

RNP RAP

Serviço de Registro, Autenticação e Preservação Digital de Documentos

Guido Lemos (UFPB), Rostand Costa (UFPB), Daniel Faustino (UFERSA)

InovaTIC

Fortaleza

26/Março/2018



MOTIVAÇÃO E CONTEXTO

Relatos de Fraudes Apenas no Último Mês

15/05/2017 23:31 - Atualizado em 16/05/2017 07:02

Preso professor acusado de vender diploma falso em Nova X Polícia

Quarta-Feira, 03 de Maio de 2017, 23h:12 | Atualizado: A | A

R\$ 550

Sedu pode levar até 180 dias para investigar diplomas falsos

16 de maio de 2017

Cinco diplomas falsos em Guarapari

Por Da Redação - 18 de maio de 2017

Renato Silva confessou ter usado diploma falso da Universidade de Cuiabá (Unic) para solicitar inscrição no Conselho Regional de Educação Física (CREF)

Renato Silva confessou ter usado diploma falso da Universidade de Cuiabá (Unic) para solicitar inscrição no Conselho Regional de Educação Física (CREF)

Evolução Tecnológica x Transformações Culturais

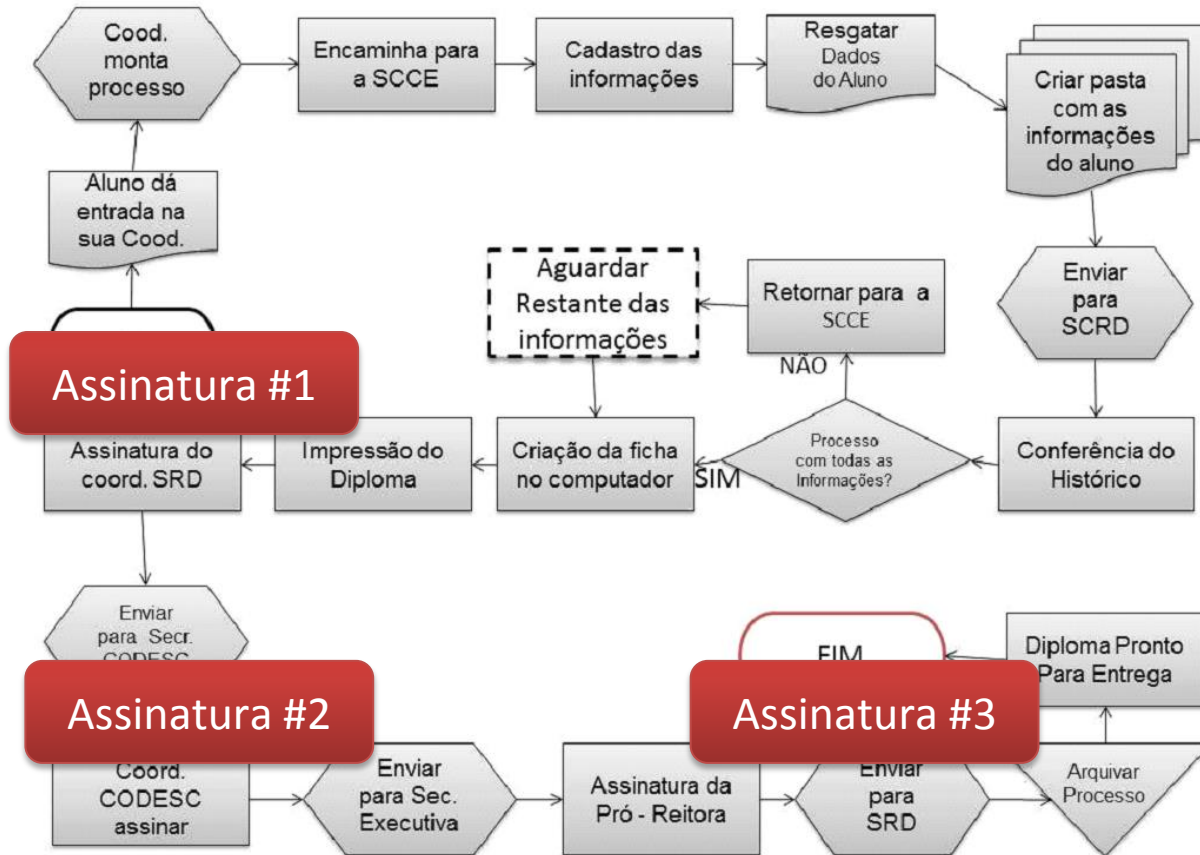
- Em outubro/2011 a UNIVAP fez uma consulta ao MEC sobre a emissão de diploma digital:
“...se a **expedição de diploma em formato digital em substituição ao impresso** em papel simples ou padrão, **sem opção ao formando e com custo pelo segundo, é medida amparada por ato administrativo interno...**”
- Emitido em junho/2012 o parecer final (CNE 226/12) foi:
“...a **adoção da nova sistemática pela UNIVAP não pode causar transtornos** ao formando no momento em que ele mais necessita de seu diploma para obter registro profissional no órgão de classe pertinente, entende este Relator que, até que haja plena regulamentação do tema pelo MEC, **as instituições de ensino superior que estiverem adotando a nova sistemática também forneçam aos formandos o diploma na forma convencional (em papel) ...**”

Atores e Fluxos Principais

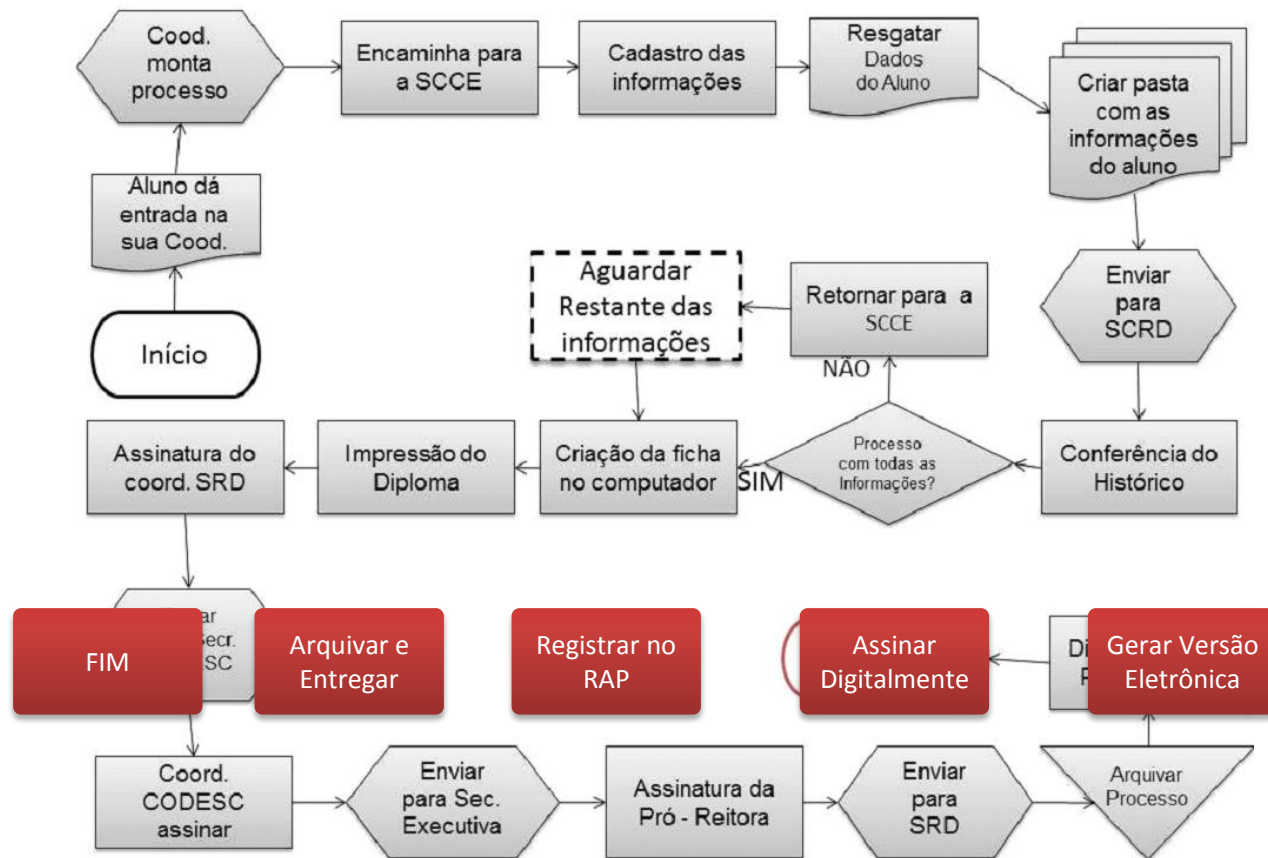


lavid

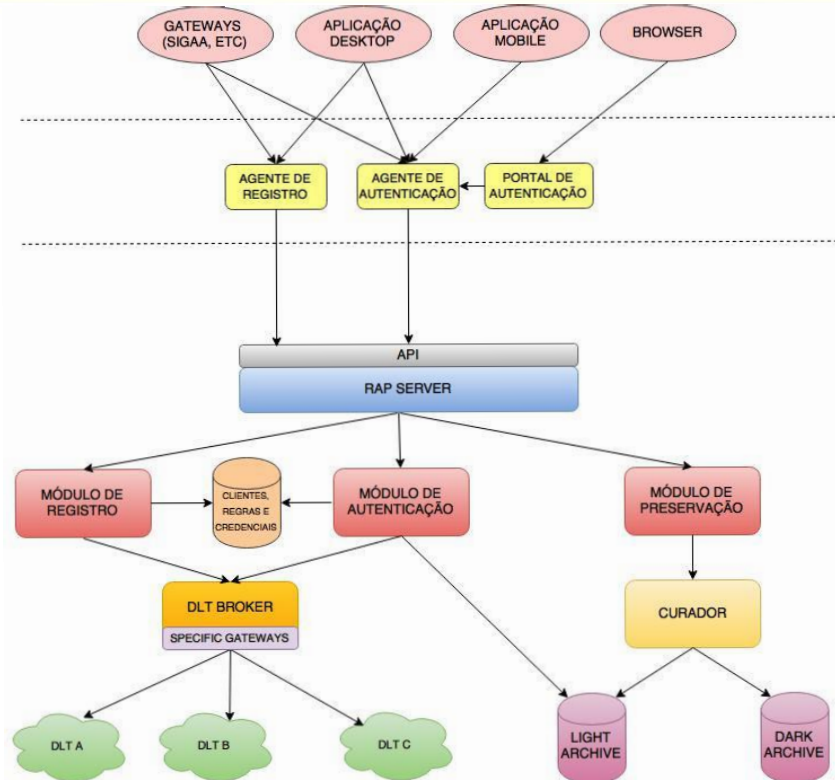
Emissão de Diplomas: Fluxo Atual UFPB



Possível Estratégia de Integração/Transição



Visão Arquitetural Preliminar



lavid

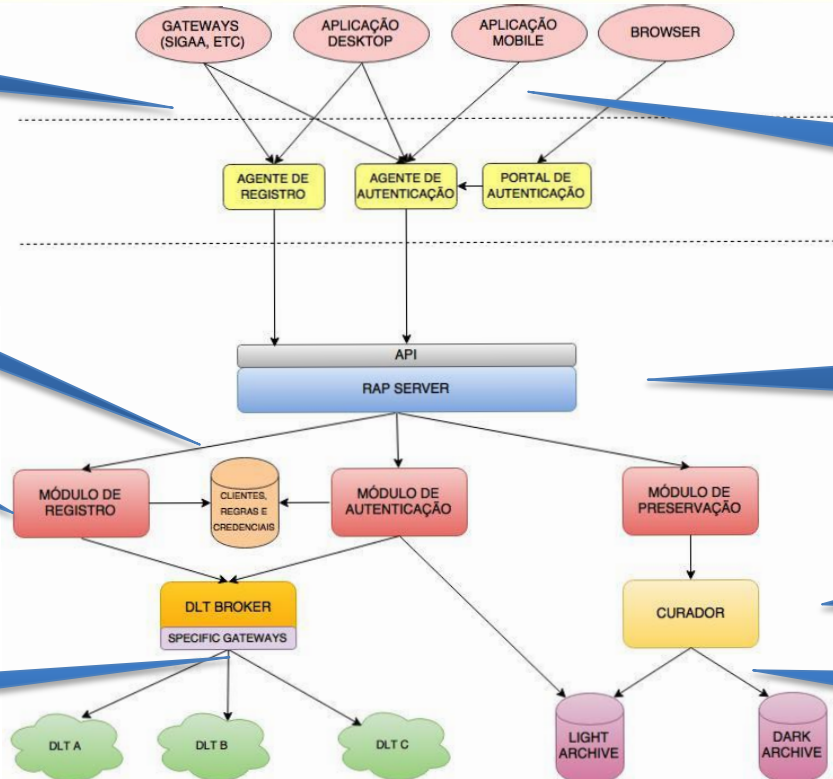
Tecnologias Utilizadas/Candidatas (Fase 1)

PDF/A (F1)
OpenBadges (F2)

ICP EDU (F1)
ICP Brasil (F2)

MIT BlockCerts (F1)
Chainpoint (F2)

Bitcoin (F1), Ethereum,
Hyperledger ou permissionária (F2)



Emissão e Assinatura:
Geração Simulada (F1)
Workflow/Portal (F2)

Mean Stack (F1)
Microsserviços,
RabbitMQ e
Docker (F2)

Archivematica (F1)

Local (F1)
Swift RNP e
TDR (F2)



lavid



Blockchain

Conceitos e Aplicações



lavid



GT-RAP: Workshop de Transferência de Conhecimento
João Pessoa, 19-20/03/18

COMO BLOCKCHAIN FUNCIONA



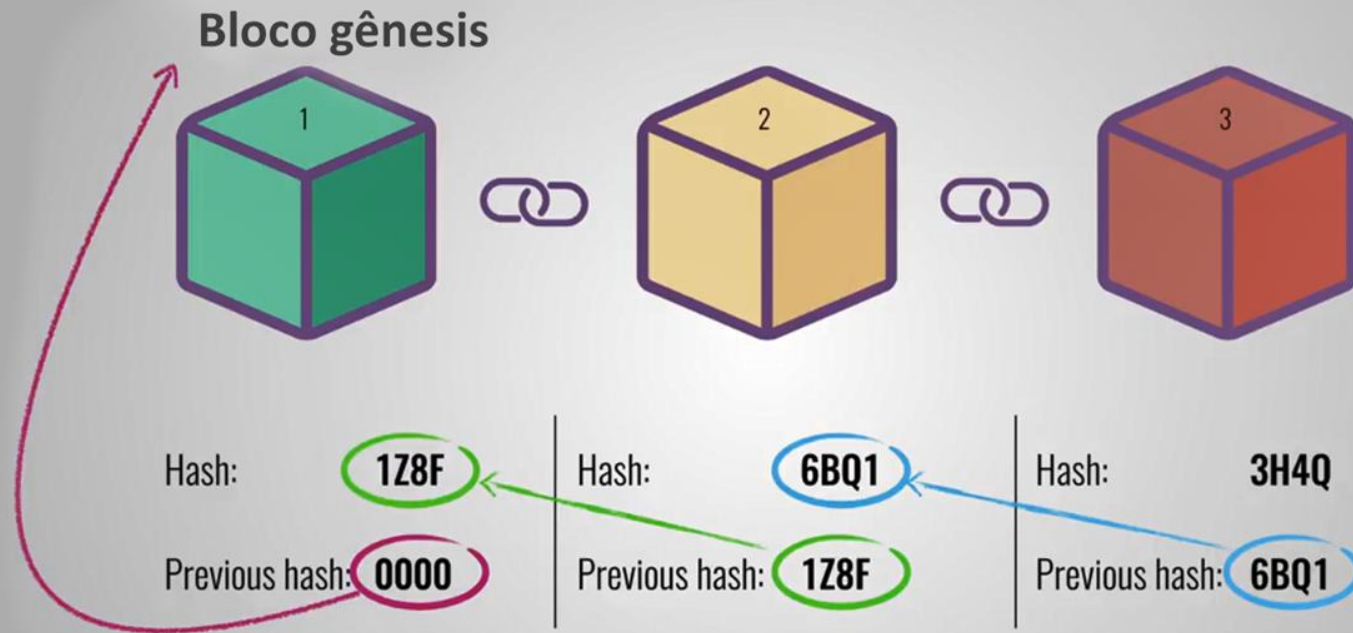
Razão Distribuído (Distributed Ledger)

Uma blockchain é um registro de transações público, confiável e compartilhado:
→ qualquer um pode inspecionar e não é controlado por ninguém em particular



Uma propriedade relevante é que uma vez inserida uma informação na blockchain é praticamente impossível modificá-la

Bloco Gênese: o primeiro bloco de uma Blockchain

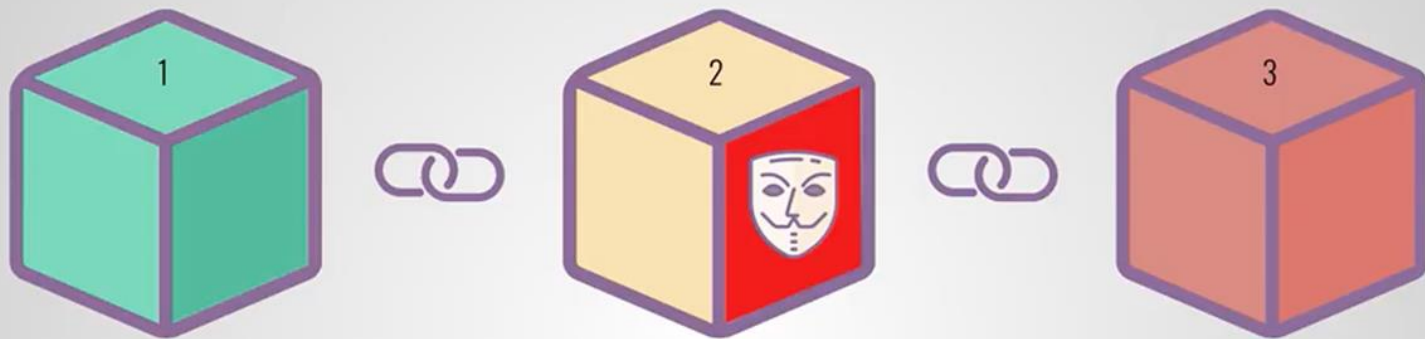


lavid



GT-RAP: Workshop de Transferência de Conhecimento
João Pessoa, 19-20/03/18

Como a cadeia é quebrada, o bloco adulterado não é aceito



Hash: **1Z8F**

Previous hash: **0000**

Hash: ~~6BQ1~~ **H62Y**

Previous hash: **1Z8F**

Hash: **3H4Q**

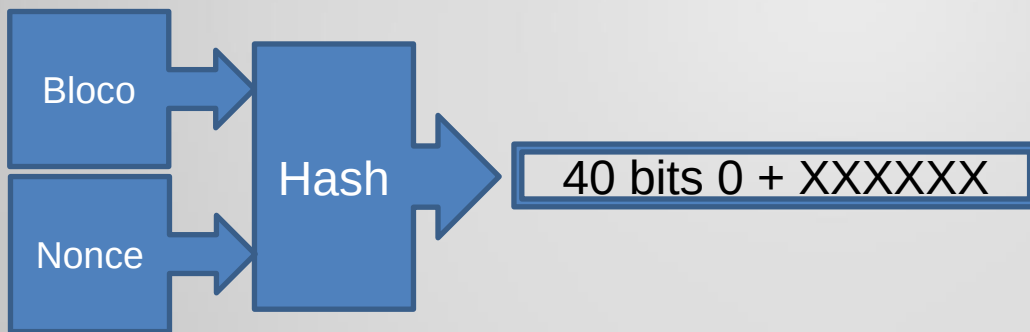
Previous hash: **6BQ1**



lavid

Proof of Work

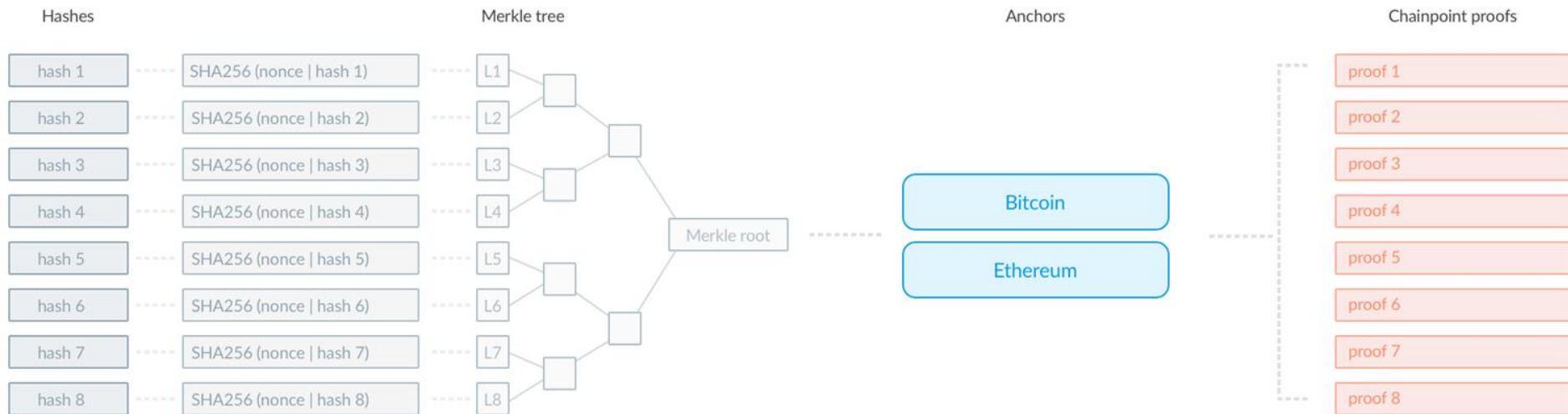
- Calcular um *hash* é trivial
- Desafio: calcular um *hash* abaixo de um limite
- *Nonce*: única variável que o minerador pode manipular para resolver o desafio



Para calcular um hash com 40 zeros são necessárias 2^{40} , aproximadamente 1 trilhão de tentativas.



Otimizando o uso de registros na Block Chain



CONSENSO



Um novo bloco candidato é submetido aos pares da rede

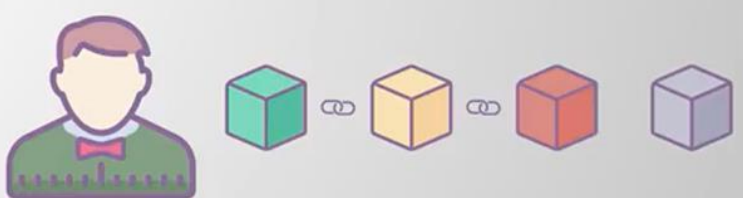
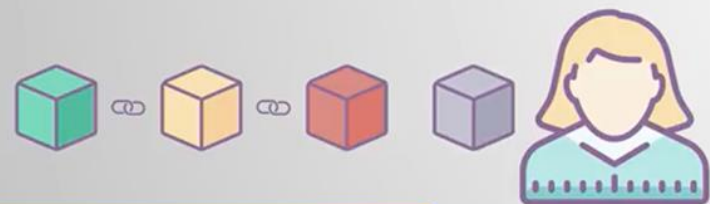
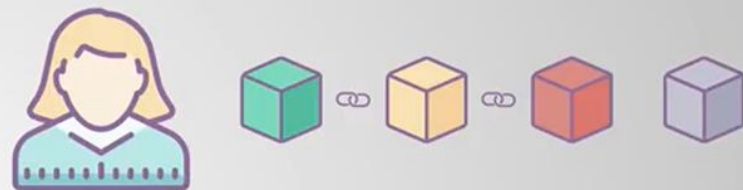
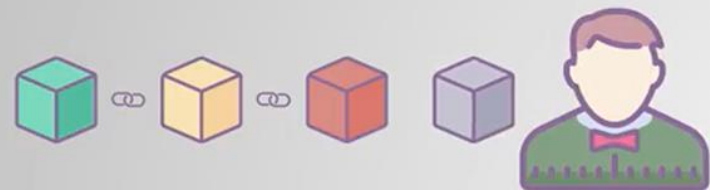


Novo bloco



lavid

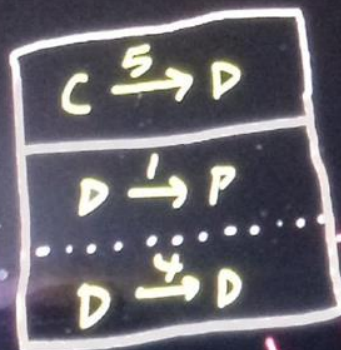
O novo bloco é validado por cada par



honest computing nodes >
 Dan's computing



Dan

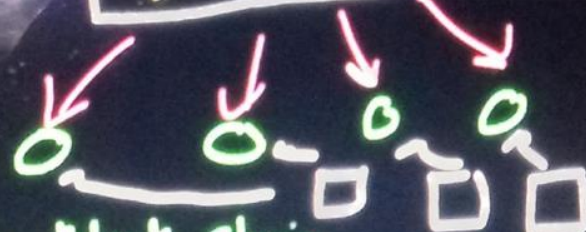


Pete's Pizza

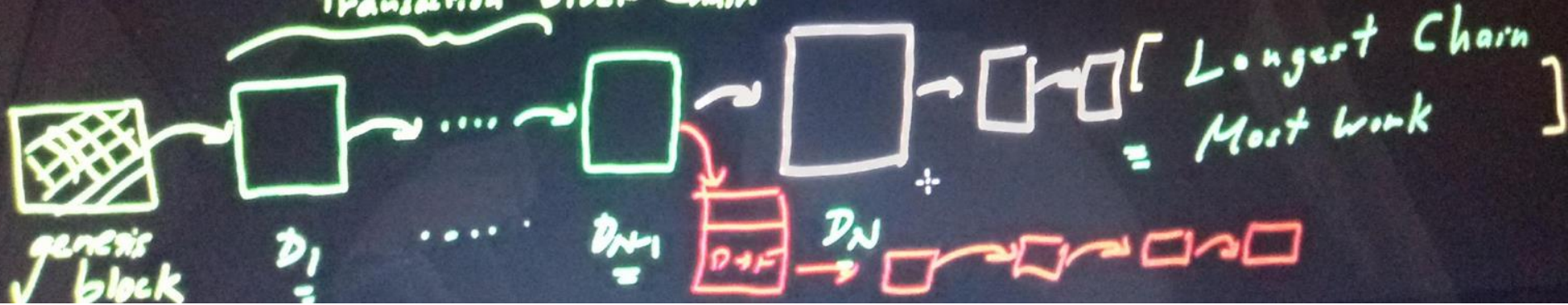


$\leftarrow 1 \text{ } \textcircled{\text{B}}$
 $=$

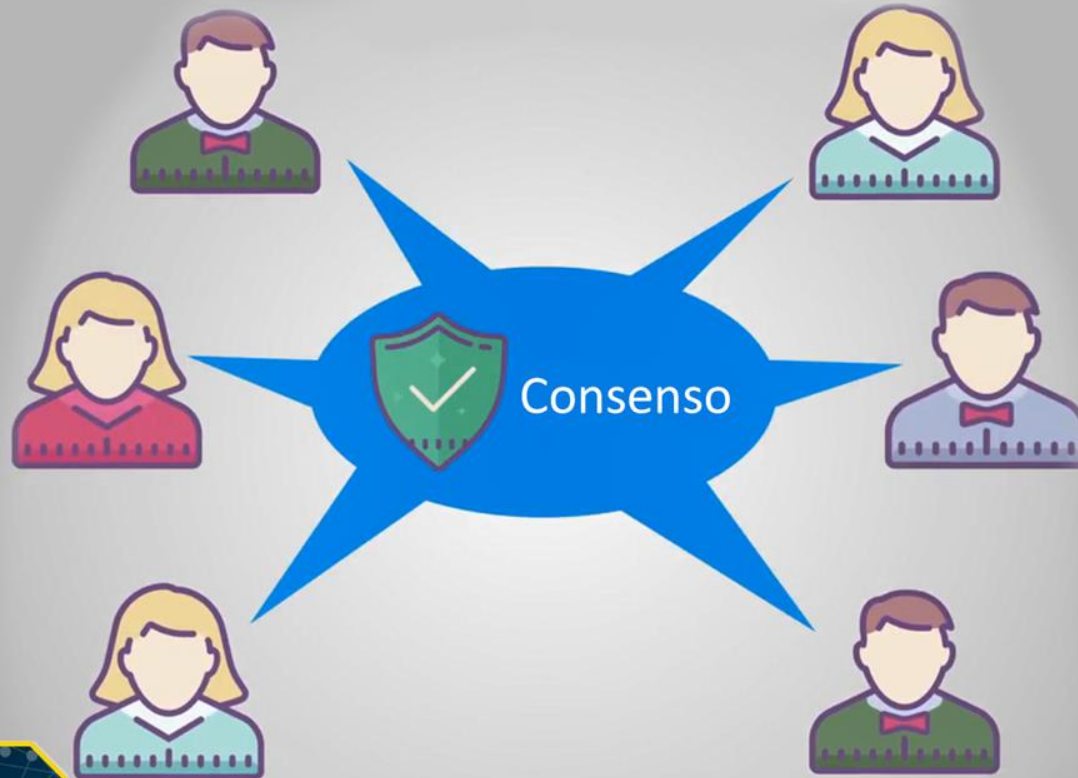
$\text{C} \xrightarrow{5 \text{ } \textcircled{\text{B}}} \text{D}$
 $=$



Transaction Block chain



Consenso: Quando a maioria dos pares valida o novo bloco



lavid



GT-RAP: Workshop de Transferência de Conhecimento
João Pessoa, 19-20/03/18

Contato:
guido@lavid.ufpb.br

Referências:

<https://pt.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-security-of-transaction-block-chains>

https://www.youtube.com/watch?v=SSo_ElWHs4

