Info DApp

Iuri Teles

Problema/Motivação

- Perda ou mudança em informações necessárias para recuperação ou autenticação de sessões.
- Obs: Comumente informações pessoais.
- Exemplos:
  - Número de telefone celular (Whatsapp, Telegram , etc.)
  - E-mail secundário para recuperação de acesso.
  - Pergunta e resposta para recuperação de acesso.

Opção por Blockchain

- Vantagens:
  - Não necessita de API (Basta acessar o contrato). *
  - Consulta dos dados sem custo de transação. *
- Desvantagens:
  - Custo para atualizar as informações e disponibilizá-las para o serviço. *
  - Dependência externa de interface para compreensão e gravação dos dados.

Implicações

- Como prover informações privadas em um meio público de maneira segura?
- Como prover apenas as informações necessárias para cada serviço?
- Como garantir que um serviço não tenha acesso a informações providas a outros?

Solução

- Implementação de um smart contract com as seguintes características:

    - Todos dados cifrados por RSA *
    - Armazena informações privadas (opcional)
    - Disponibiliza apenas as informações necessárias para o serviço por meio de sua respectiva chave pública.

Aplicação e Código Fonte

Extrapolação da solução

- A solução desenvolvida pode ser extrapolada de maneira a resolver outros problemas ou ajudar em áreas:

    - Identidade Digital
    - LGPD sobre questões de:
        - Finalidade
        - Necessidade
        - Anonimização e pseudoanonimização *

Trabalhos futuros

- Melhorar interação com os serviços, permitindo que o próprio serviço faça a requisição direta ao contrato, registrando a finalidade dos dados requisitados, período de uso, etc.

- Definição de padrão para ABI deste tipo de contrato, estabelecendo tanto padrão de chamada, quanto padrão para chave de informações (tipos de informações fornecidas).

Dúvidas?