



Institute  
and Faculty  
of Actuaries

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

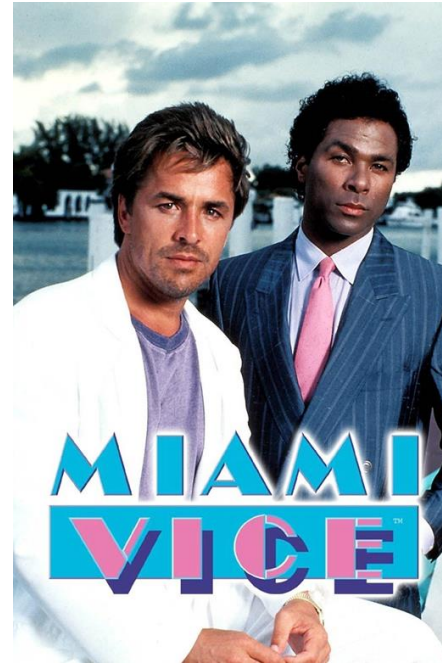
Richard FOSTER – Brainstorm  
Security Ltd

# About Me



Institute  
and Faculty  
of Actuaries

# About Me



Institute  
and Faculty  
of Actuaries

# About Me

The News, Thursday, June 18, 1998 **17**

**PORTSMOUTH** / Police perplexed by boxes of treats dumped in a recycling bin

## Jaffa Cakes riddle takes the biscuit

■ Police believe teatime delights may have fallen off the back of a lorry

**By Darren Beck**  
The News

It is a case worthy of TV's cooking detective Henry Crabbe – the mystery of the dumped Jaffa Cakes.

Why were 230 Jaffa Cakes and 120 individual triple chocolate cakes dumped in a recycling bin at Southsea?

But perhaps finding the answer might baffle even the detective inspector played by Richard Griffiths in

The mystery began when police were alerted by a passer-by who spotted the cakes and biscuits spilling out of the bin in Regent Place.

Fearful they might attract unwanted attention from sweet-toothed passers-by, PC Richard Foster recovered the haul.


After examining them they believe they were dumped after being stolen.

They are now safely under lock and key at the city's central police station in Winston Churchill Avenue.

PC Foster said: 'A member of the public called to report some cakes. They are all freshly stolen or have fallen off the back of a lorry.'

'They probably came from a catering company of some description or a local hotel maybe.'

'Anyone who owns them can call me on 859333 and collect them. That is if I can keep police officers from eating them!'



**Baffling:**  
TV detective **Richard Griffiths**

**PC Richard Foster with a selection of the dumped cakes**

# About Me



10 Years



18 Years



Institute  
and Faculty  
of Actuaries

# About Me

## Crimes in Action - Traditional

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



## Modern criminals

- Cybercrime
- Hackers
- Data theft
- Data destruction



Institute  
and Faculty  
of Actuaries

Who has heard of Bitcoin before today?



# What is Bitcoin?

“Bitcoin is digital Money”



Institute  
and Faculty  
of Actuaries



# Before Bitcoin ...what is money?



# Money is: A Medium of Exchange



# Money is: A Medium of Exchange



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

# Money is: A Medium of Exchange



- Stable supply
- Durable
- Securable
- Stable value.

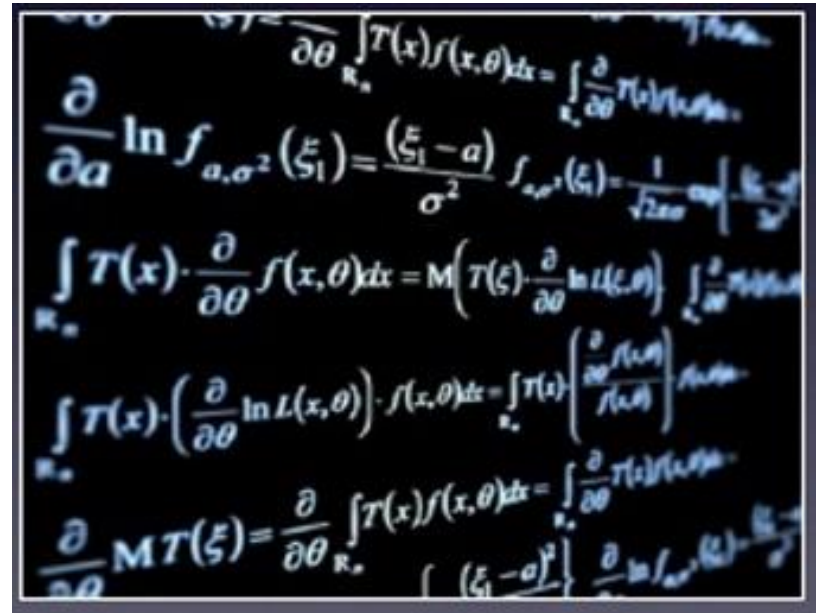
# Cryptocurrency is: A Bearer Instrument

- 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.



# Cryptocurrency is: A Bearer Instrument.....Based on Digital Cryptography

- Lots of computers doing complex maths problems



# What do Bitcoins look like?

1454A2geTxaJwF8eqry7oLECDomgDSj6Zx



## Public Key (“Address”)

34 characters starting with **1** or **3**  
Represents a possible destination for payment

5JHkYd4mYkTsCsF5axnFj573PG6tqpeJ39Rz2M33vwBka4S1hu6



## Private Key

51 characters starting with **5**  
Required to transfer value from the address



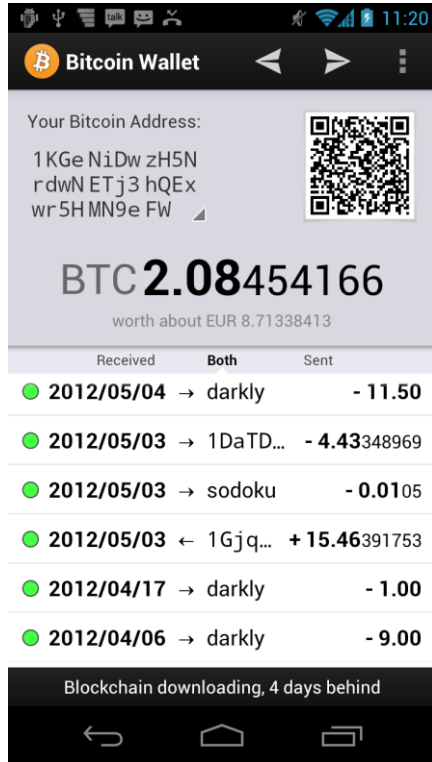
Institute  
and Faculty  
of Actuaries

# What do Bitcoins look like?

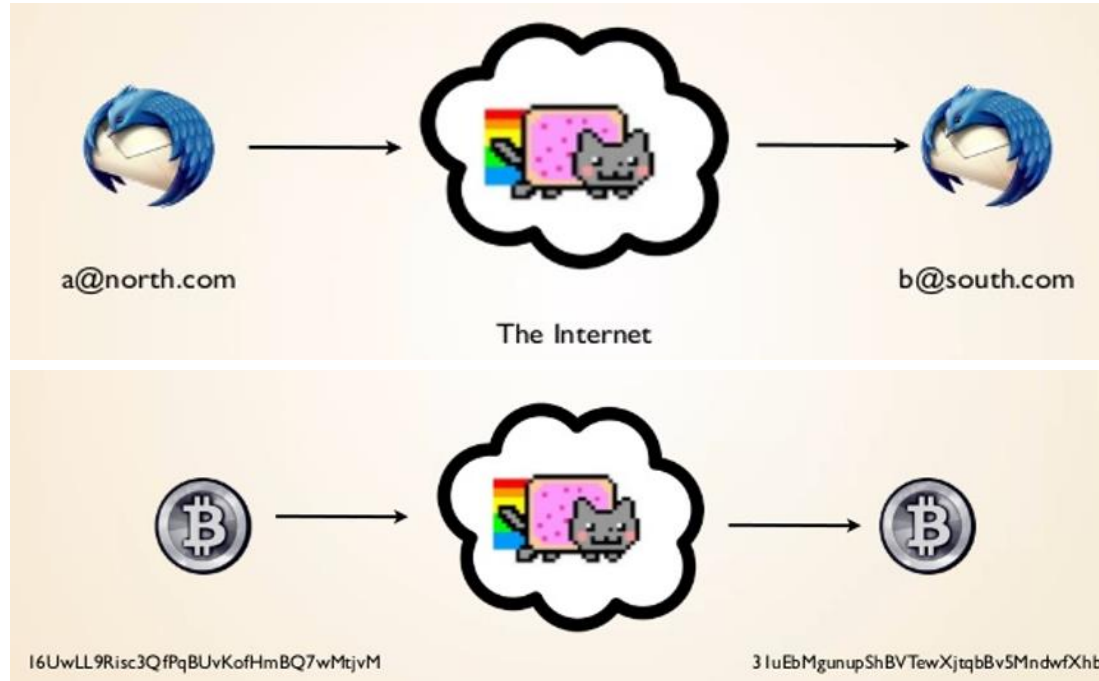




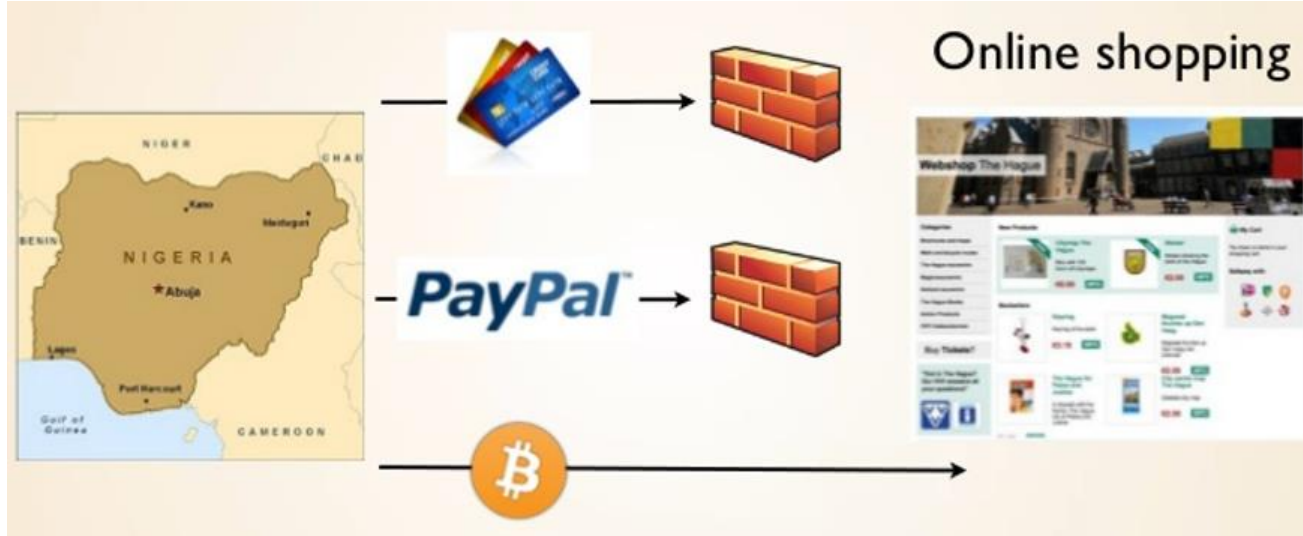
# What does a Bitcoins Wallet look like?



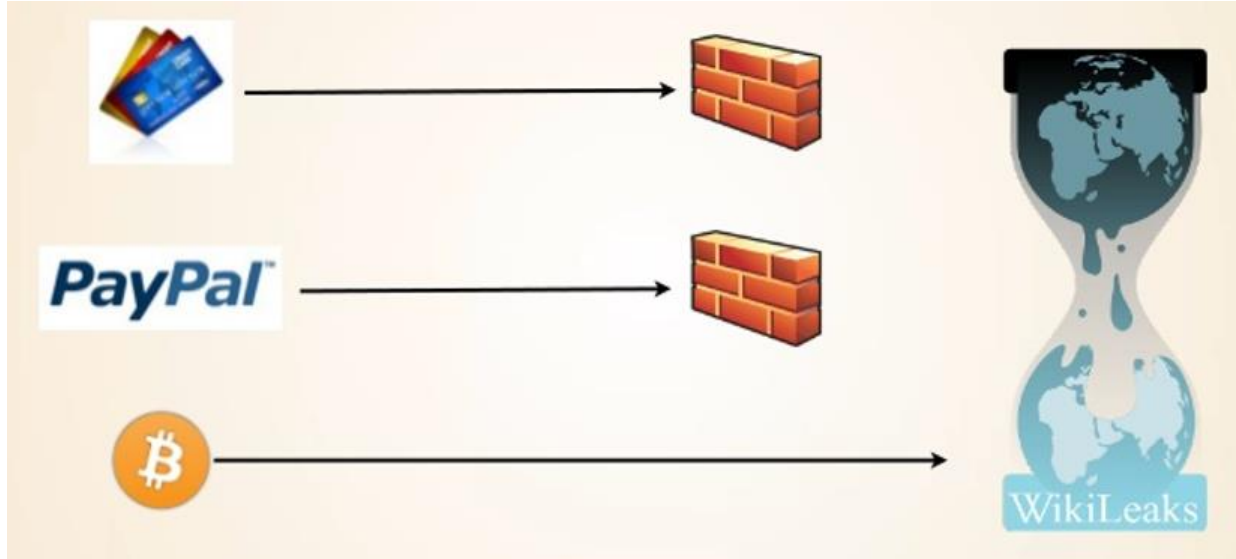
# Bitcoin is like email



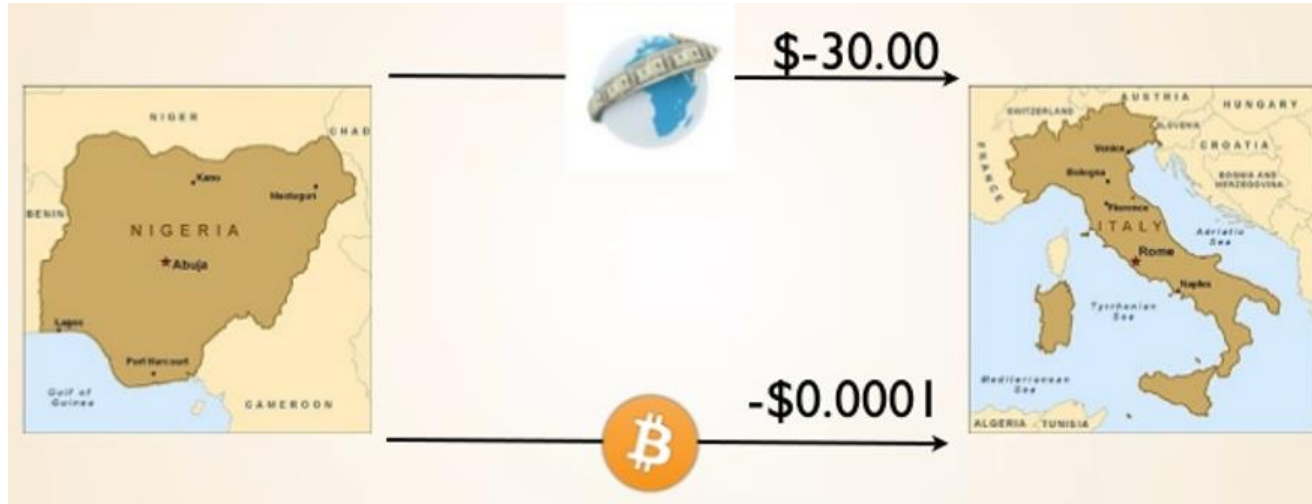
# Bitcoin is truly International



# Bitcoin is difficult to block



# Bitcoin is cheaper than wire transfer





# Where do Bitcoins come from?

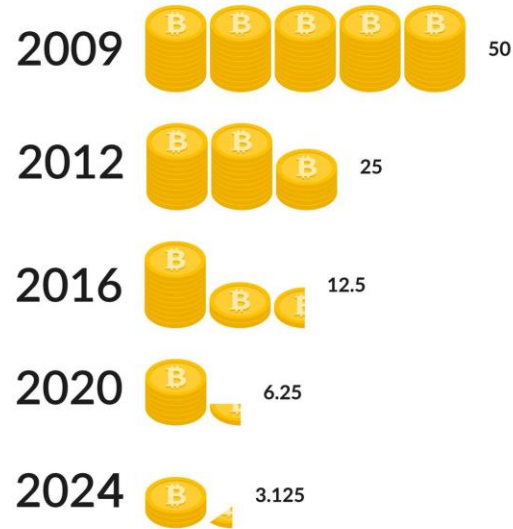


**Miners** - Generate new coins by solving maths problems



# Bitcoin has a limited supply – Ensuring value

## Bitcoin Halving





# What are Bitcoins worth?

HOME > BTC / GBP • CRYPTOCURRENCY

## Bitcoin to Pound sterling

17,473.31 ↓ 56.50% -22,694.13 1Y

Oct 10, 9:51:25 AM UTC · Disclaimer

1D 5D 1M 6M YTD 1Y 5Y MAX



- 10 Oct 2022



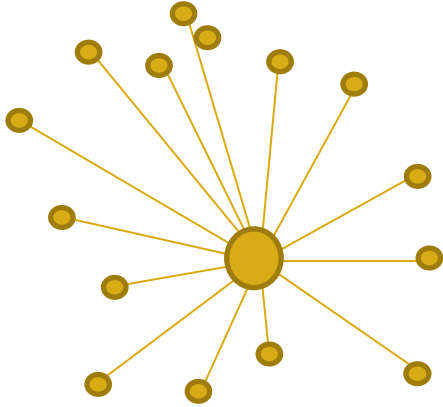
Institute  
and Faculty  
of Actuaries

# What are Bitcoins worth?

- 19 April 2023



# A Decentralised Currency



**CENTRALISED**

## Problem

Central point of failure

Expensive to secure

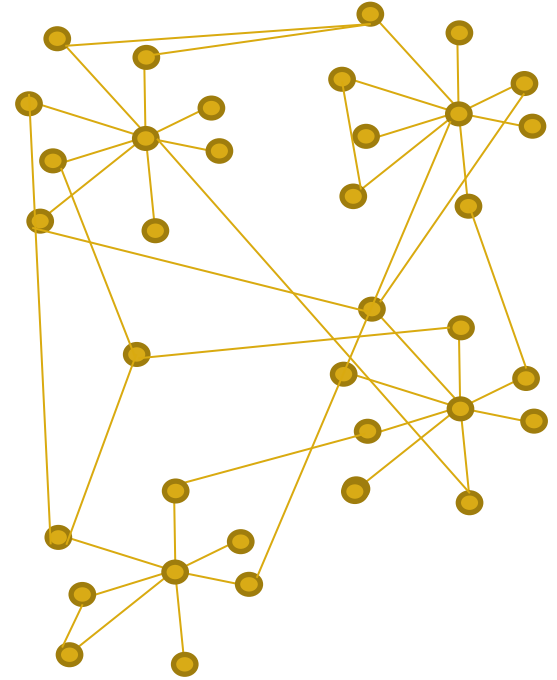
Trust who is in charge

## Solution

Decentralised network

Shared security cost

Trust a fixed set of rules



**DECENTRALISED**

# How to Get Bitcoin?

- ATM



- In Person exchange

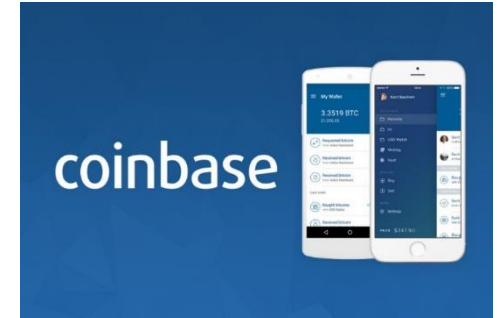


- Bank Transfer



Bank  
Transfer

- Crypto Exchange



# Difficulties

- 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 being ripped off
- Fake / corrupt exchange could take all your money

# Bitcoin & Crime

## Silk Road Case

Silk Road is an underground website, sometimes called the "Amazon.com of illegal drugs" or the "eBay for drugs". Silk Road had collected 9.5 million Bitcoin in revenue

Oct, 2013

The FBI cracked down on 'Silk Road', a website which sold



and other drugs paid for by Bitcoins.



'Silk Road' has carried out over

**\$1.2 billion**

worth of business



# BTC Mixers/Tumblers

- Scams / Trusted ??

## High volume bitcoin mixer



### YOUR TRUST IS OUR PRIORITY

CryptoMixer.io is the part of [Bitcoin community](#). We value our reputation and build it upon trust. We generate the "Letter of Guarantee" for each transaction, signed by our public address. Our reserves are publicly proven on BitcoinTalk (1, 2, 3). Our support works 24/7 and always ready to assist you. We are here to make your mixing experience better than ever!

Why should I mix my coins?

START

**BTC MIXERS**

# Interactive Questions

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



# 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
- Some gangs will sell your data to others to maximise profits

# 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 day
- The ransom payments may fund terrorism (Legal)

# 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.

# 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?)

# 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.

# 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;
  - (ii) the risks from paying the ransom; and
  - (iii) negotiation and payment options.

# 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.

# Considerations

- Passwords.
- Bitcoin transactions normally confirmed after 10 minutes.
- Consider buying some before kidnap?
- Use a ransomware negotiator:
  - MORE TIME
  - LESS MONEY
  - MORE INTELLIGENCE
  - LESS RISK



# Questions

# Comments

Contact me

## Richard Foster



[richard@brainstormsecurity.com](mailto:richard@brainstormsecurity.com)  
[www.brainstormsecurity.com](http://www.brainstormsecurity.com)



020 8058 0047

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



Institute  
and Faculty  
of Actuaries



Institute  
and Faculty  
of Actuaries

# THANK YOU

