

Blockchain e IPFS para registro e autenticidade de certificações

Maurício Witter

Tópicos

- Problema
- Proposta
- Objetivos gerais
 - Objetivos específicos
- Literatura
- Tecnologias

Problema

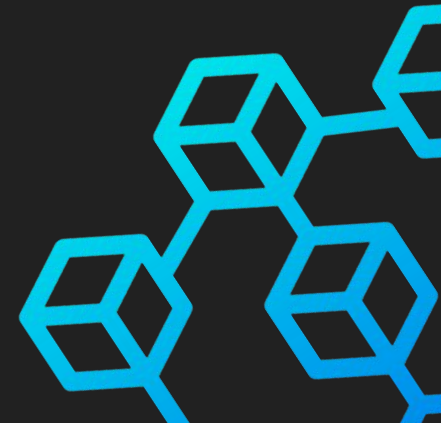
— Sistemas centralizados
apresentam obscuridade
operacional.

- Documentos fraudulentos
- Segurança
- Disponibilidade
- Transparência

Proposta

— A centralização leva à eficiência momentânea, a descentralização promove a robustez a longo prazo.

- Registro
- Armazenamento distribuído
- Consulta
- Autenticidade



Objetivo geral

Desenvolver uma aplicação que use redes Blockchain e armazenamento distribuído.

Objetivos específicos

- Desenvolver Smart Contracts
- Integrar a aplicação com o protocolo IPFS
- Criar uma interface de usuário
- Testar e avaliar a aplicação

Benefícios

- Imutabilidade
- Rastreabilidade
- Armazenamento distribuído
- Descentralização

Implicações

- Entrada de dados falsos
- Privacidade
- Conformidade Regulatória

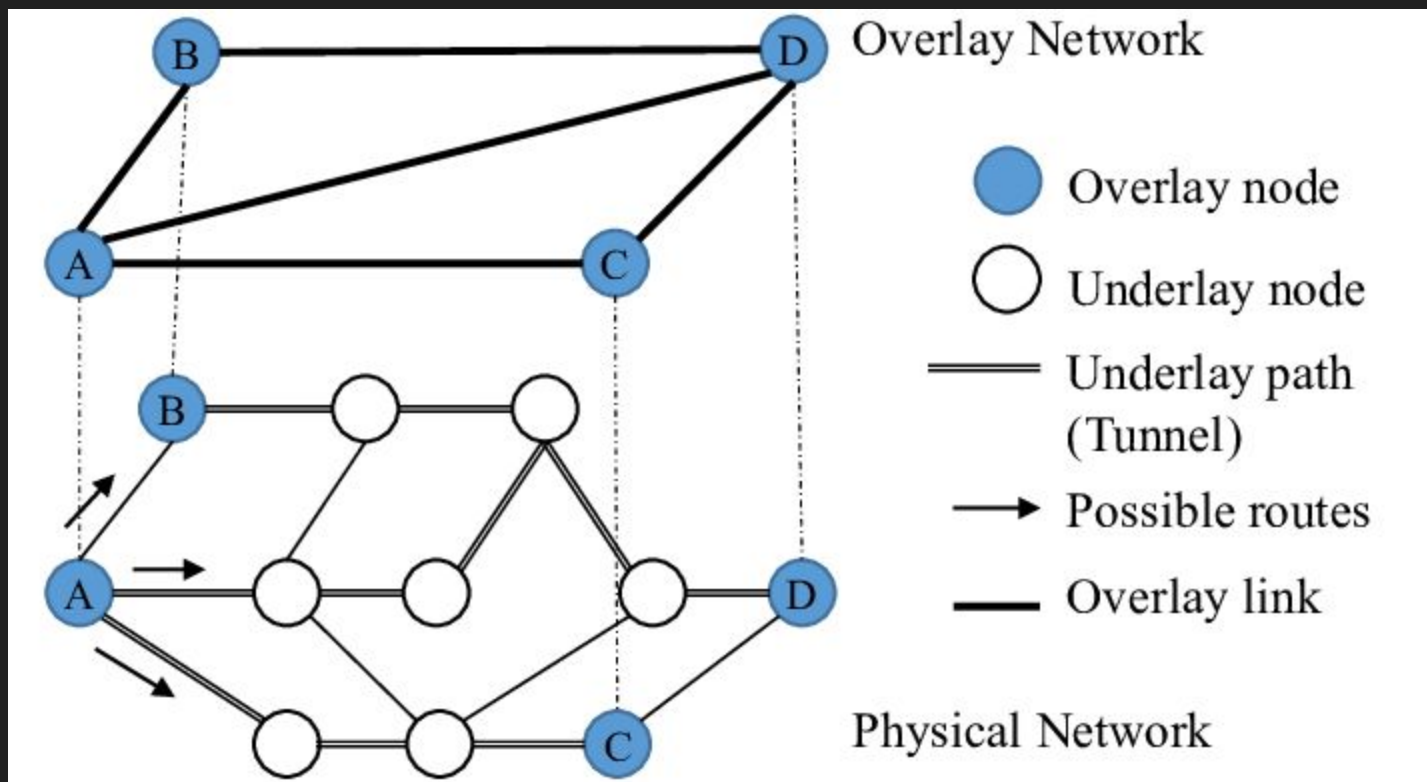
Literatura

- SOUZA B. E., CARNEIRO E., COUTINHO A. Geração e Validação de Diplomas e Certificados utilizando Blockchain (2021).
- BARROSO L. R.. Emissão e validação de diplomas digitais usando a tecnologia Blockchain (2023).
- BCdiploma
- Blockcerts

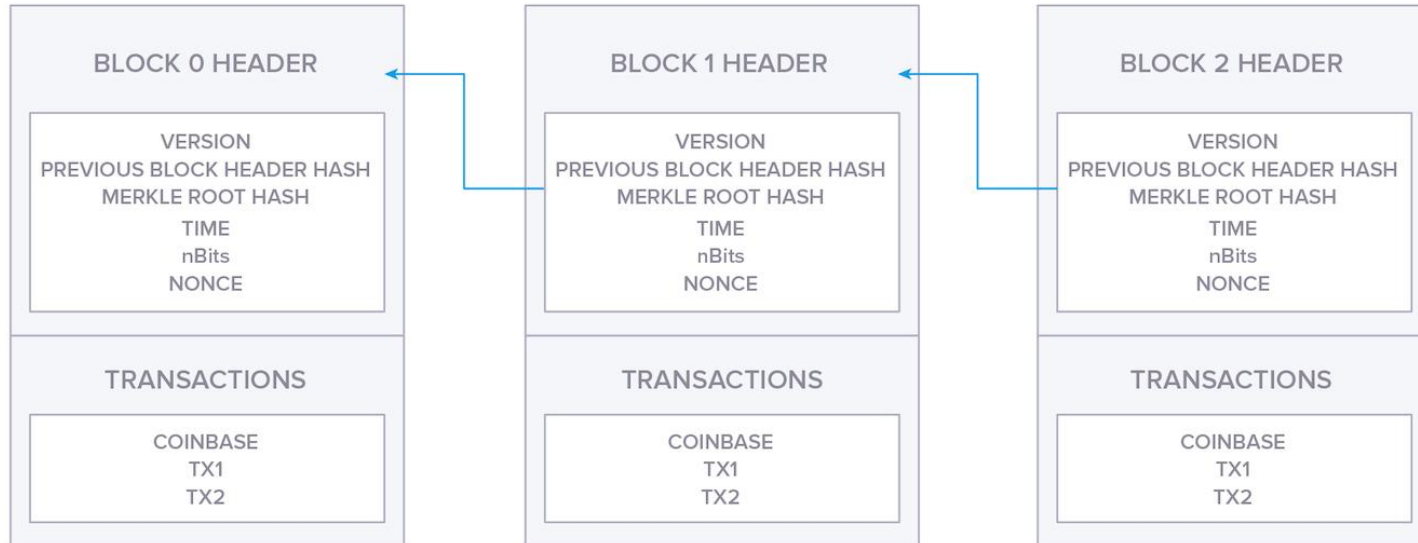
Blockchain

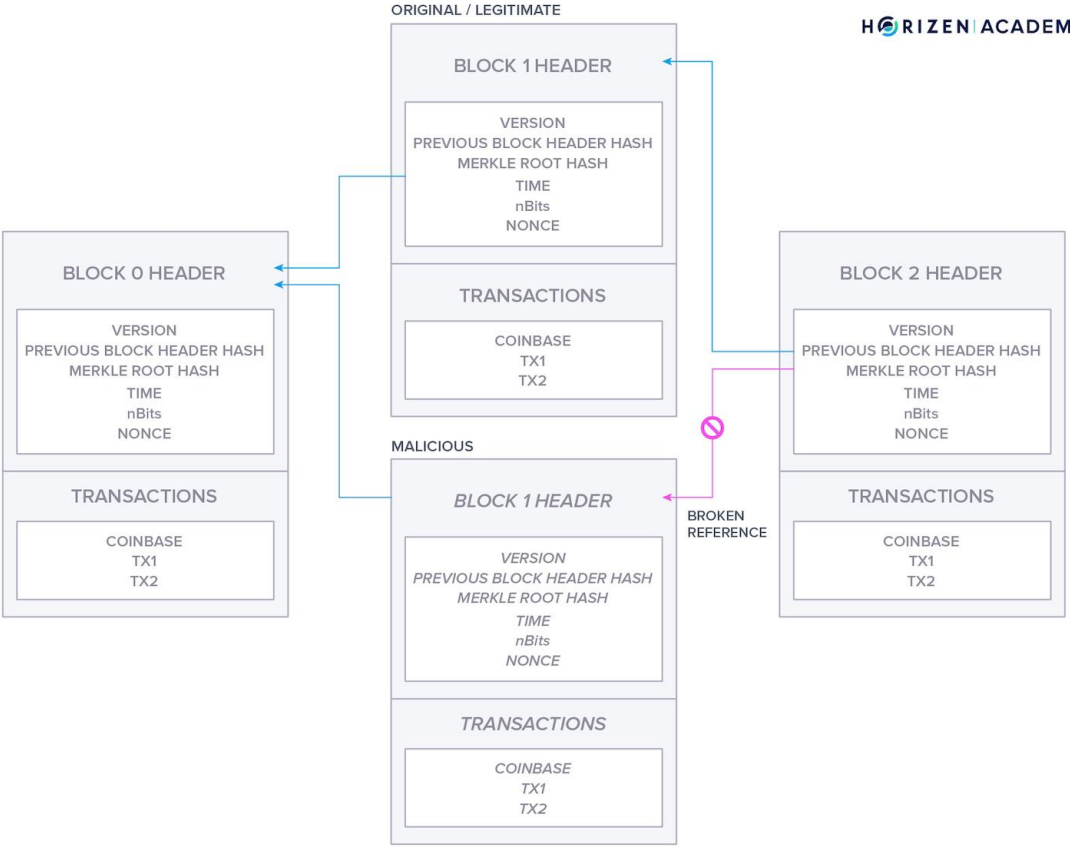
— Consenso baseado em algoritmos redefine a confiabilidade das transações, rompendo com a dependência de autoridades centralizadas.





- Se um processo falha, isso não derruba o sistema.
- Se um processo falha, outros nodes podem recuperar o que for necessário.
- Falhas locais não cascadeiam.
- Recursos operacionais dos nodes da rede.

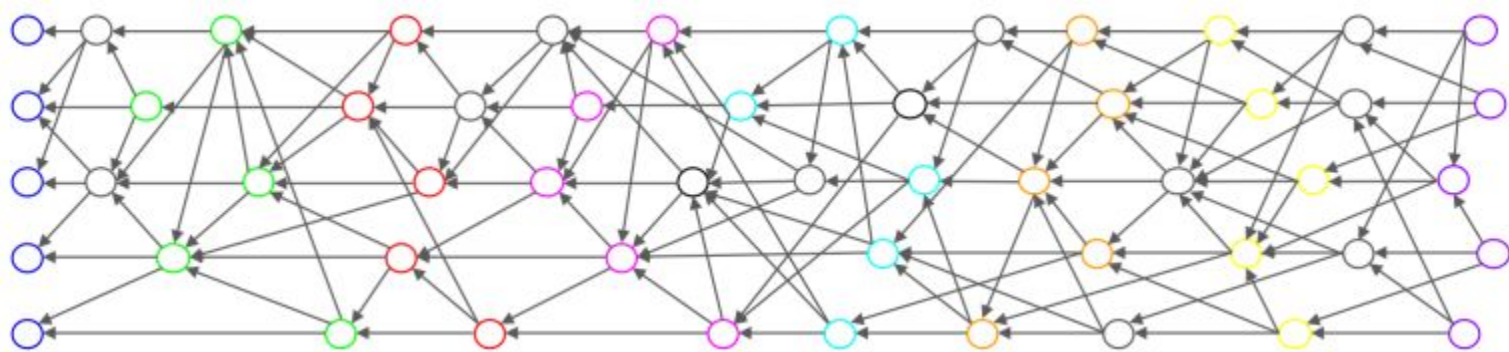
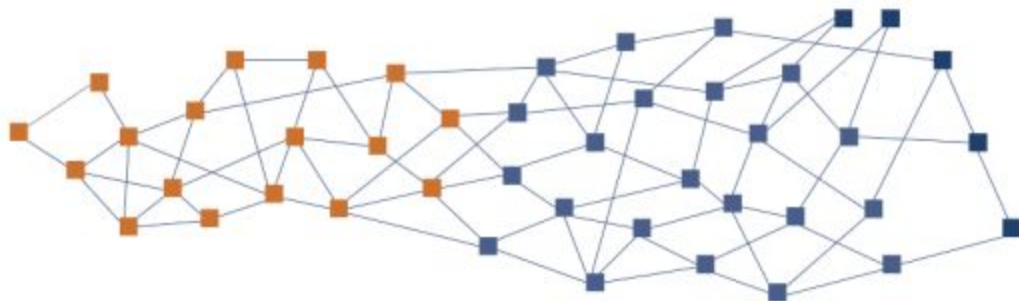




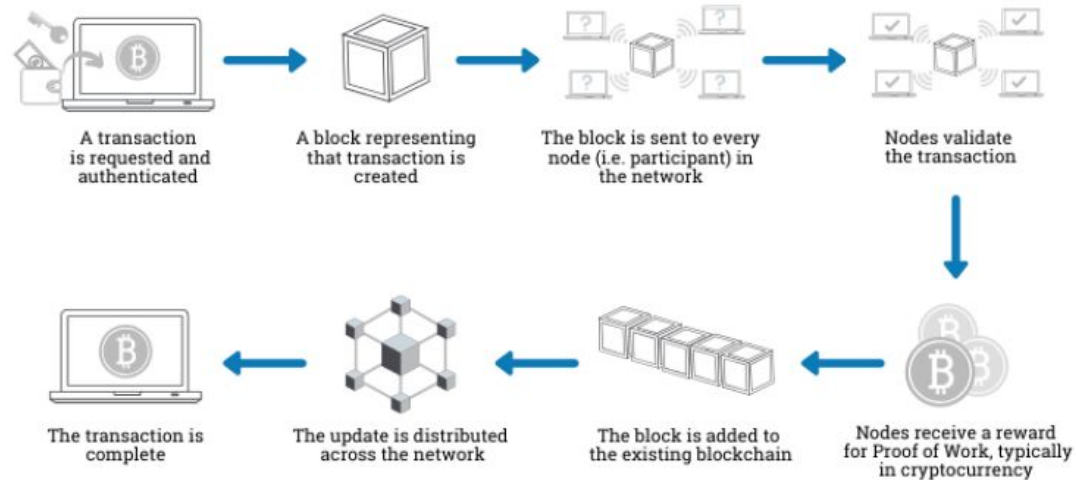
Blockchain



(DAG/Directed Acyclic Graph)



How does a transaction get into the blockchain?

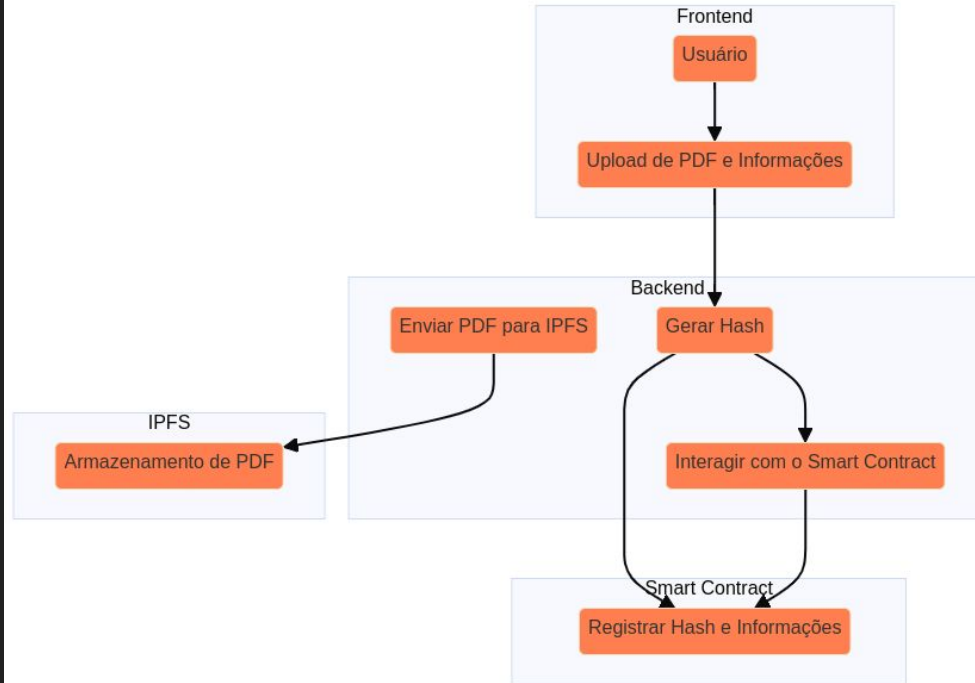


IPFS

— Armazenamento peer-to-peer
baseado endereçamento de conteúdo

- Protocolo P2P
- Identificadores de Conteúdo (CIDs)
- Merkle Directed Acyclic Graphs (MDAG)
- Deduplicação

Fluxo de comunicação



Próximos passos...

- Desenvolver os Smart Contracts
- Deploy na testnet da Fantom
- Criar Frontend
- Consumir os Smart Contracts

Recapitulando

- Instituições registram certificações
- Blockchain fornece a transparência, segurança, disponibilidade e imutabilidade de forma descentralizada.
- IPFS fornece o armazenamento distribuído imutável e descentralizado.

Referências

- CHOI, S. M., PARK, J., NGUYEN, Q., CRONJE, A. FANTOM: A Scalable Framework for Asynchronous Distributed Systems.
- LUU L., CHU H. D, OLICKEL H., SAXENA P., HOBOR A.. Making Smart Contracts Smarter.
- SOUZA, B. E., CARNEIRO E., COUTINHO A.. Geração e Validação de Diplomas e Certificados utilizando Blockchain Público.
- BARROSO L. R.. Emissão e validação de diplomas digitais usando a tecnologia Blockchain.

Dúvidas?

Obrigado!



@rwietter



@rwietter



/in/rwietter

Slides, repositório, proposta e artigo

