ZK Smart NFC by TrustChain

TrustChain is a company that aims to provide secure and efficient solutions for anti-counterfeiting, document security, and off-chain payments using blockchain technology. TrustChain's flagship product, ZK Smart NFC, uses secure NFC technology combined with the Mina Protocol blockchain to provide an innovative and secure solution for a range of use cases.

Github

Problem

Counterfeiting is a major problem in many industries, including fashion, food and beverage, and electronics. Counterfeit goods not only result in lost revenue for legitimate businesses but can also be dangerous for consumers. Document fraud is also a problem, with fake IDs and other documents being used for identity theft and other illegal activities. Traditional payment methods can also be slow and expensive, with high transaction fees and long processing times.

Solution

TrustChain's ZK Smart NFC technology provides a secure and efficient solution to these problems. By combining NFC technology with the Mina Protocol blockchain, TrustChain can provide a secure and immutable ledger of data that can be easily accessed and verified. The NFC chip is embedded with a secure chip that stores the private key, making it impossible for the private key to be accessed. The NFC data is encoded during setup, and the hash data is saved in the leaf of the NFC Merkle Tree. The root hash of the Merkle Tree is saved in the smart contract.

Architecture

Smart NFC TrustChain's ZK Smart NFC technology works by encoding NFC data during setup, which is then saved in the leaf of the NFC Merkle Tree. The root hash of the Merkle Tree is saved in the smart contract, which can be easily accessed and verified. For each scan, a new hash is generated by [tagId, publicKey, scan counter], ensuring that each scan is unique and verifiable.

Step 1. Encode The first step in using TrustChain's ZK Smart NFC technology is to scan an empty NFC by the Trusted Service Manager. This can be done by clothing and fashion brands, food and beverage factories, or any other company that wants to ensure the authenticity of their products.

Metadata, including the URL and zkApp private key, is then saved on the NFC chip.

Step 2. Save hashes of NFC's on Merkle Tree The next step is to save the hashes of the NFCs on the Merkle Tree. This is done by the Trusted Service Manager

and ensures that each NFC is unique and verifiable.

Step 3. Deloy Smart Contract on Mina Protocol and saved NFC root hash of the NFC's on Merkle Tree The next step is to deploy the smart contract on the Mina Protocol and save the NFC root hash of the NFCs on the Merkle Tree. This creates an immutable ledger of data that can be easily accessed and verified.

Step 4. Scan and verify The final step is to scan the NFC and verify its authenticity. This can be done using a simple smartphone app that can easily access the NFC data and compare it to the hash stored on the Merkle Tree.

Market

The global anti-counterfeit packaging market size was accounted at **USD 140.27 billion** in 2022 and it is expected to reach around **USD 472.08 billion** by 2032.

Anti-Counterfeit Clothing & Fasion

TrustChain's ZK Smart NFC technology can be used to provide secure and efficient solutions for anti-counterfeiting in the clothing and fashion industry. Smart NFCs can be embedded in clothing, shoes, and other fashion products, ensuring that each product is unique and verifiable.

Document security

TrustChain's ZK Smart NFC technology can also be used to provide secure solutions for document security. Smart NFCs can be used for identity cards, key passes for building access, and other official sign documents, ensuring that each document is unique and verifiable.

MinaCash/ Custom token Cash NFC

TrustChain's ZK Smart NFC technology can also be used for off-chain physical payments without transaction costs. This can be used as a payment method during events, as a gift card, or as a marketing product physical airdrop.

Use Cases: - Offchain physical payment without transaction cost - Payment method during events - Payment method as gifcard - Marketing product physical airdrop

Products: - Mina / Custom token on Smart NFC physical coin - Mina / Custom token on Smart NFC bracelet - Mina / Custom token on Smart NFC ring - Mina / Custom token on Smart NFC giftcard - Mina / Custom token on Smart NFC business card

Smart contract interface:

```
type IMinaCash = {
  updatecommittedNfcRoot(newcommittedNfcRoot: Field): Bool; // emits "NfcRootUpdated" event
```

```
  updateTrustedServiceManager(newTrustedServiceManager: PublicKey): Bool; // emits TrustedSe
  withdraw(to: PublicKey, amount: UInt64): Bool; // emits "Withdraw" event
  // events
  events: {
    NfcRootUpdated: ProvablePure<{
      oldRoot: Field;
      newRoot: Field;
    }>;
    TrustedServiceManagerRootUpdated: ProvablePure<{
      oldRoot: Field;
      newRoot: Field;
    }>;
    Withdraw: ProvablePure<{
      from: PublicKey;
      to: PublicKey;
      amount: UInt64;
    }>;
  };
};
```

Standard budget $50,000

Branding & Design $5,000 Website $5000 Encoding Mobile App for TrustedServiceManager $10,000 Scan & Verify Mobile App $10,000 Backend NFC tag management $10,000 Backend Whitelabel API for Brands/Factory $10,000

Advanced budget $80,000

Marketing - Organize Events $10,000 - Production Mina Cash Smart NFC for Offchain Airdrop $20,000

Team

Als Albrick - Owner Irman - Co-Owner Trustchain dev (anonymous) - Freelancer