

Blockchain e Smart Contracts e gerenciamento de Digital Evidence em Cadeias de Custódia

Projeto Final: Digital Evidence

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



Made with GAMMA



A Fragilidade da Evidência Digital e o Risco de Manipulação

1

Fragilidade e Suscetibilidade à Manipulação

A evidência digital (ED) é, por natureza, **extremamente frágil e suscetível à manipulação**. Sua autenticidade e integridade podem ser comprometidas por alterações mínimas, tornando-a um desafio crucial em investigações.

2

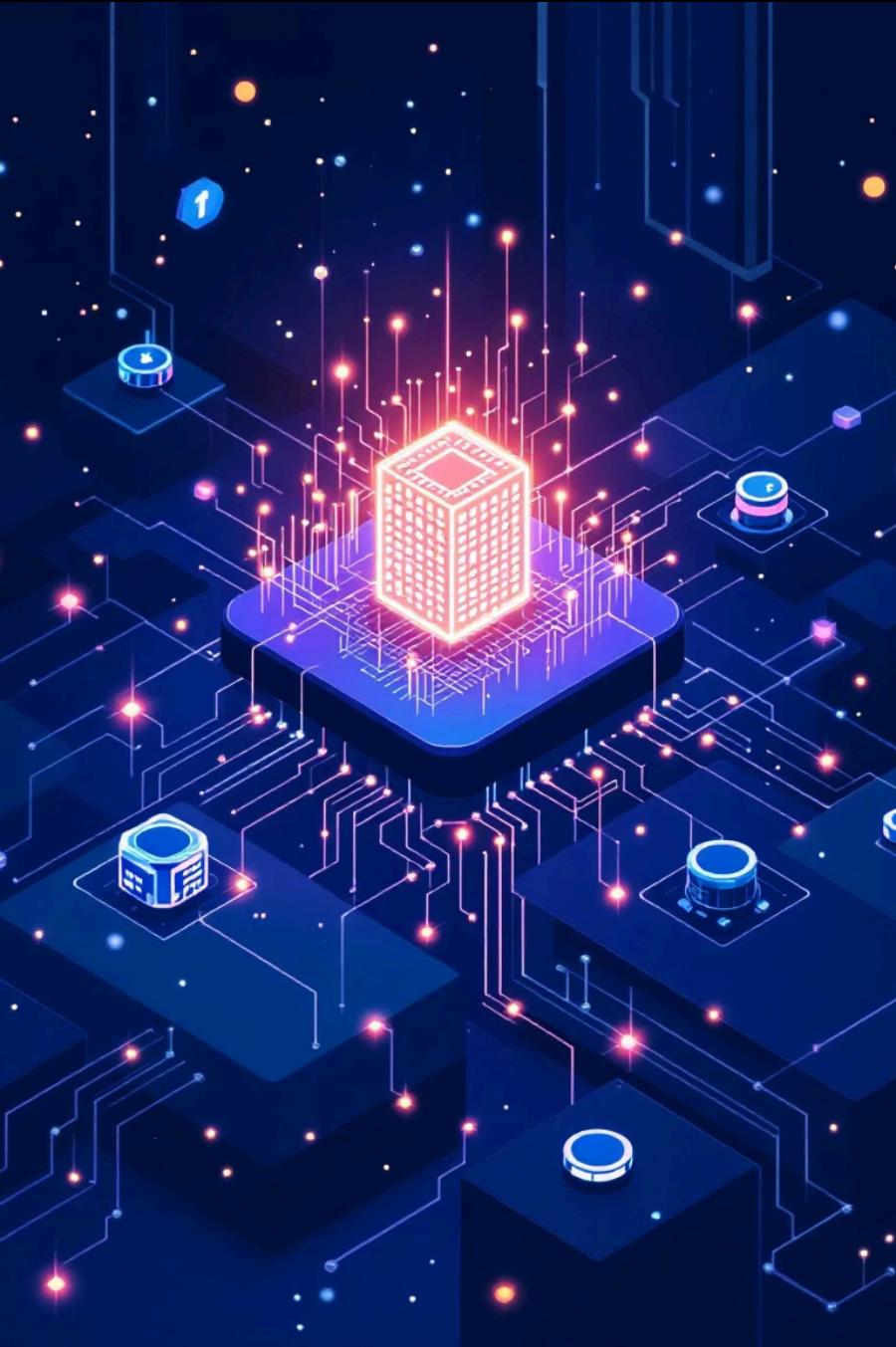
Mecanismos de Manipulação da ED

A **manipulação da evidência digital** pode ocorrer de diversas formas, incluindo a alteração de metadados, a modificação do conteúdo dos arquivos, a exclusão de dados ou a criação de informações falsas, muitas vezes sem deixar rastros evidentes para métodos tradicionais.

3

Consequências Jurídicas da Fragilidade

A ausência de mecanismos robustos para garantir a integridade da ED e evitar sua manipulação resulta em **graves consequências jurídicas**. Provas comprometidas perdem seu valor probatório, levando à inadmissibilidade em juízo, falhas na justiça e à impunidade de criminosos.



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.

Análise de Custo-Benefício da Implementação



Custos Administrativos Reduzidos

A automação dos processos de cadeia de custódia via Smart Contracts elimina tarefas manuais, reduzindo significativamente a necessidade de intervenção humana e, consequentemente, os custos operacionais e administrativos.



Custos Iniciais Elevados

A implementação inicial exige investimento substancial em desenvolvimento de software, integração com sistemas existentes e aquisição de infraestrutura tecnológica, além da contratação de especialistas.



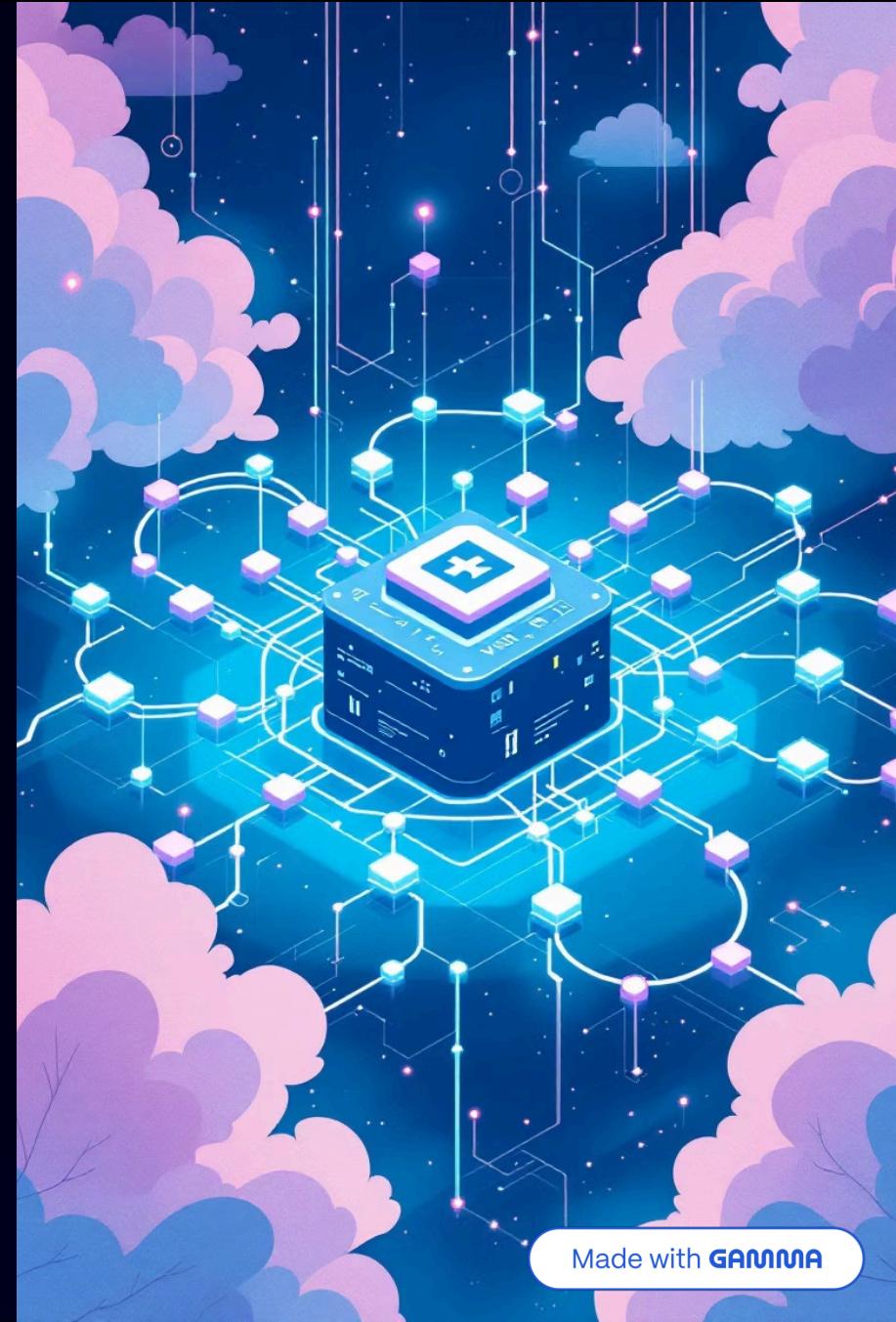
Produtividade: Curto vs. Longo Prazo

Inicialmente, a curva de aprendizado das equipes pode resultar em uma queda temporária da produtividade. No entanto, a longo prazo, os ganhos em eficiência e agilidade processual compensam amplamente, otimizando fluxos de trabalho e liberando recursos.

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.

Conclusão e Próximos Passos

Nosso "Digital Evidence Management System" é uma solução eficaz para organizar e proteger provas digitais.

O que a Solução Faz

Ela cumpre as exigências da investigação forense (como RBAC, FSM, Imutabilidade) usando uma tecnologia blockchain controlada.

Próximos Passos Importantes

Vamos trabalhar para padronizar os contratos inteligentes (Smart Contracts) da Cadeia de Custódia. E aplicar a solução em redes de Consórcio que são verificadas por parceiros independentes.

