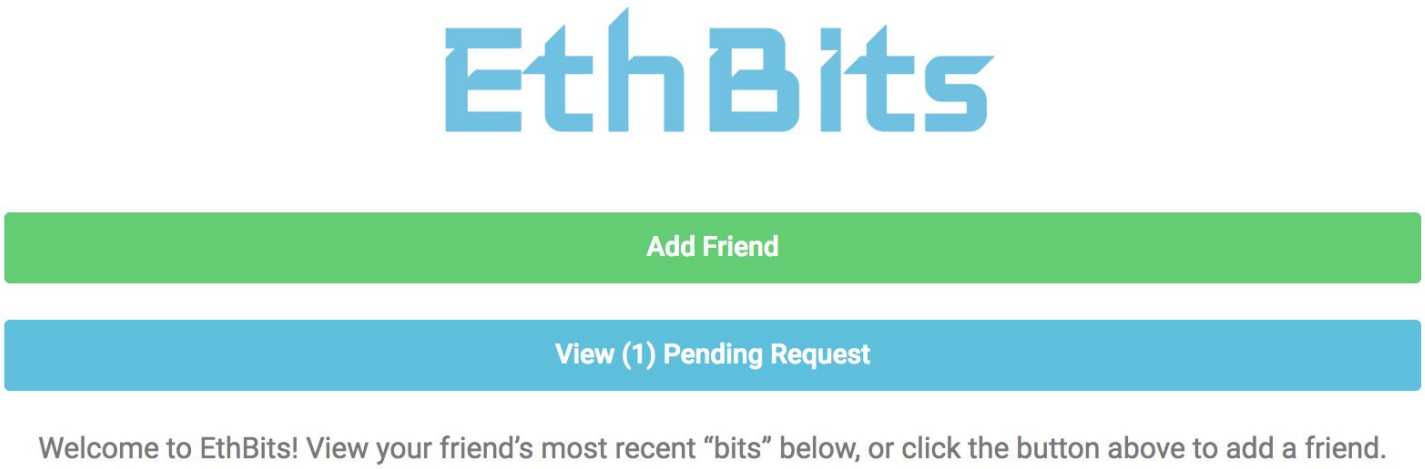
EthBits

A decentralized social networking platform made on the ethereum blockchain.

Caitlin Bahari
Caleb Ditchfield
Linda Ge
John Tam

NYC Blockchain Hack | March 31, 2018

Censorship resistance & privacy



What is EthBits?

A decentralized social network which aims to maintain 100% privacy for those who want it.

- It’s a mix of Facebook and twitter
- It’s built in Solidity
- It allows posting, commenting
  - Publicly (to anyone that wants to see your posts)
  - Privately (to friends only)

Contracts

Two smart contracts built in Solidity:

1. EthBitAccount(s): stores user data - one per user account
    - Friends list
    - Follow list
    - Public “bits”
    - Private “bits”
    - Created when a user first uses EthBits

2. EthBitRegistry: stores lookup information for address → name (and vice versa)
    - Allows “registering” of usernames (and prevents duplicate username registrations)
    - Enables username lookups instead of relying on addresses

Technical Overview

Privacy is a big concern . That's why we allow both public posts (anyone can see) and private posts (only your friends can see).

- Public posts: stored as unencrypted plaintext in a "publicBits" mapping
- Private posts: encrypted with a "friends-only" password in a "privateBits" mapping

Secure Private Posting via Public Key Cryptography

- Private posts are encrypted with a “friend password” (symmetric-encryption)
- This password is encrypted with the user’s public key and stored in the user’s profile
- When adding a friend, the user retrieves and decrypts his password
- The user then *re-encrypts* the password with the *friend’s public key*, and sends this newly-encrypted password via the blockchain to the friend’s account
- The friend then decrypts the password with their own private key - the friend now has the plaintext password
- The friend retrieves the original user’s *encrypted* posts and *decrypts* them with the newly acquired password

Quick Demo

Challenges

- Difficult to retrieve public key from ethereum address
- Metamask and most other Web3 providers do not provide a way to decrypt a message signed with your public key - you have to provide this manually
  - (but this is an incoming feature, hopefully!)
- Password “leaks”
  - This could be mitigated by a different encryption schema

Future

- Commenting on posts
- Sending money or ERC20 tokens to friends
- More than two layers of security
- Encryption of ALL non-public data:
  - Number of private posts
  - Number of friends & friend list

Contact

CONTACT

Caitlin Bahari | @cbahari
Caleb Ditchfield | ditchfieldcaleb@gmail.com
Linda Ge | @linda-ge
John Tam | john.tam@aya.yale.edu