Institute and Faculty of Actuaries

GIRO Conference 2022

21–23 November, ACC Liverpool

#GiroConf22

Institute and Faculty of Actuaries

Ethics & considerations when paying cyber insurance policies with bitcoin for ransom demands

Richard FOSTER – Brainstorm Security Ltd

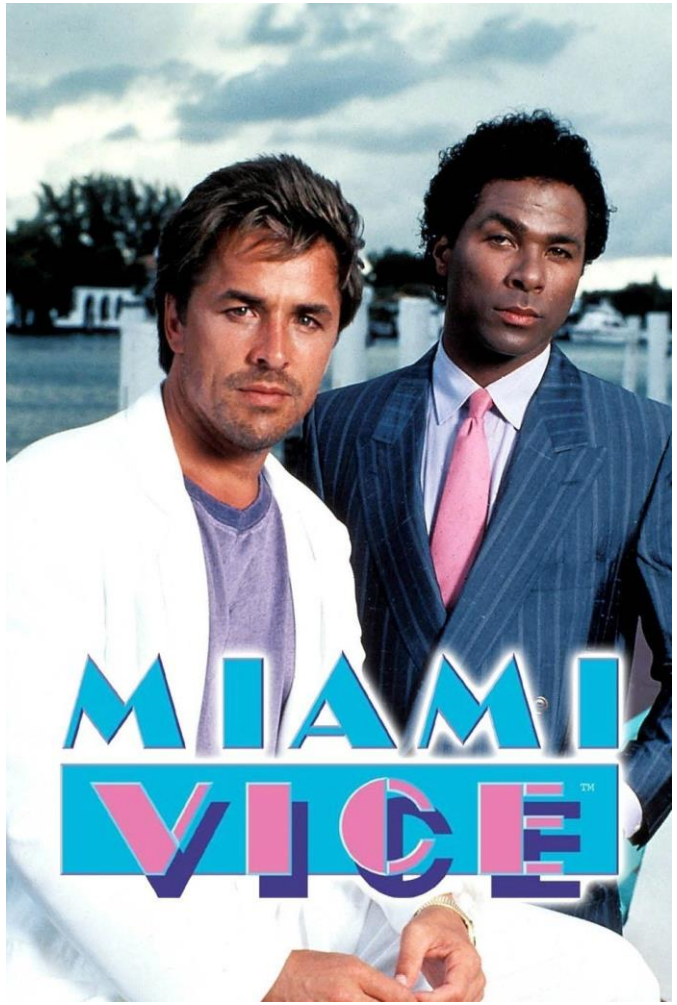
#GiroConf22

About Me

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

About Me



BRAINSTORM SECURITY

Institute and Faculty of Actuaries

My Career

10 Years

18 Years

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

My Career

Crimes in Action - Traditional

- Kidnap
- Extortion
- Abduction
- Hostage taking
- Product Contamination

Modern criminals

- Cybercrime
- Hackers
- Data theft
- Data destruction

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Who has heard of Bitcoin before today?

What is Bitcoin?

"Bitcoin is digital Money"

Before Bitcoin ...what is money?

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Money is: A Medium of Exchange

- Items that can be bartered and are widely accepted.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Money is: A Unit of Account

- Recognisable
- Fungible
- Divisible
- Transportable
- Transferable
- Hard to Counterfeit.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Money is: A Store of Value

- Stable supply
- Durable
- Securable
- Stable value.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Cryptocurrency is: A Bearer Instrument

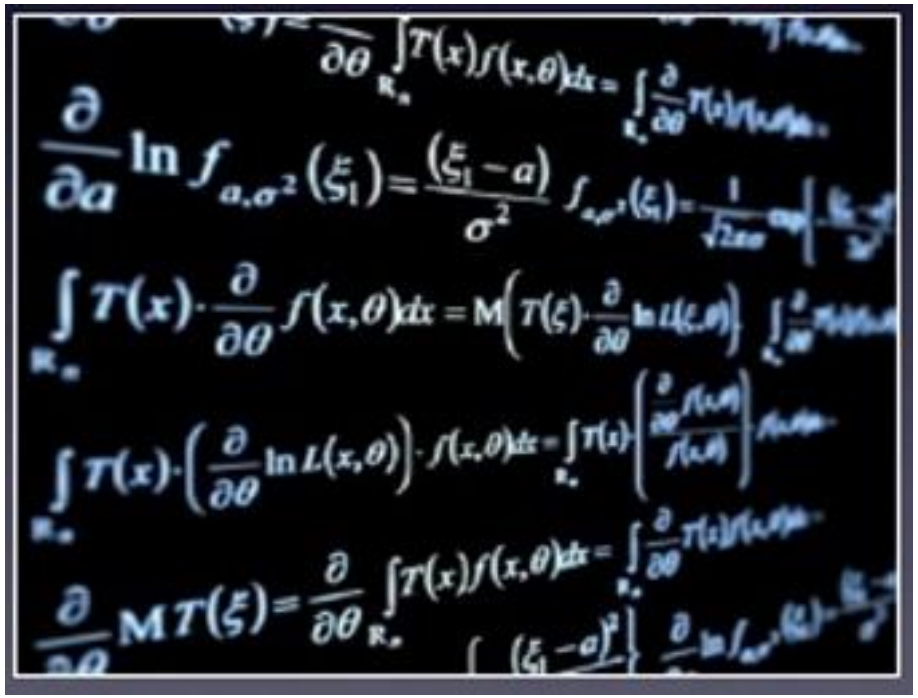
- Holder has ownership
- No other records kept as to the identity of owner
- Easy to keep anonymous
- Hard or impossible to replace if lost or stolen.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Cryptocurrency is:
A Bearer Instrument……Based on Digital Cryptography

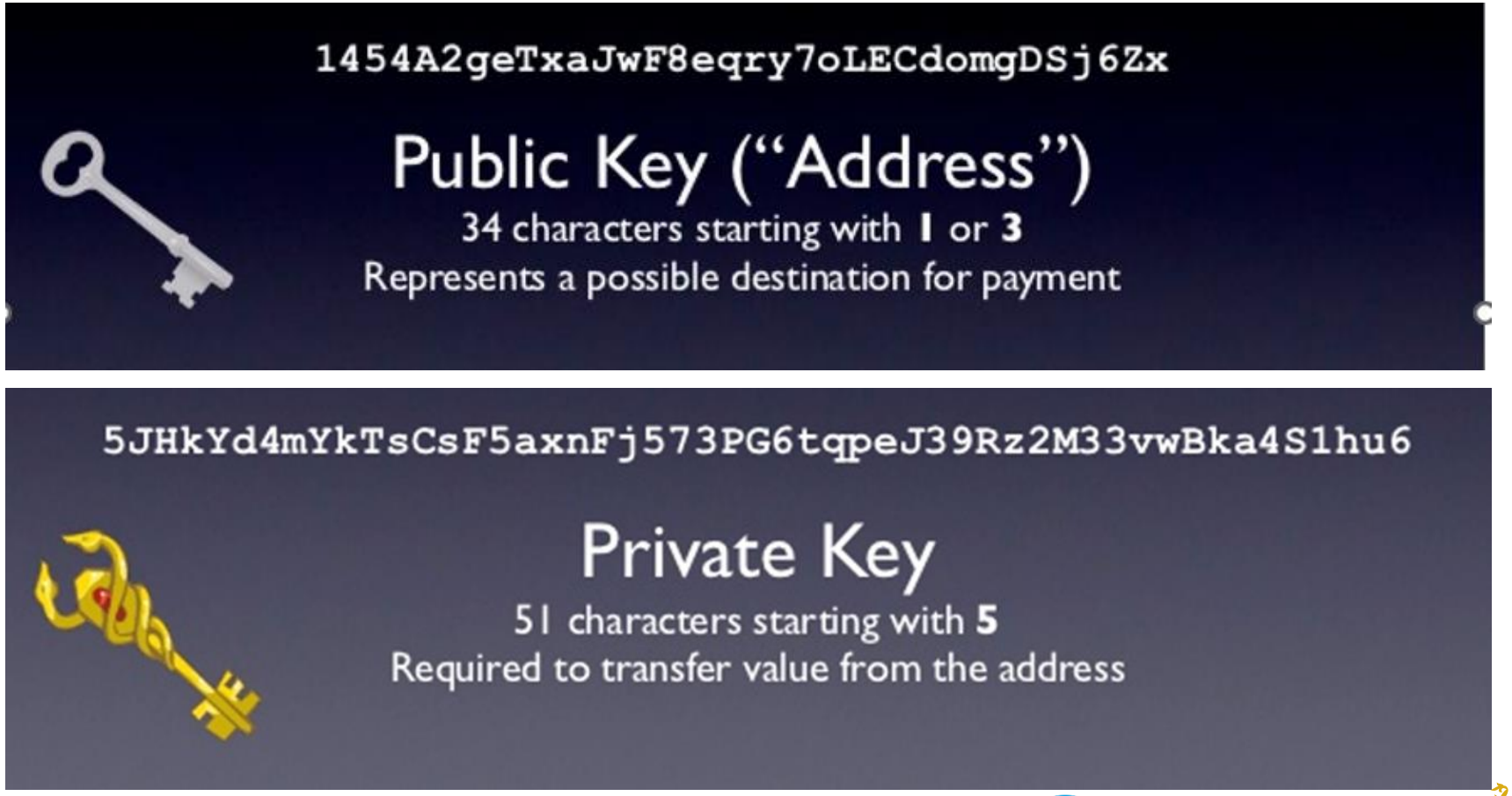
- Lots of computers doing complex maths problems
- Derives trust from known established mathematical properties.



BRAINSTORM SECURITY

Institute and Faculty of Actuaries

What do Bitcoins look like?



BRAINSTORM SECURITY

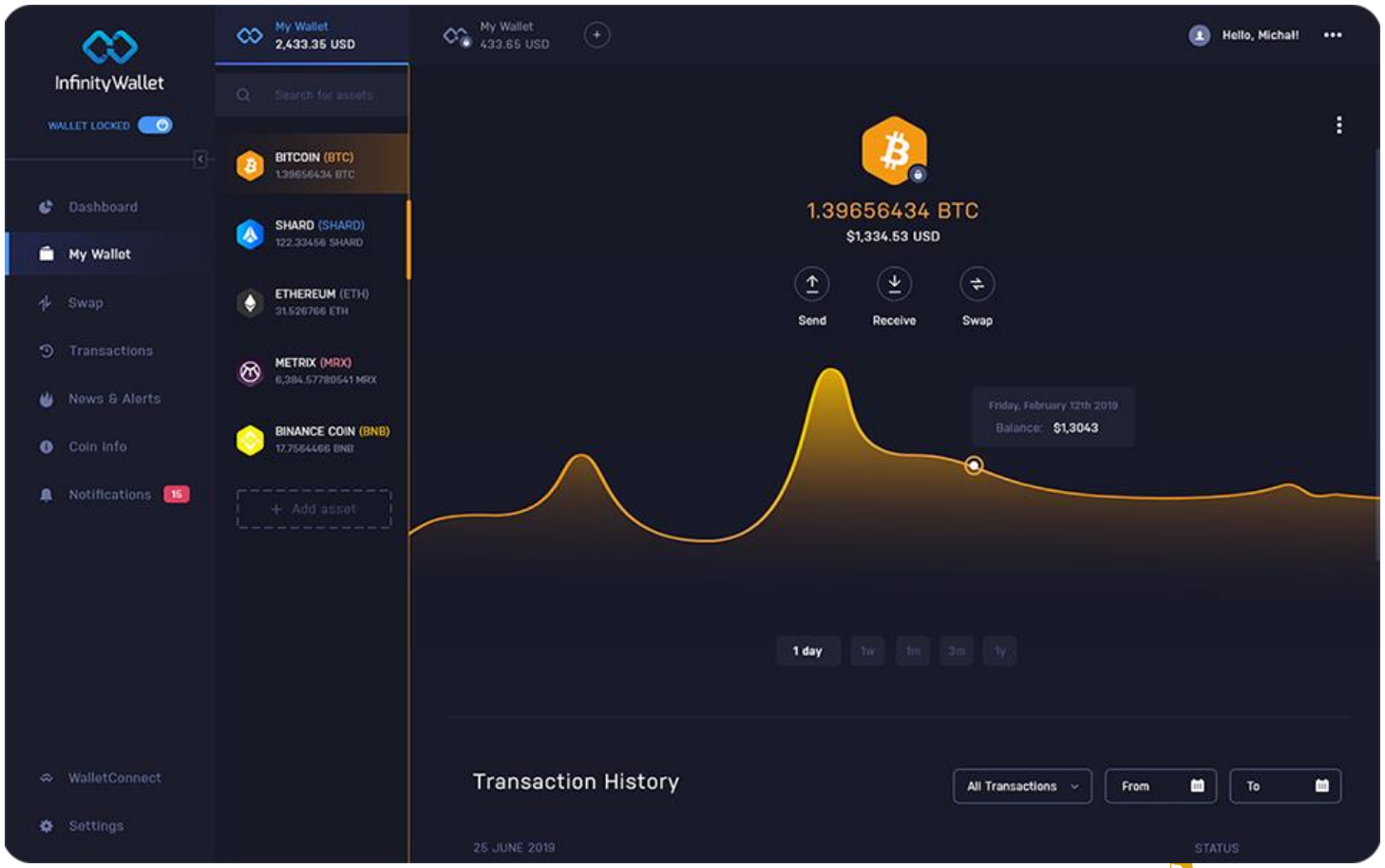
Institute and Faculty of Actuaries

What do Bitcoins look like?

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

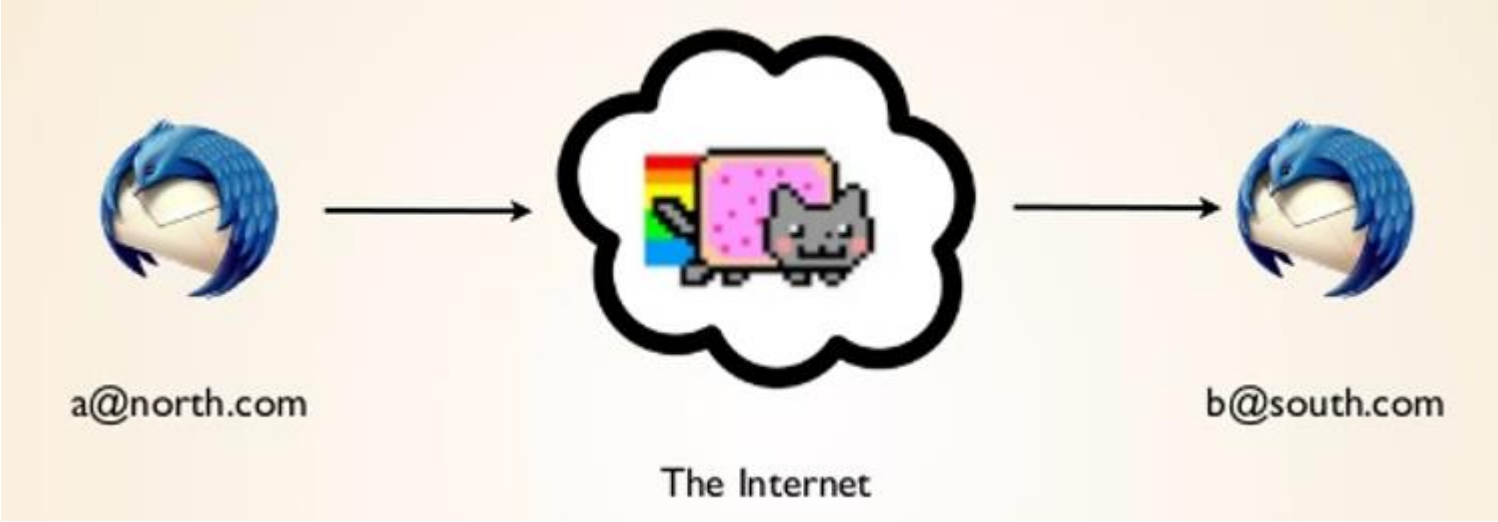
What does a Bitcoins Wallet look like?



BRAINSTORM SECURITY

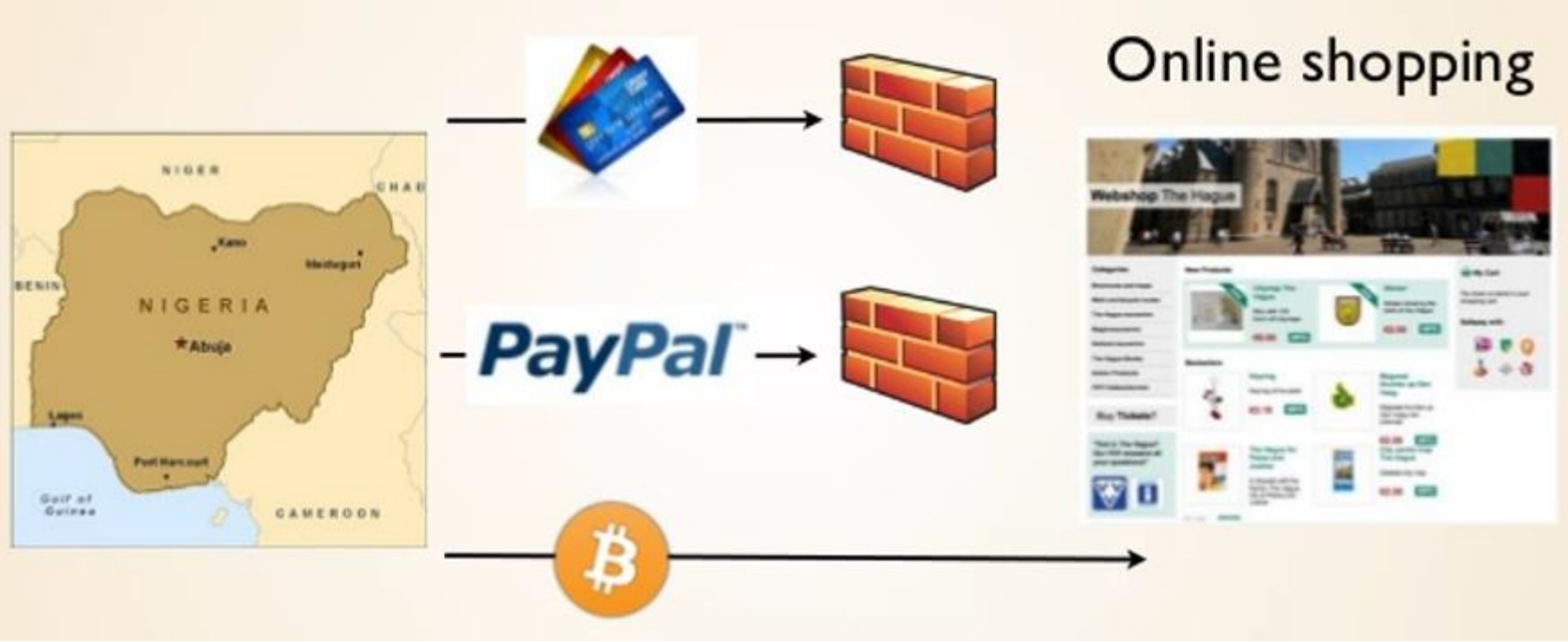
Institute and Faculty of Actuaries

Bitcoin is like email



Institute and Faculty of Actuaries

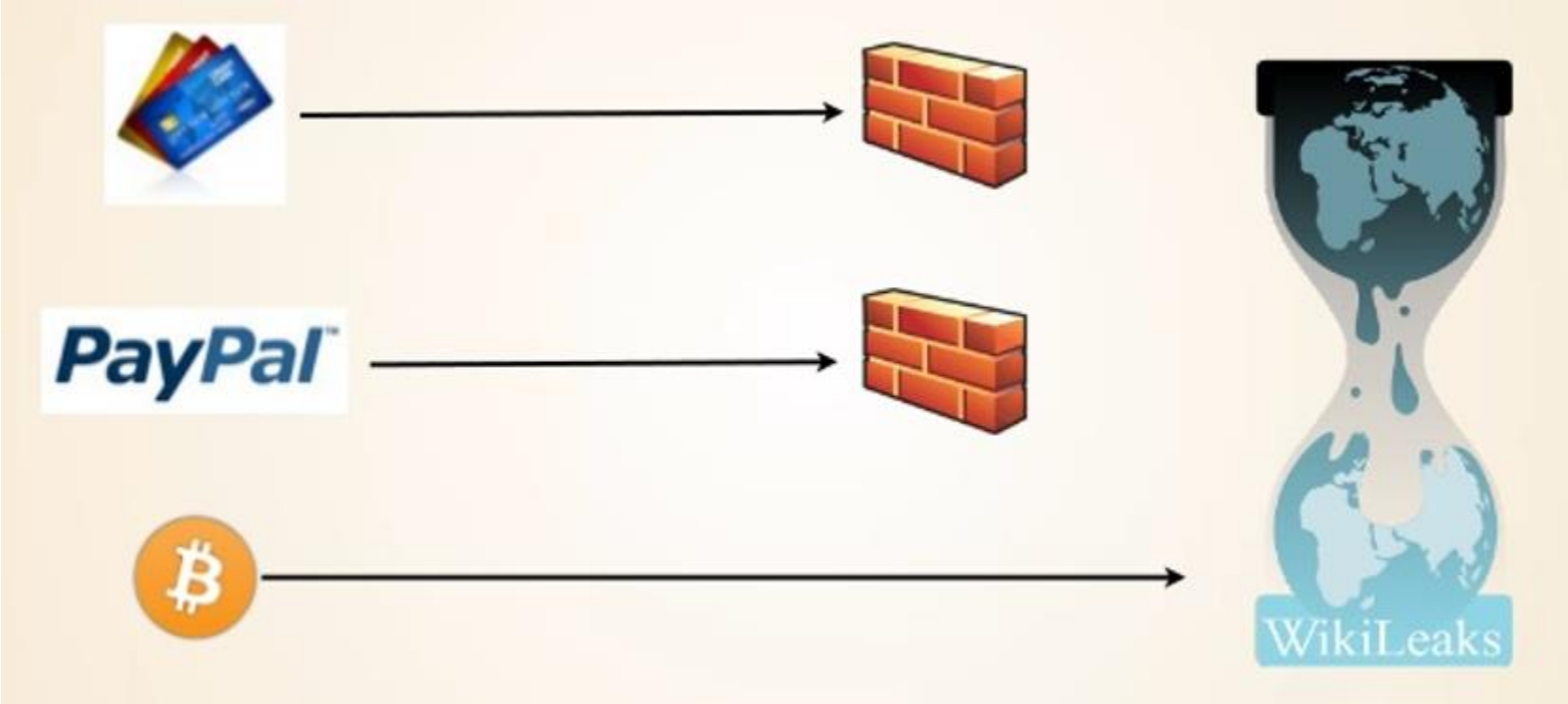
Bitcoin is truly International



BRAINSTORM SECURITY

Institute and Faculty of Actuaries

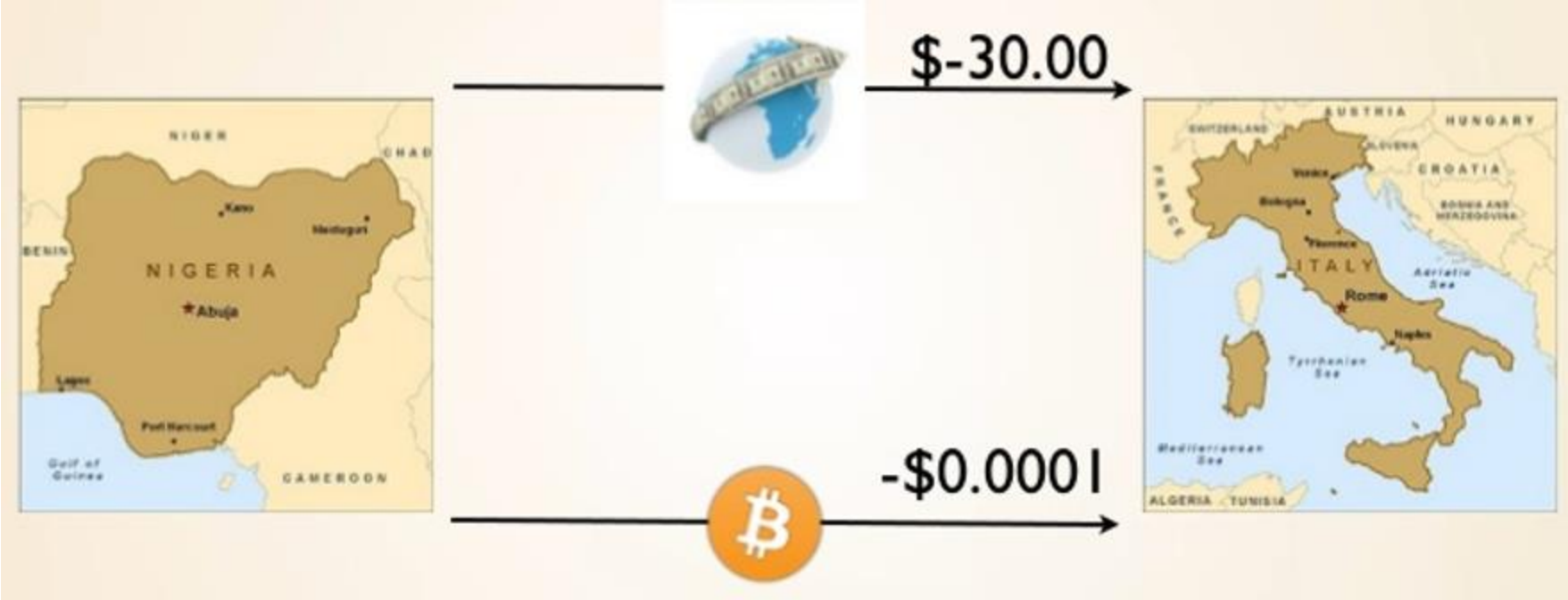
Bitcoin is difficult to block



BRAINSTORM SECURITY

Institute and Faculty of Actuaries

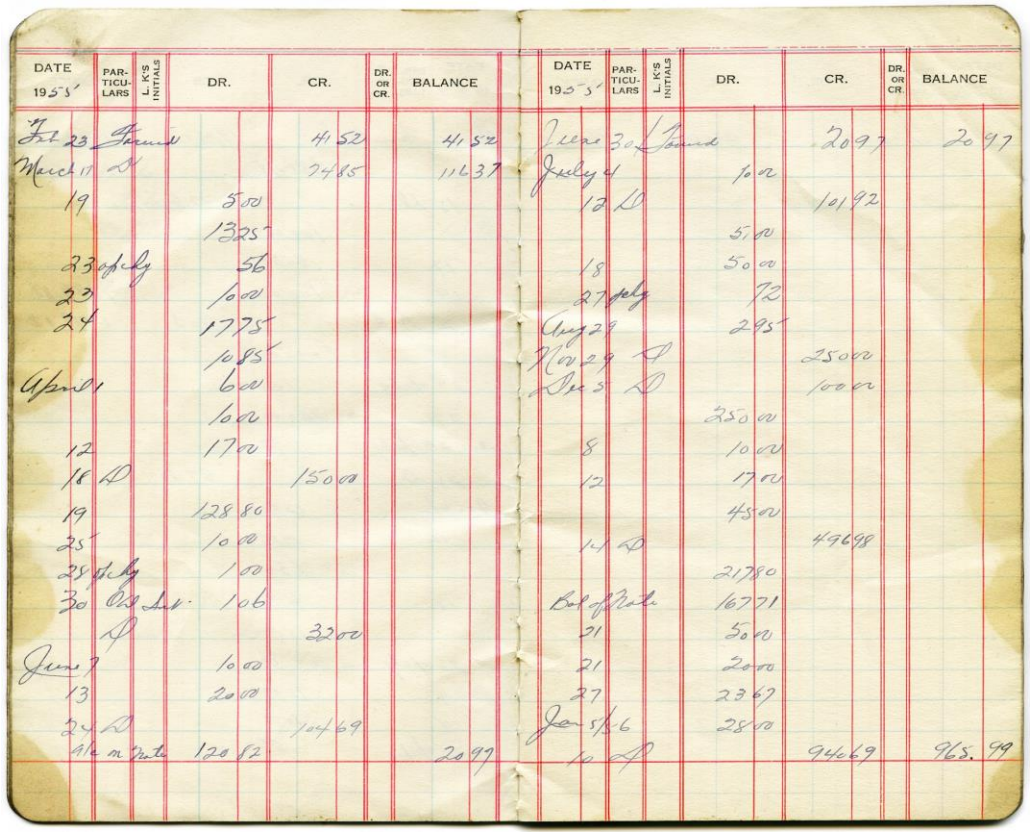
Bitcoin is cheaper than wire transfer

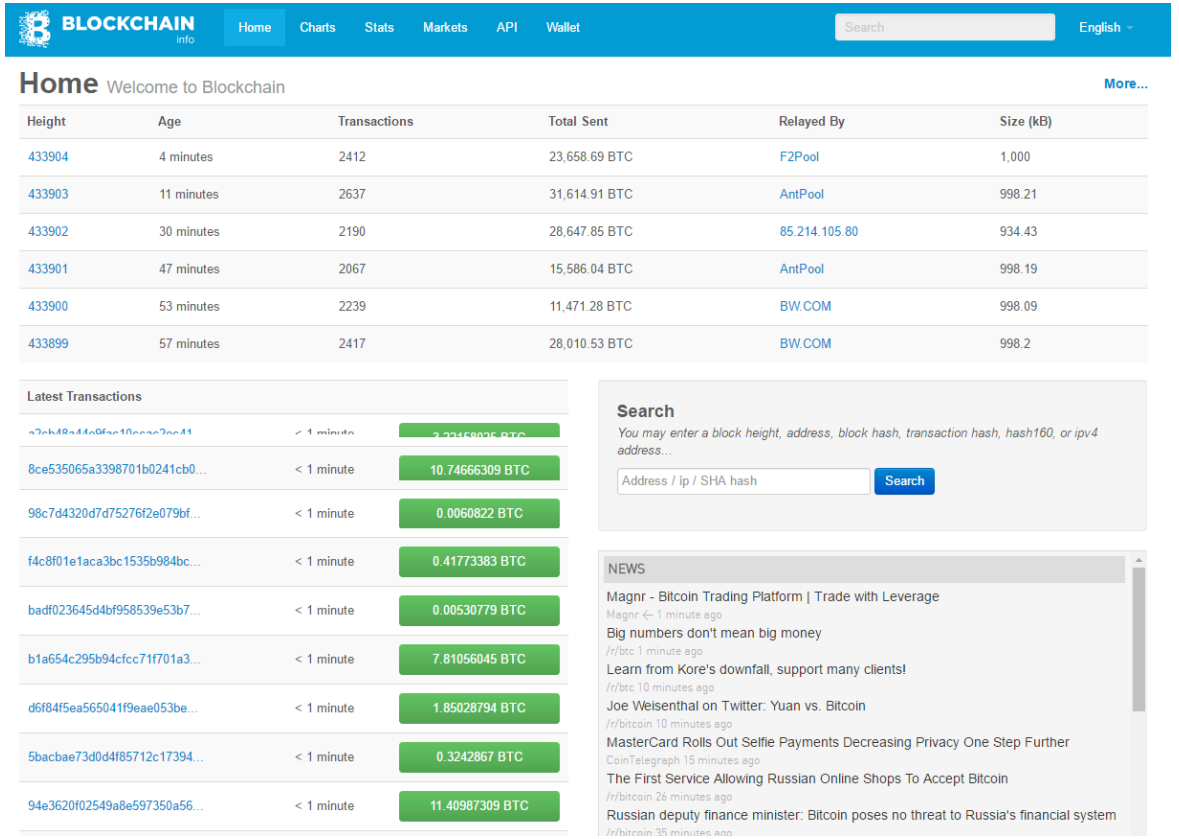


BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Bitcoin is a ledger





BRAINSTORM SECURITY

Institute and Faculty of Actuaries

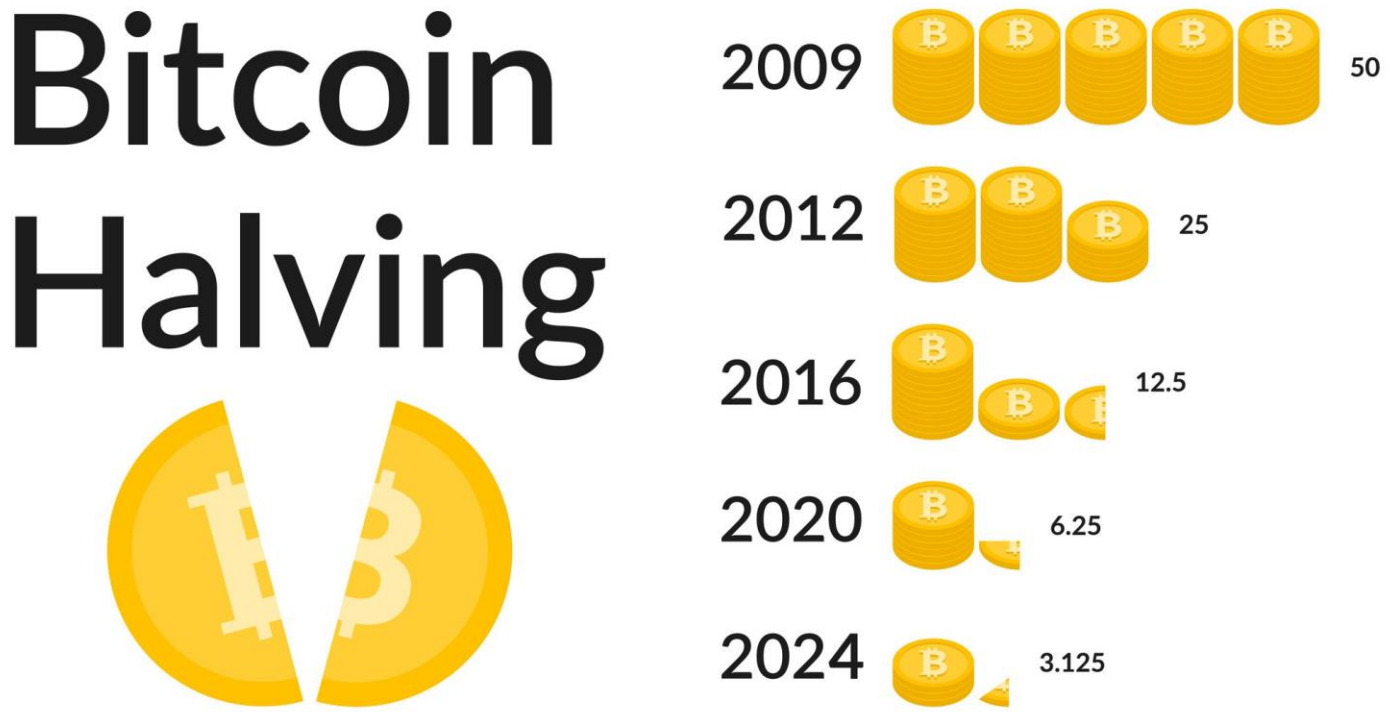
Where do Bitcoins come from?

Miners - Generate new coins by solving maths problems

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Bitcoin has a limited supply – Ensuring value



BRAINSTORM SECURITY

Institute and Faculty of Actuaries

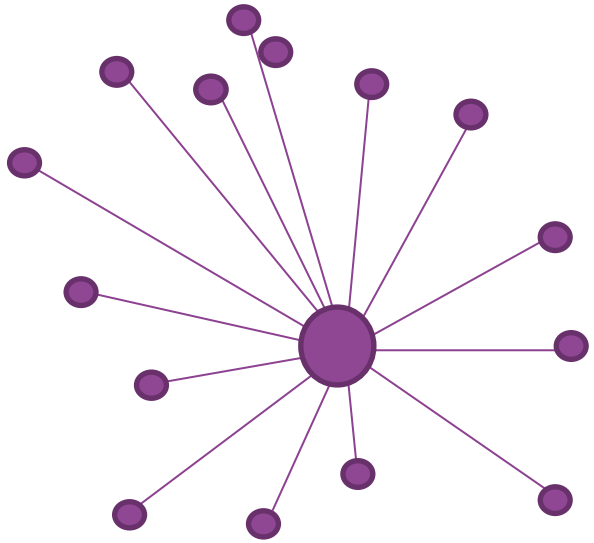
What are Bitcoins worth?

- 10 Oct 2022

BRAINSTORM SECURITY

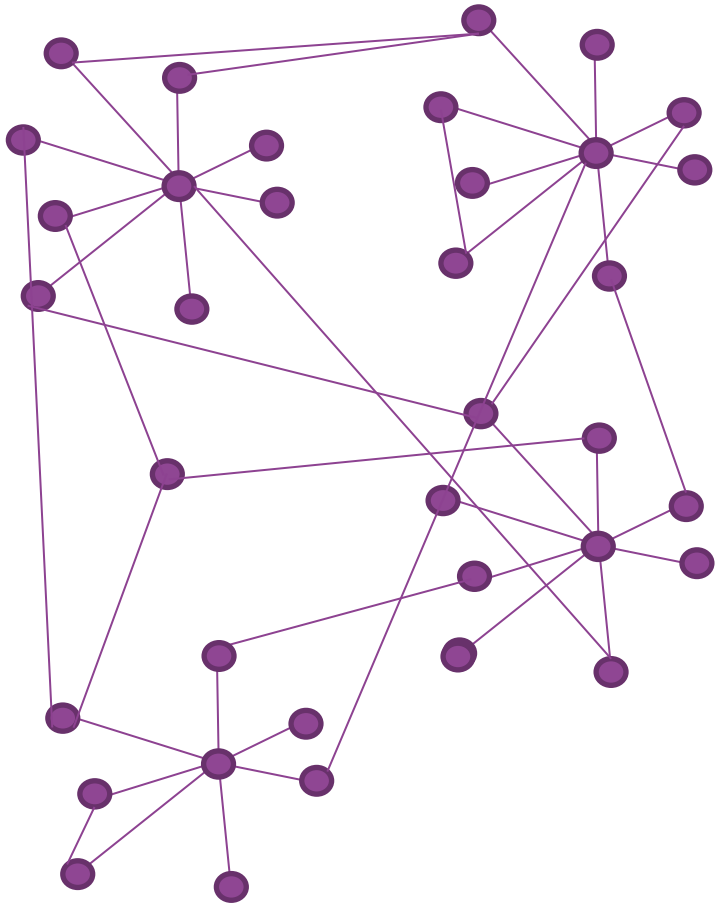
Institute and Faculty of Actuaries

A Decentralised Currency



CENTRALISED

Problem	Solution
Central point of failure	Decentralised network
Expensive to secure	Shared security cost
Trust who is in charge	Trust a fixed set of rules



DECENTRALISED

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

How to Get Bitcoin?

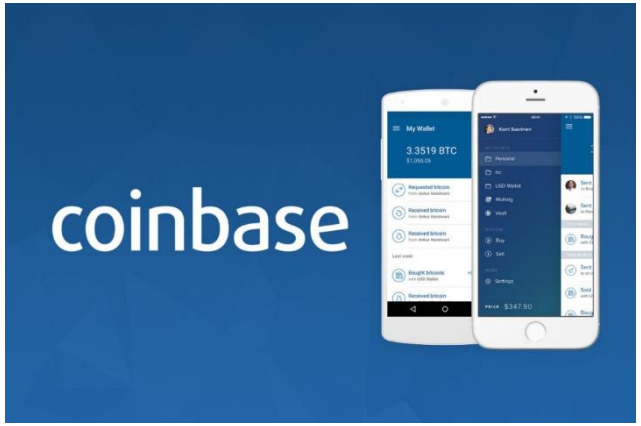
- ATM

- Bank Transfer

- In Person exchange

- Crypto Exchange

MT.GOX



BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Difficulties in buying Bitcoin

- Need to set up Bitcoin wallet/address in advance
- Need smartphone and QR reader?
- Some ATMs and Exchanges require ID to be uploaded before transaction.
- If using Local Bitcoin the person, may try and rip you off, or the Bank may stop transaction during funds transfer.
- Face to Face meets done in public to avoid rip off
- Fake / corrupt exchange could take all your money

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

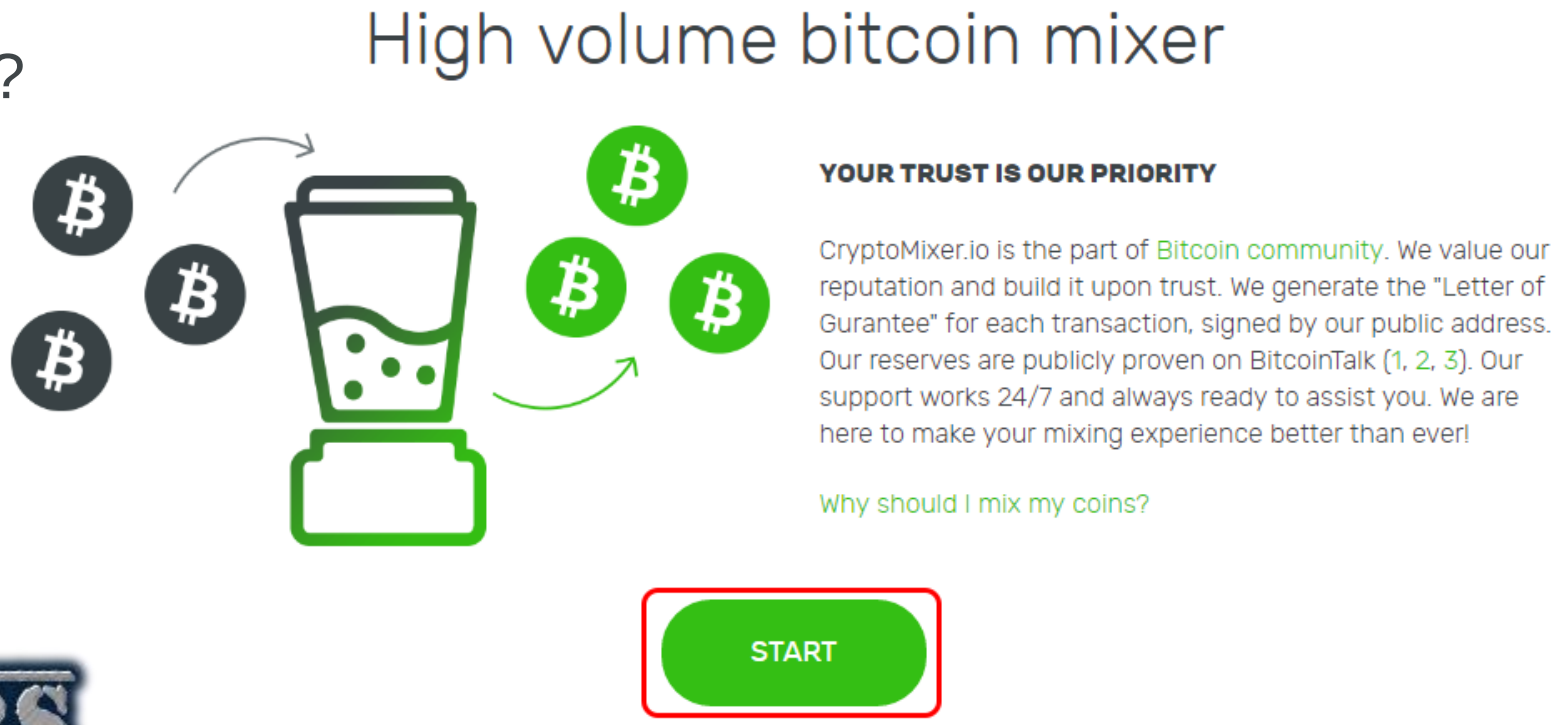
Bitcoin & Crime

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

BTC Mixers/Tumblers

- Scams / Trusted ??



BTC MIXERS

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Good / Bad

Good	Bad
Public ledger keeps record of every transaction	Once spent its gone – no charge back
Cheap to send / pay for items	Could be stolen by Hackers
Micro payments	Difficult to attribute to a person
Anonymous	Could be lost or data corrupted
Simple to use	No Financial compensation - FSA
Can send large amounts of money internationally for little/no fees	

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Interactive Questions

Using your phone,
type in a browser
menti.com then
add the code

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Interactive Questions

Who carries out cyber attacks?

Nation states

Hacking / Crime groups

 Youngsters and lone-actors

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Interactive Questions

Do criminals attack big or small companies?

Big & Small!

- Small companies have websites, online payments, email.
- They don’t have IT Dept, Cyber awareness Training, Backups, Disaster recovery plan.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Interactive Questions

How can companies reduce the risk of cyber attacks and limit any insurance claim?

- Training
- Cyber Essentials
- Backups
- Planning

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

The Chief of the UK's National Cyber Security Centre (NCSC) has said that ransomware was the key threat facing the UK, and urged the public and business to take it seriously.

National Cyber Security Centre
a part of GCHQ

In the last 12 months there has been a 400-500% increase in Ransomware attacks

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations - potential legal and commercial risks of paying ransoms?

- You may not end up getting the data back
- A recent Canadian study suggest 9% don’t release the data
- If successful, 80% of data is usable
- Still need to clean up computer systems afterwards
- Making payments will likely encourage further ransomware attacks

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations - potential legal and commercial risks of paying ransoms?

- Some gangs will sell your details to other hackers for further attacks.
- The attackers may learn more about your business and systems (EXTORTION)
- The ransom payments ultimately fund criminal activity
- The ransom payments ultimately fund the purchase of zero days (More malware)
- The ransom payments may fund terrorism (Legal)

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations - potential legal and commercial risks of paying ransoms?

- You can face fines / enforcement from data protection regulators
- ICO guidance says “Law enforcement do not encourage, endorse, nor condone the payment of ransom demands”
- You can face fines / enforcement from other regulators - FCA’s position is that “you need to tell the FCA as soon as you know of ‘material’ cyber incidents which affect your firm.” The FCA’s view is that a ransomware attack is likely to be reportable if malicious software is present on your information and IT systems even if you pay the ransom.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations - potential legal and commercial risks of paying ransoms?

- You could face criminal penalties under anti-bribery laws – in the UK, for example, there is an argument at least that a person making unlawful payments to a ‘foreign public official’ (e.g. in the case of state-sanctioned ransomware attacks) could be prosecuted under the Bribery Act 2010
- You could contravene sanctions regimes – some foreign actors involved in ransomware attacks are subject to sanctions (Think Russia?)

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations - potential legal and commercial risks of paying ransoms?

- You could have difficulties with KYC or other obligations – you are not going to be able to do proper compliance checks or do other due diligence on anyone you are paying a ransom to. If you are subject to any form of KYC, due diligence or money laundering obligations, you are unlikely to be able to meet them.
- It is hard to cover up a ransomware payment – ransomware attacks often become public either through gang activity or a growing number of bloggers and journalists covering ransomware attacks.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations - potential legal and commercial risks of paying ransoms?

- We recommend three assessments for victim companies deciding whether to pay:

(i) The value of the breached data in light of modern ransomware attacks (and is backup data available?);

(ii) The risks (inc reputation) from paying the ransom; and

(iii) Negotiation and payment options.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Practical Considerations

- Email demands can provide time. (Careful to forward on)
- Does the hostage or victim have Bitcoins?
- Would the offenders know? **Insider Threat?**
- Time to obtain Bitcoins.
- Delays (Positives and negatives) – ID verification / unable to buy in large amounts quickly.
- Follow the money – can be done but

  may become untraceable.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Considerations

- Passwords.
- Bitcoin transactions normally confirmed after 10 minutes

What if the Ransom is not paid?

- Loss of the business?
- Loss of Jobs?
- Loss of Life?

Questions

Comments

Contact me

Richard Foster

richard@brainstormsecurity.com

020 8058 0047

www.brainstormsecurity.com

The views expressed in this presentation are those of the presenter.

BRAINSTORM SECURITY

Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

Thank you

#GiroConf22