

# Blockchain e Smart Contracts na Preservação da Evidência Digital

Rumo a uma Cadeia de Custódia Imutável e Auditável

Projeto Final de Curso: Segurança da Informação e Forense Digital

Autores: Gabriel Canaan, João Citino, João Gabriel, Mateus Porto





# O Problema da Confiabilidade da Evidência Digital

1

## Fragilidade da Evidência Digital

A evidência digital (ED) é vital em investigações, mas inherentemente frágil. Pequenas alterações podem invalidar seu valor probatório.

2

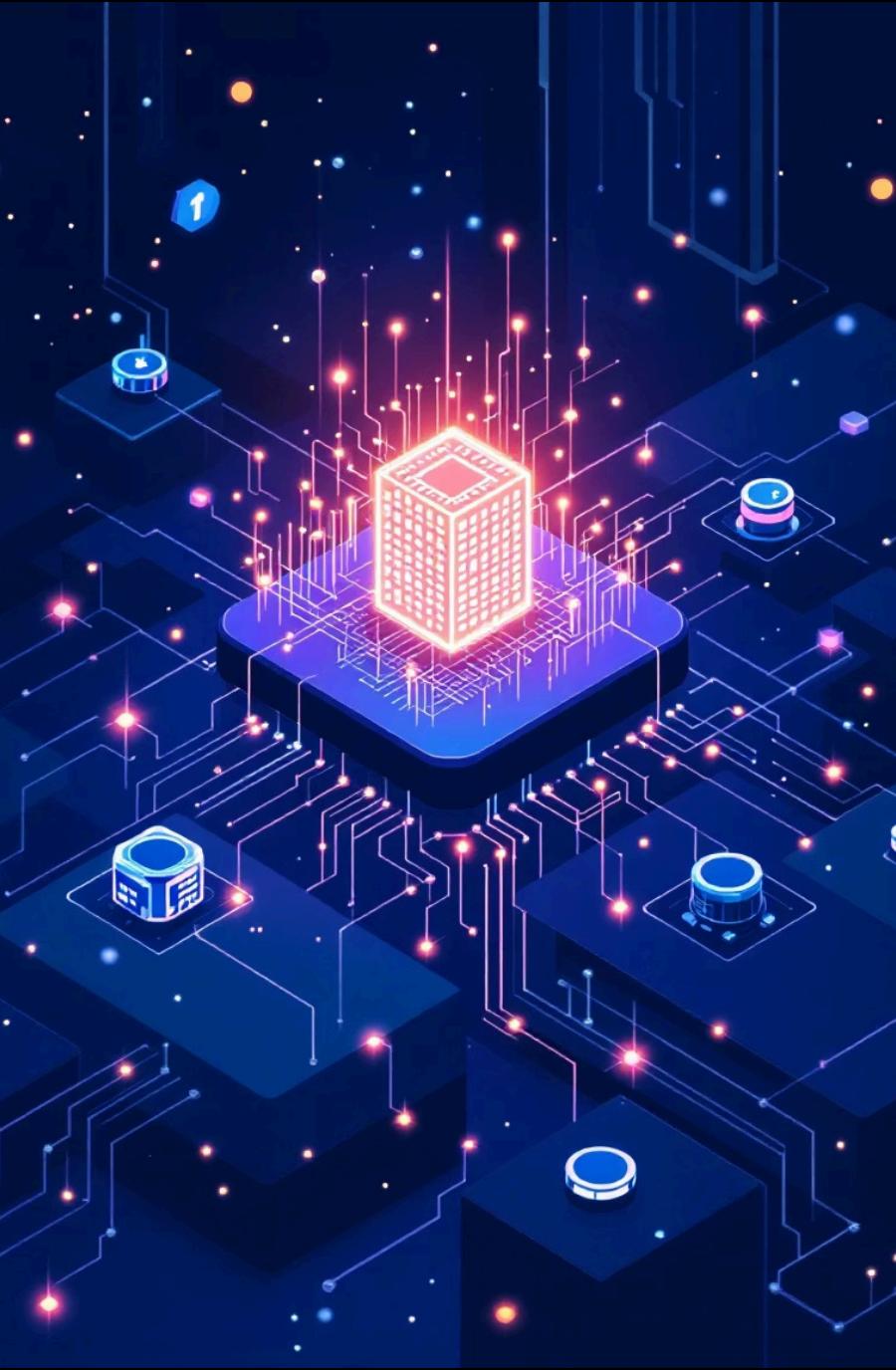
## Cadeia de Custódia Tradicional

A CoC tradicional, baseada em registros em papel e confiança humana, representa o elo mais fraco nas investigações digitais.

3

## Impacto Jurídico

A quebra da CoC compromete a admissibilidade da prova em juízo, levando a falhas na justiça e impunidade.



# Blockchain como Solução para a Confiança



## Protocolo de Confiança

Blockchain (DLT) surge como um "protocolo de confiança", oferecendo um registro distribuído e criptograficamente imutável.



## Confiança na Tecnologia

A confiança migra do agente humano para a robustez da tecnologia, fundamentada em criptografia e consenso distribuído.



## Presunção de Autenticidade

O registro em DLT confere presunção de autenticidade, integridade e tempestividade aos dados probatórios.

# Digital Evidence Management System: Arquitetura Híbrida

Nossa solução proposta, o "Digital Evidence Management System", emprega uma arquitetura híbrida para otimizar privacidade e escalabilidade.



## Blockchain (On-chain)

Armazena apenas o hash (bytes32) da evidência e seu CID (Content Identifier) do IPFS.



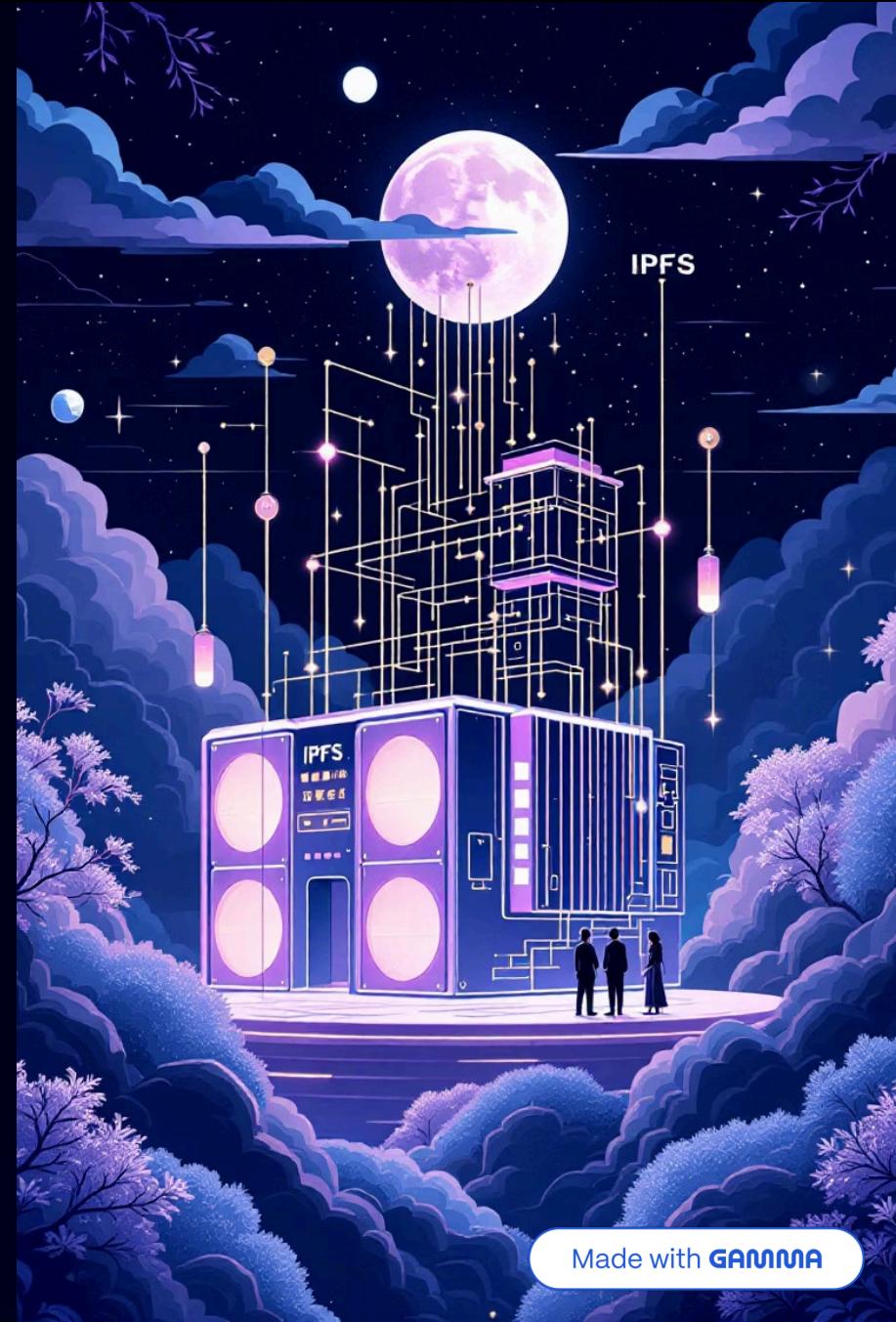
## Evidência Digital (Off-chain)

O arquivo bruto da evidência é armazenado de forma descentralizada no IPFS (InterPlanetary File System).



## Garantia de Integridade

Qualquer alteração no arquivo no IPFS será detectada, pois o hash calculado não corresponderá ao hash registrado no blockchain.



# Smart Contracts: Gestão Automatizada da Custódia

Os Smart Contracts são o coração da automação da Cadeia de Custódia, garantindo rastreabilidade e conformidade processual.

## Códigos Autoexecutáveis

Automatizam a Cadeia de Custódia sem intermediários, seguindo regras pré-definidas.



## Rastreabilidade Imutável

Cada transferência de posse é registrada no array `custody_history`, incluindo agente, razão e data/hora.

## Controle de Estados (FSM)

O Smart Contract usa um Status Enum para gerenciar o fluxo da evidência (ex: `Collected` -> `InAnalysis` -> `Archived`).

# Controle de Acesso Baseado em Papéis (RBAC)

Para atender aos requisitos forenses, implementamos um controle de acesso rígido, baseado em papéis, garantindo que apenas agentes autorizados interajam com a evidência.

- **Implementação:** O RBAC é detalhado utilizando roles (bitmap) e modifiers (ex: `_only_role`) para definir permissões.
- **Segurança:** Garante que apenas agentes autorizados possam interagir com o registro da custódia, prevenindo acessos indevidos.



## ROLE\_POLICE

Registro inicial (`register_evidence`).



## ROLE\_LAB

Análise e adição de relatórios (`add_file_to_evidence`).



## ROLE\_JUDGE

Alteração de status final.



# Vantagens Chave da Solução



## Validade Probatória

Reforça a admissibilidade legal da evidência, com um registro imutável que confere uma camada superior de autenticidade.



## Eficiência Operacional

A automação da documentação da CoC via Smart Contracts reduz tempo e custos de auditoria, otimizando processos investigativos.



## Segurança Aprimorada

Redução drástica de fraudes e proteção criptográfica robusta contra qualquer forma de adulteração da evidência digital.

# Desafio Crítico I: O Oracle Problem

A imutabilidade do blockchain garante o registro, mas não a veracidade do evento subjacente.

- **Risco:** O ponto de falha migra para a aquisição da prova (off-chain) e a manipulação do Oráculo que alimenta o Smart Contract com o hash inicial.
- **Conclusão:** Esforços de pesquisa devem focar na proteção do hardware de aquisição da evidência, ponto crítico para a integridade inicial.



# Desafio Crítico II: Regulamentação e Privacidade



## Imutabilidade vs. Direito ao Esquecimento

A natureza imutável do Blockchain pode colidir com regulamentações como LGPD/GDPR, que preveem o direito à exclusão de dados.

### Nossa Mitigação:

Separamos dados brutos (IPFS) do registro (Blockchain), garantindo privacidade sem comprometer a integridade da CoC.

## Avanço Futuro: Zero-Knowledge Proofs (ZKP)

Necessidade de ZKP para provar a integridade do hash sem expor dados sensíveis, conciliando transparência forense e privacidade.

# Conclusão e Próximos Passos

O "Digital Evidence Management System" é uma solução robusta para a gestão da Cadeia de Custódia da evidência digital.

## Síntese da Solução

Atende aos requisitos forenses (RBAC, FSM, Imutabilidade) em DLT permissionada.

## Próximos Passos (Estratégicos)

Promover a padronização de Smart Contracts de CoC.  
Implementar em redes de Consórcio validadas por terceiros independentes.

