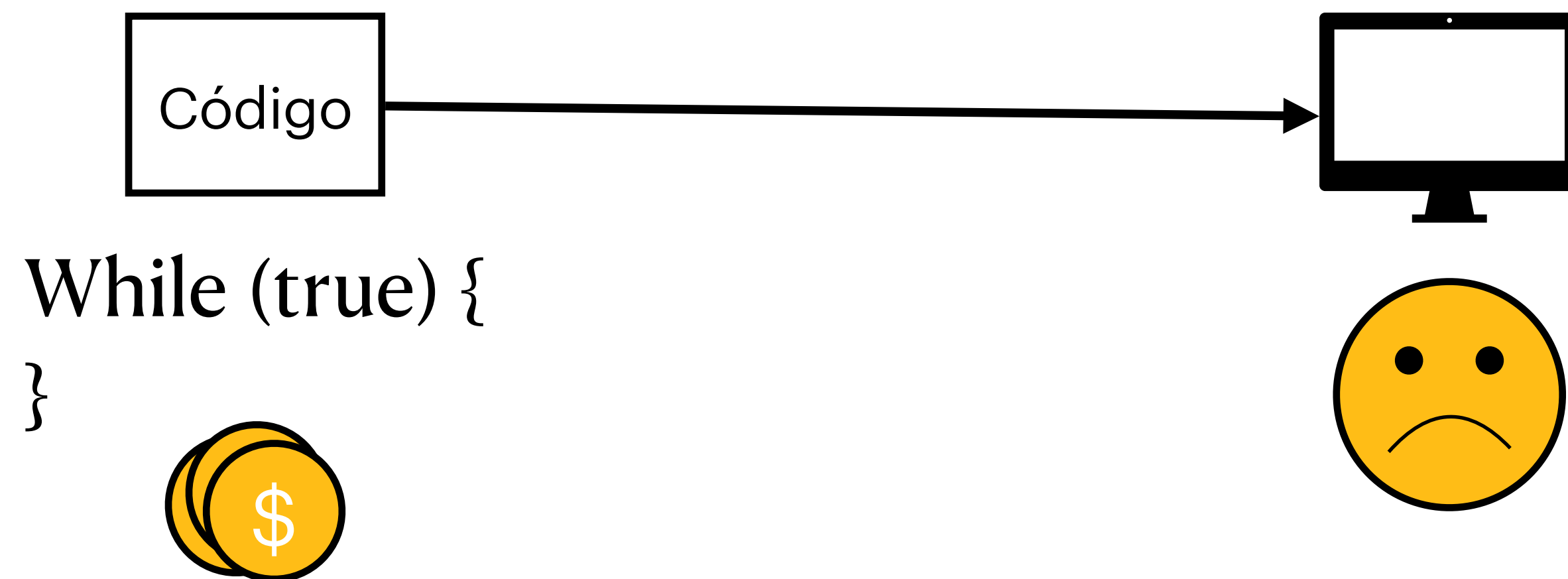


- Vaults podem controlar outros validators.
- Diferentes parâmetros de vault.
 - Liquid staking.

Conclusão

- Diferenças entre PoW e PoS.
- Smart contracts podem expandir e melhorar o sistema.
- Recursos para construir modelos de programas económicos.
- Absorvido pelo sistema financeiro/bancos?

Exemplo



Exemplo

