

Introduction To Digital Identity

...

Alex Melville

5F11 78CD D43A 49E9 10D6 D27C 773A E36E 3704 569C

Intro

Current Digital Identities

PGP

Cryptography Basics

Blockchain Identity

Let's Make Some Keys

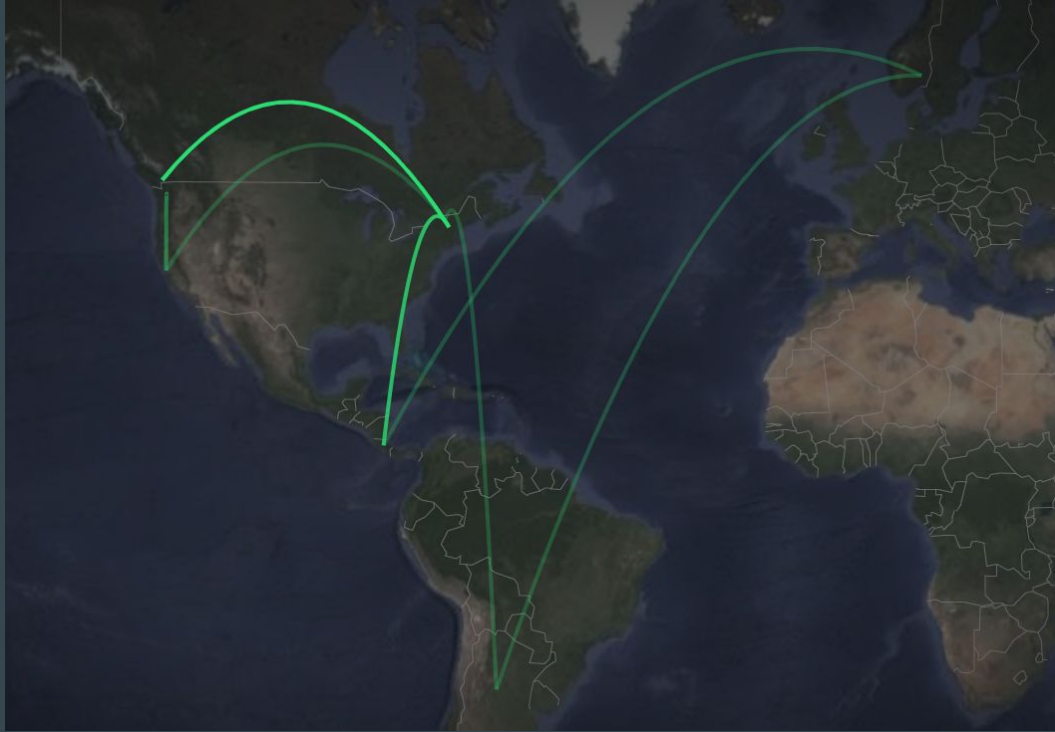


Alex Melville

Software Engineer

@ BitGo

github.com/Melvillian



Alex Melville

Digital Nomad

Audience Poll!

What is identity?

Audience Poll!

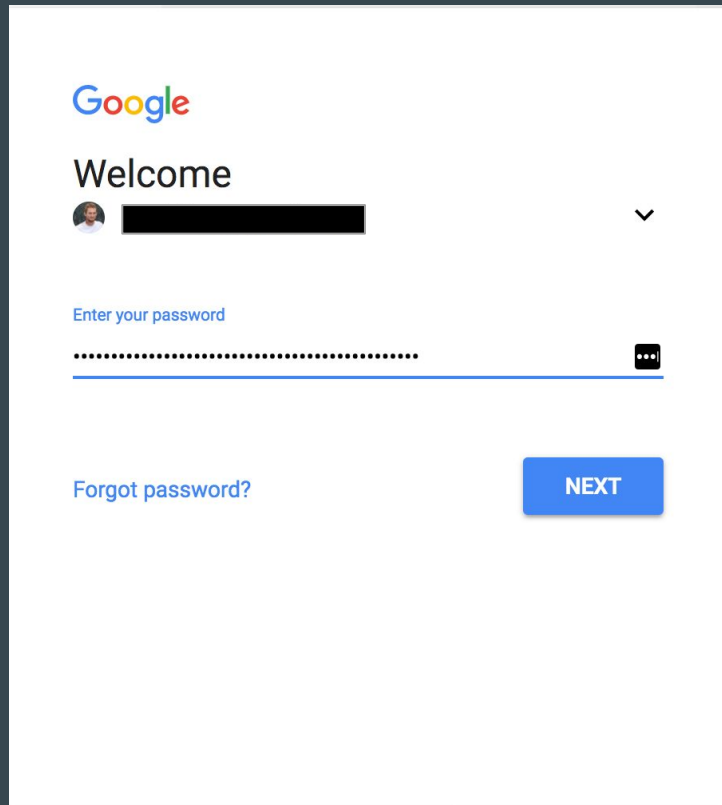
What is identity?

Something you know, something you have,
something you are

Commonly Used Digital Identities

Web Accounts

- 200+ accounts
- Lightweight
- Non-transferable



A screenshot of a Google account login page. At the top is the Google logo. Below it, the word "Welcome" is displayed next to a profile picture icon and a blacked-out name. A small downward arrow is to the right of the name. Below this is a password prompt "Enter your password" followed by a password input field with a blue underline and a black eye icon on the right. At the bottom left is a link "Forgot password?" and at the bottom right is a blue button labeled "NEXT".

Commonly Used Digital Identities

Web Accounts

- 200+ accounts
- Lightweight
- Non-transferable
- Need a Password Manager



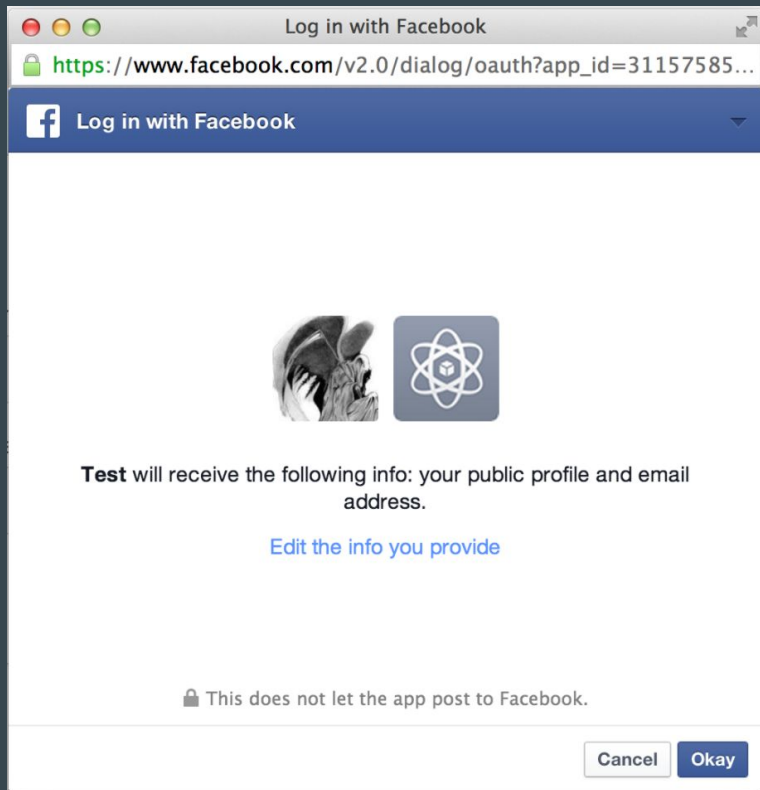
1Password



Commonly Used Digital Identities

OAuth

- Facebook
- Twitter
- Google
- Username + Password (+ 2FA)



Commonly Used Digital Identities

Social Insurance
Numbers :(

- Identification AND
Authentication



PGP (Pretty Good Privacy)

“PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.”

-Wikipedia

PGP (Pretty Good Privacy)

Created by Phil Zimmermann in 1991



By PRZ_closeup.jpg: User Matt Crypto on en.wikipediaderivative work: Beao - PRZ_closeup.jpg, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=9009023>

Created by Phil Zimmermann in 1991

PGP (Pretty Good Privacy)



By PRZ_closeup.jpg: User Matt Crypto on en.wikipediaderivative work: Beao - PRZ_closeup.jpg, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=9009023>

PGP (Pretty Good Privacy)

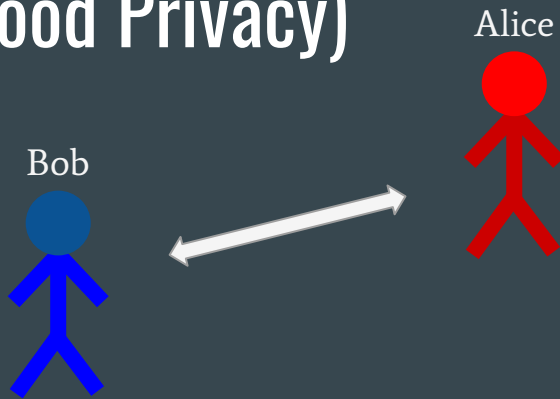
1. Decentralized Web of Trust
2. Public/Private Key Cryptography

PGP (Pretty Good Privacy)

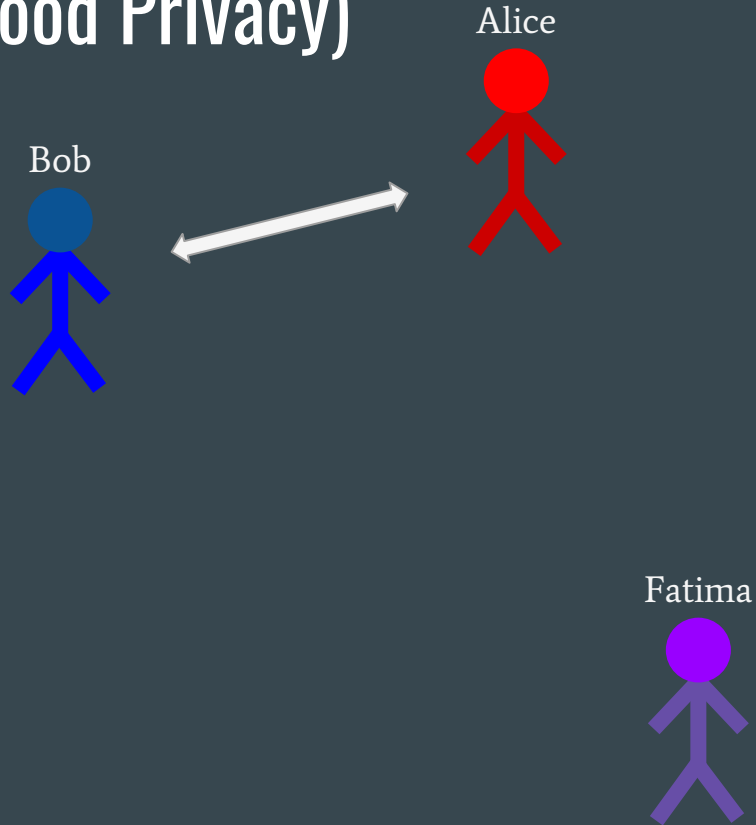
Bob



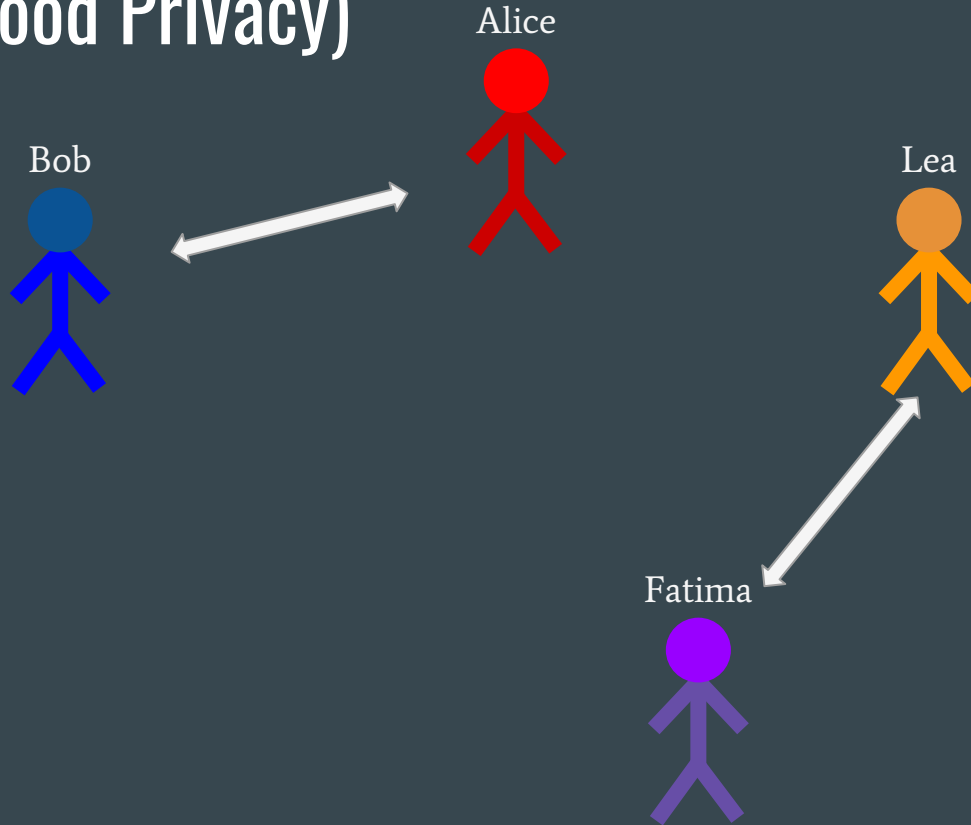
PGP (Pretty Good Privacy)



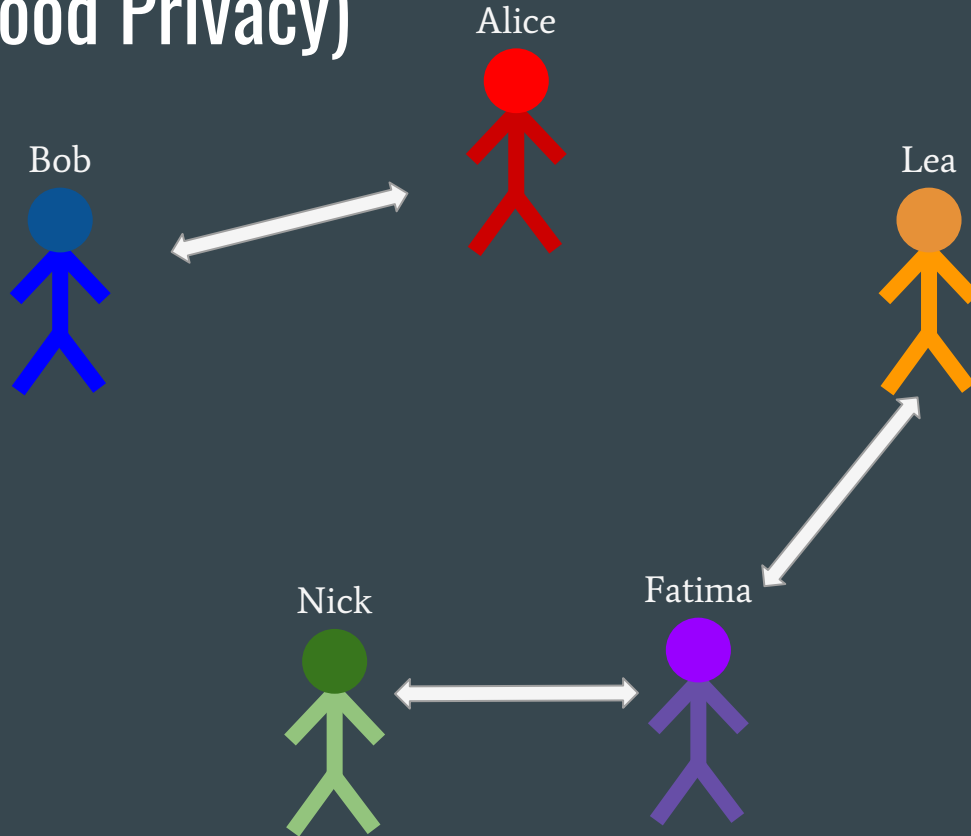
PGP (Pretty Good Privacy)



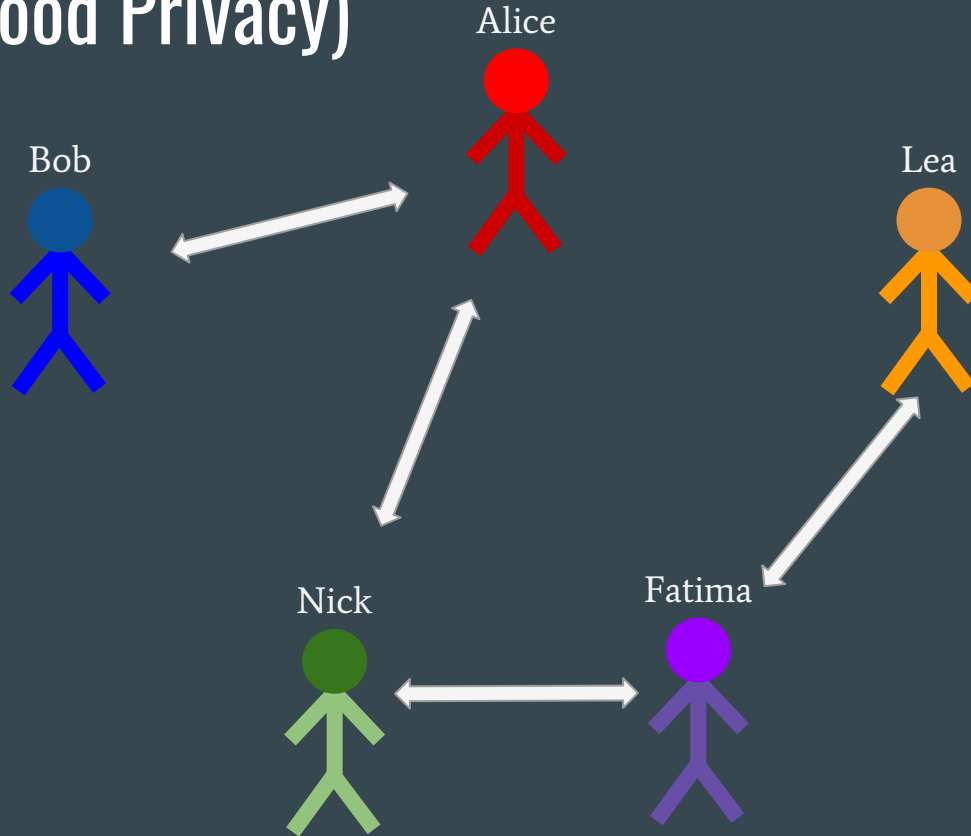
PGP (Pretty Good Privacy)



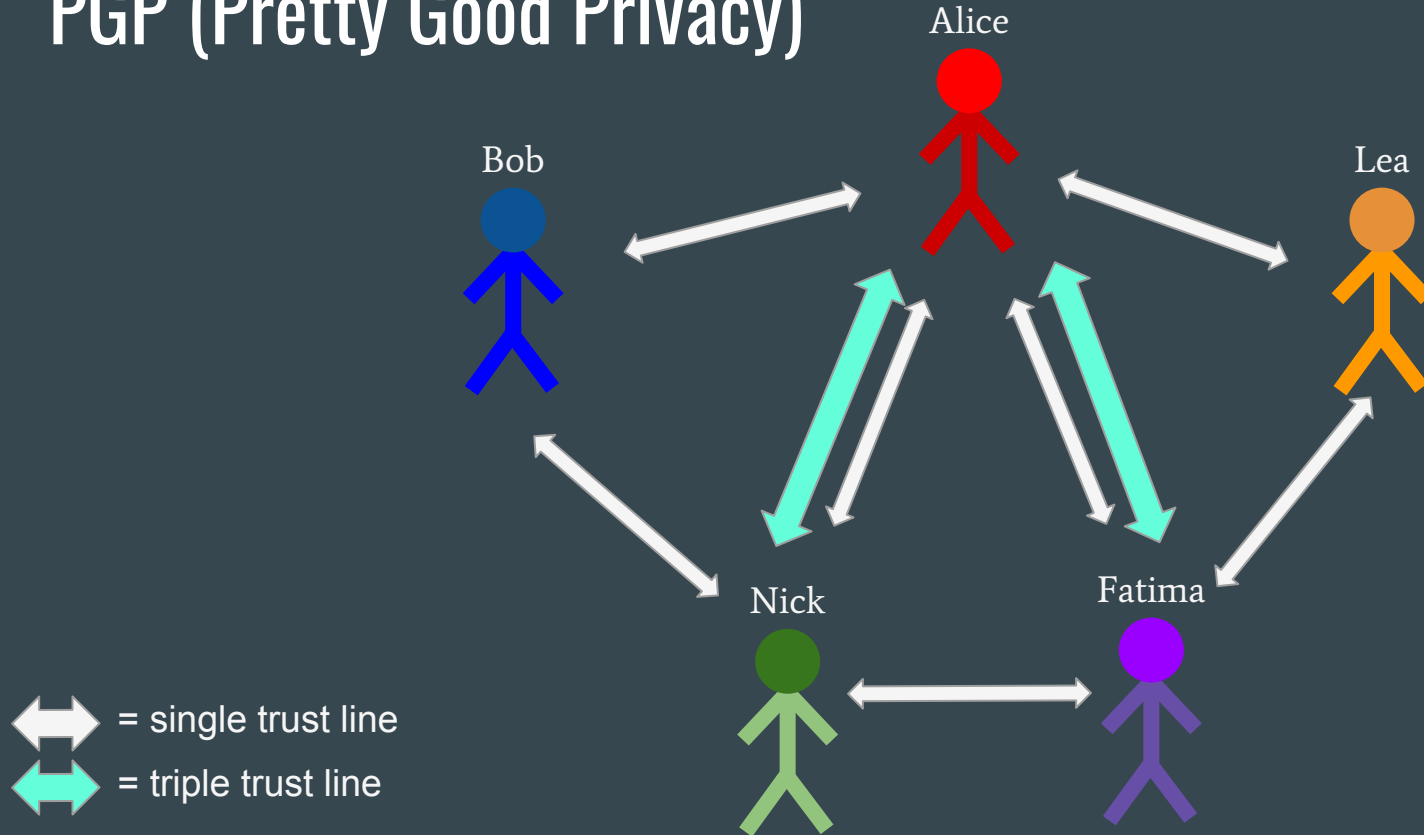
PGP (Pretty Good Privacy)



PGP (Pretty Good Privacy)



PGP (Pretty Good Privacy)



PGP (Pretty Good Privacy)

Public Keyserver



The screenshot shows a web browser window with the address bar displaying 'pgp.mit.edu'. The page title is 'MIT PGP Public Key Server'. Below the title, there are links for 'Help' (Extracting keys, Submitting keys, Email interface, About this server, FAQ) and 'Related Info' (Information about PGP). The main section is titled 'Extract a key' and contains a search form. The search string is 'satoshin@gmx.com' and there is a 'Do the search!' button. Below the search string, there are radio buttons for 'Index' (selected) and 'Verbose Index'. There are also two checkboxes: 'Show PGP fingerprints for keys' and 'Only return exact matches'. The bottom section is titled 'Submit a key' and contains a text area for entering an ASCII-armored PGP key, with a 'Clear' button and a 'Submit this key to the keyserver!' button.

← → ↻ ⓘ pgp.mit.edu ☆ 🔑 🔴 3 🔒 ⋮

MIT PGP Public Key Server

Help: [Extracting keys](#) / [Submitting keys](#) / [Email interface](#) / [About this server](#) / [FAQ](#)
Related Info: [Information about PGP](#) /

Extract a key

Search String:

Index: ☒ Verbose Index: ☐

☐ Show PGP fingerprints for keys
☐ Only return exact matches

Submit a key

Enter ASCII-armored PGP key here:

PGP (Pretty Good Privacy)

Key Signing Parties



PGP (Pretty Good Privacy)

Encrypting with Mailvelope

chrome-extension://kajlbbellbohfggdiogboambcijhke/components/editor/editor.html?id=5b8bdecb27fe521d97d28635

Compose Email

arik@bitgo.com

Add recipient

Hi Arik,

I'm encrypting this message with your private key, nobody else will be able to read it!

Cheers,

Alex

Encrypt attachments

Options

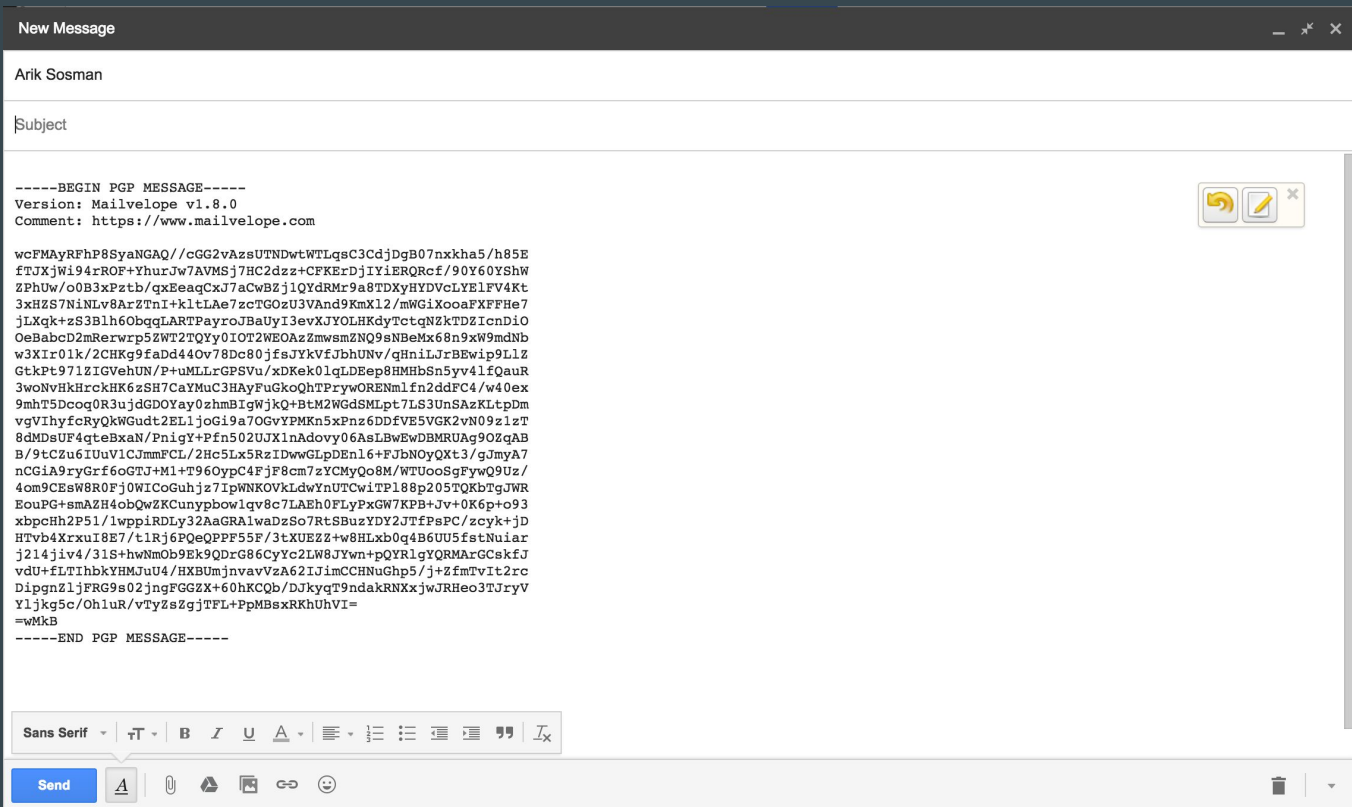
Sign Only

Cancel

Encrypt

PGP (Pretty Good Privacy)

Encrypting with Mailvelope



PGP (Pretty Good Privacy)

Command Line PGP with GNU Privacy Guard (gpg)

```
1. root@ip-172-31-41-241: /home/ubuntu/dev/dctrl-fobtap (gpg)
tachys:~ alex$> gpg --expert --full-generate-key
gpg (GnuPG) 2.2.1; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
  (7) DSA (set your own capabilities)
  (8) RSA (set your own capabilities)
  (9) ECC and ECC
 (10) ECC (sign only)
 (11) ECC (set your own capabilities)
 (13) Existing key
Your selection? |
```

PGP (Pretty Good Privacy)

Key Creation

```
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
2293i090f9b0ad0909irl0pgg: key 8A626EBBA8707FB7 marked as ultimately trusted
93pgg: revocation certificate stored as '/Users/alex/.gnupg/openpgp-revocs.d/24E76D
EF5B61C047173487768A626EBBA8707FB7.rev'
public and secret key created and signed.

pub   rsa4096 2017-10-05 [SC] [expires: 2019-10-05]
       24E76DEF5B61C047173487768A626EBBA8707FB7
uid           Alex Melville (Primary PGP Key) <myemail@gmail.com>
sub   rsa4096 2017-10-05 [E] [expires: 2019-10-05]

tachys:~ alex$>
```

PGP (Pretty Good Privacy)

Signing



Cryptography Basics

Why Use it?

Encryption

- Secure Messaging (Whatsapp)

Digital Signatures

- Used for authenticating (git signing)

Cryptography Basics

Two Main Types

Symmetric

- Only 1 key
- AES is most common
- Fast

Asymmetric (public/private)

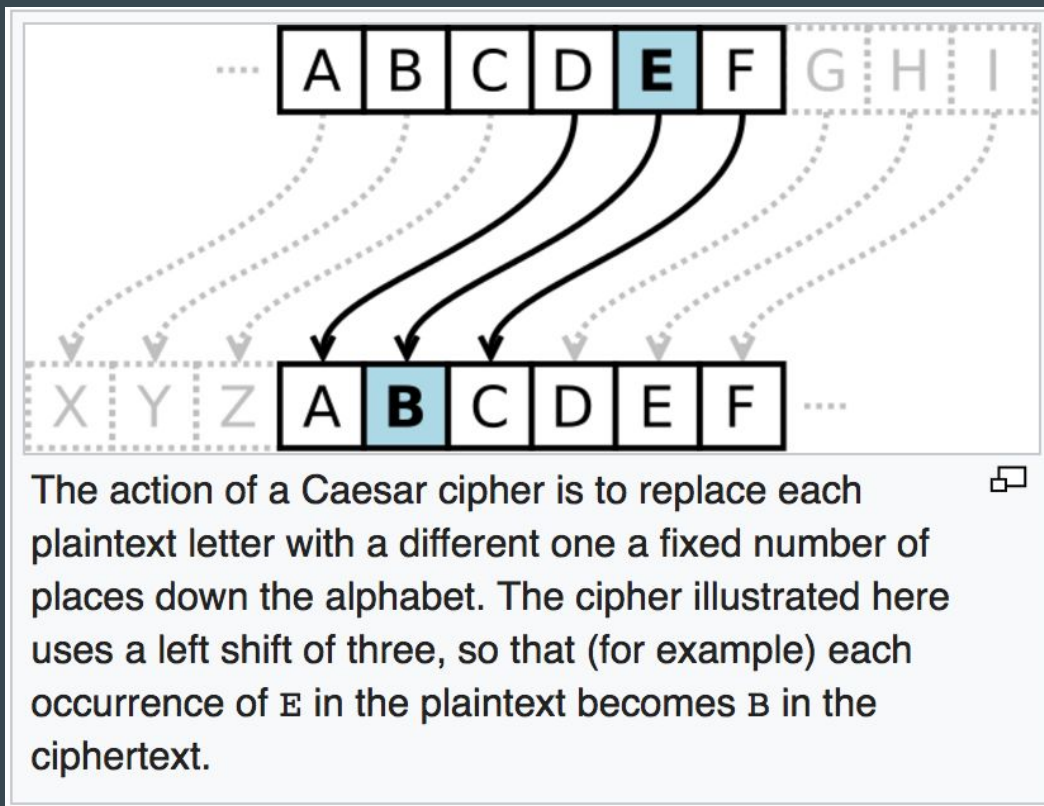
- 2 keys
- DSA is most common
- Slow

Cryptography Basics

Symmetric: Caesar Shift Cipher

abcd → bcde

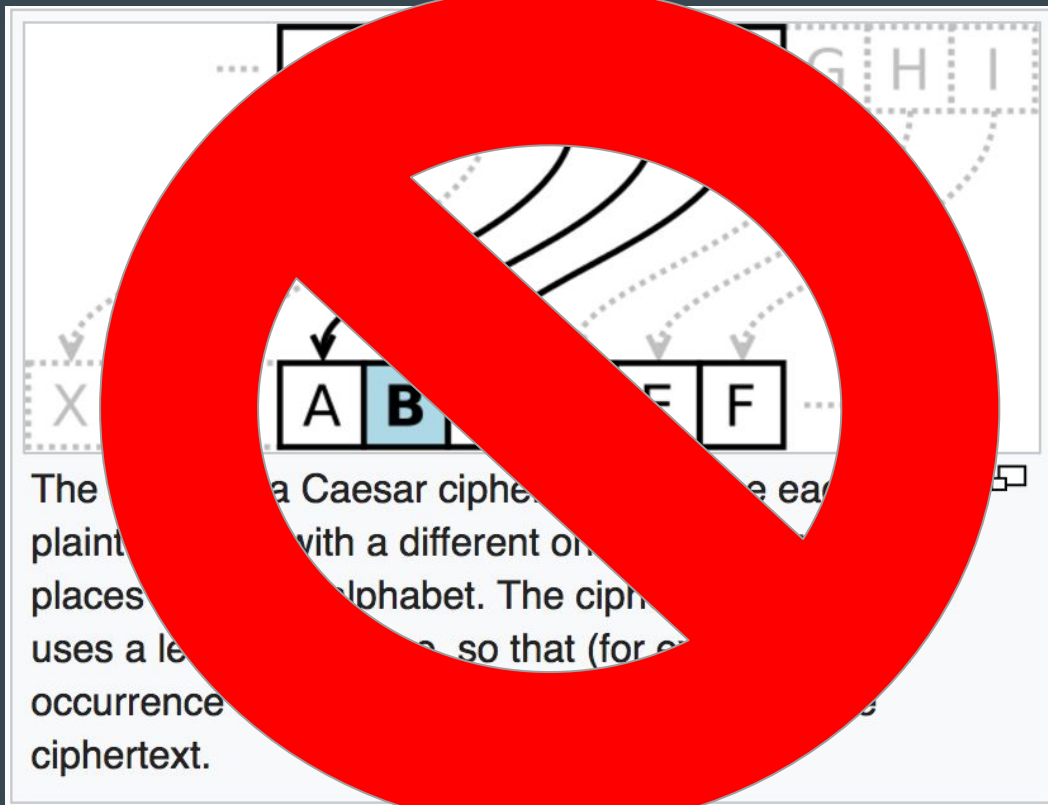
wxyz → xyza



Cryptography Basics

Toy Example!

Do Not Use At Home

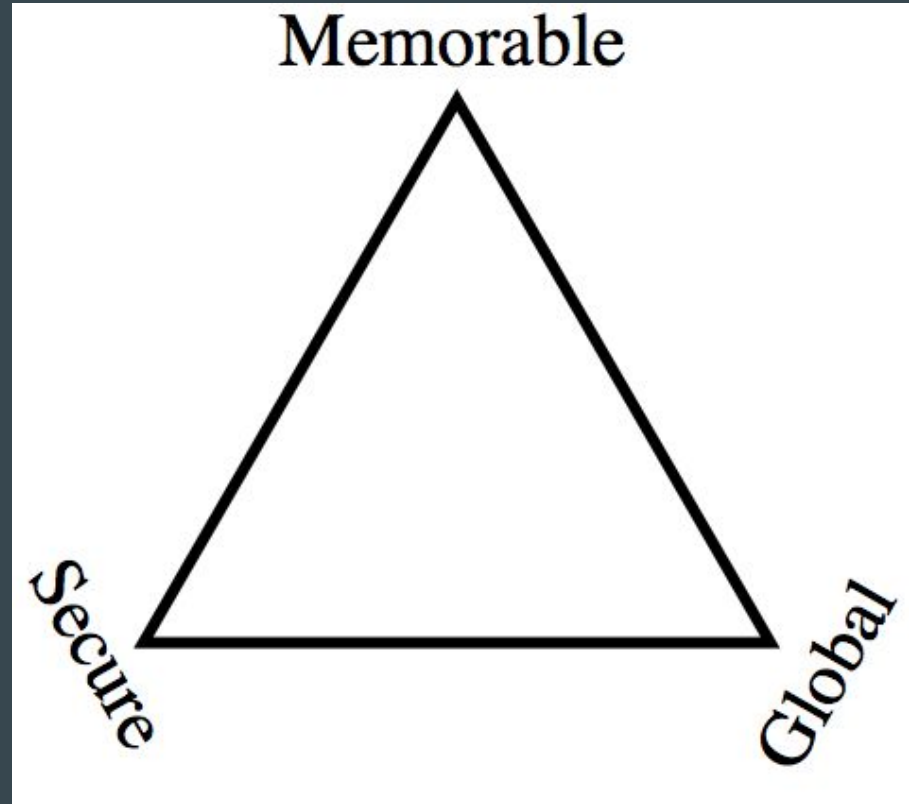


Cryptography Basics

Public/Private Key Cryptography

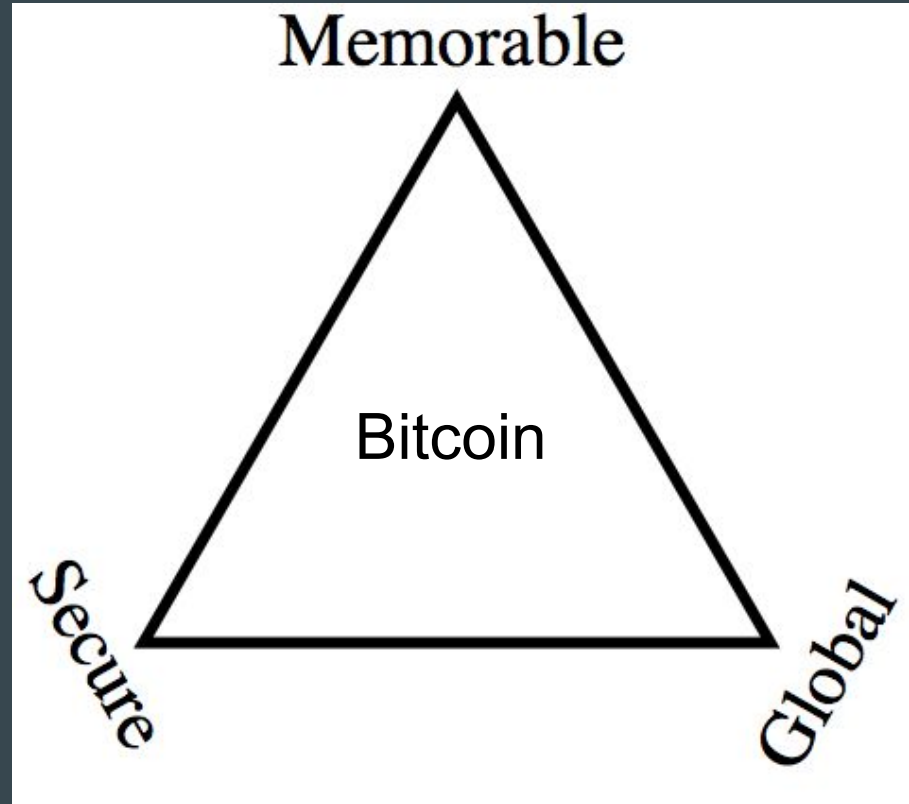
Identity on the Blockchain

Zooko's Triangle



Identity on the Blockchain

Zooko's Triangle



Identity on the Blockchain

Embed identity information in blockchain (bitcoin) transactions



Namecoin

Namecoin is an experimental open-source technology which improves decentralization, security, censorship resistance, privacy, and speed of certain components of the Internet infrastructure such as DNS and identities.

(For the technically minded, Namecoin is a key/value pair registration and transfer system based on the Bitcoin technology.)

Bitcoin frees money – Namecoin frees DNS, identities, and other technologies.

What can Namecoin be used for?

- Protect free-speech rights online by making the web more resistant to censorship.

What does Namecoin do under the hood?

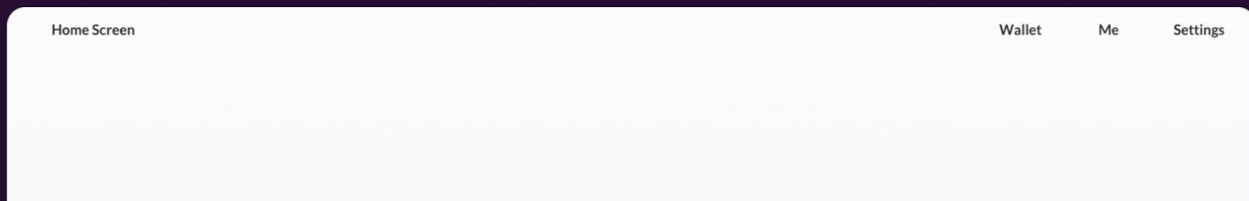
- Securely record and transfer arbitrary names (keys).
- Attach a value (data) to the names (up to 520 bytes).

A New Internet for Decentralized Apps

Blockstack is a new internet for decentralized apps where users own their data.
A browser is all that's needed to get started.

INSTALL

GET UPDATES



Breaking News: Civic Has Reached Its Goal Of Selling \$33 Million In Digital Currency Tokens

LEARN MORE



SECURE IDENTITY PLATFORM

ID THEFT PROTECTION

MARKETPLACE

PARTNERS

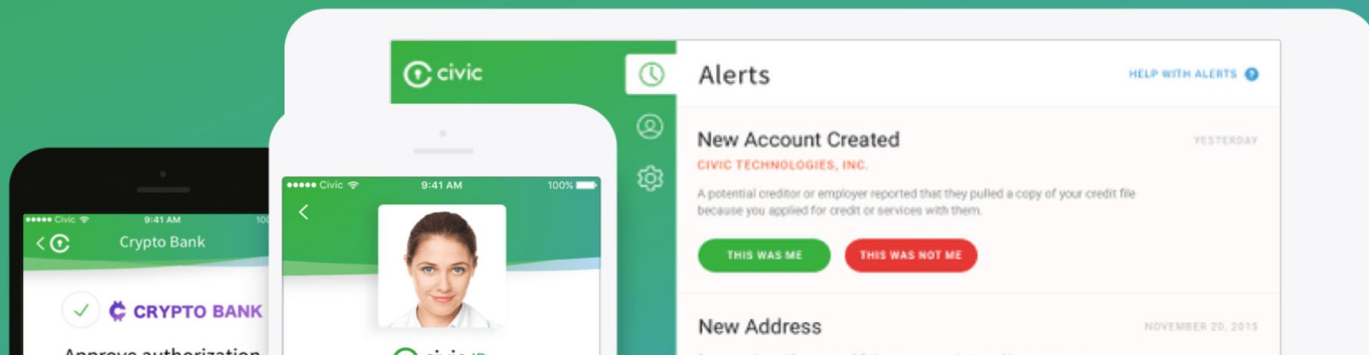
GET THE APP

Secure & Protect Identities

Giving **businesses** and **individuals** the tools to control and protect identities.

WATCH THE VIDEO

GET THE APP



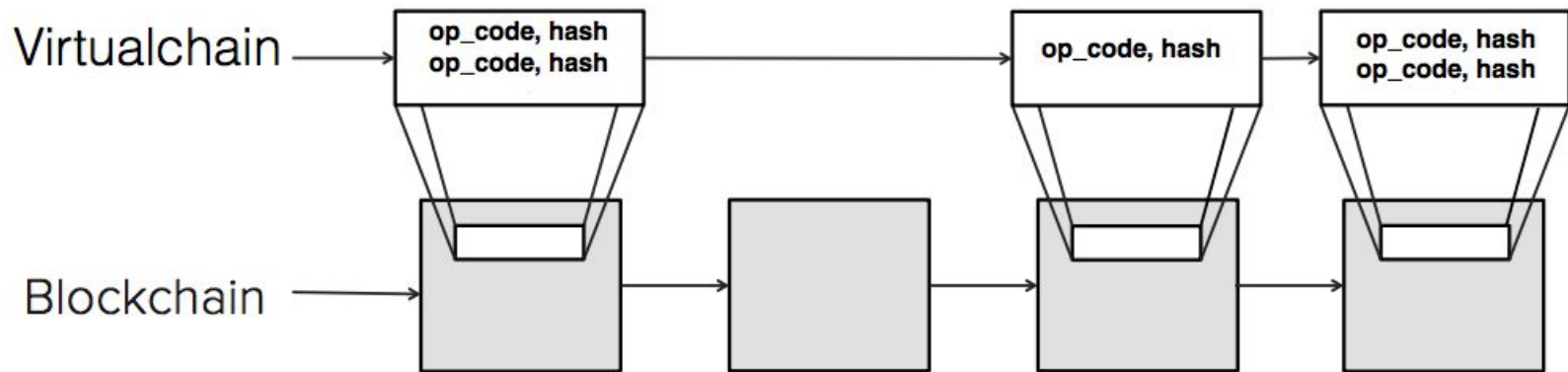


Figure 4: Virtualchain operations on top of an underlying blockchain.

Public PGP Keyserver ↔ Blockchain

Recap

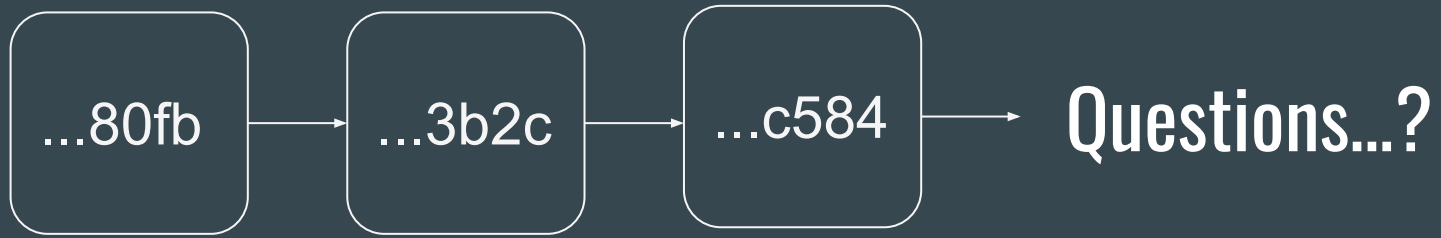
Current Digital Identities

PGP

Cryptography Basics

Blockchain Identity

Create Your Own Identity Walkthrough (if there's time!)



More PGP Resources

- https://github.com/Melvillian/gpg_tutorials
- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- <https://www.gnupg.org/documentation/manuals/gnupg/Operational-GPG-Commands.html>
- <https://spin.atomicobject.com/2013/11/24/secure-gpg-keys-guide/>
- <https://malcolmsparks.com/posts/yubikey-gpg.html>
- <https://steemit.com/security/@the-tech-guy/how-to-configure-your-yubikey-for-use-with-gnupg>
- <https://getpocket.com/a/read/1914461520>
- https://developers.yubico.com/PGP/Card_edit.html