



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**

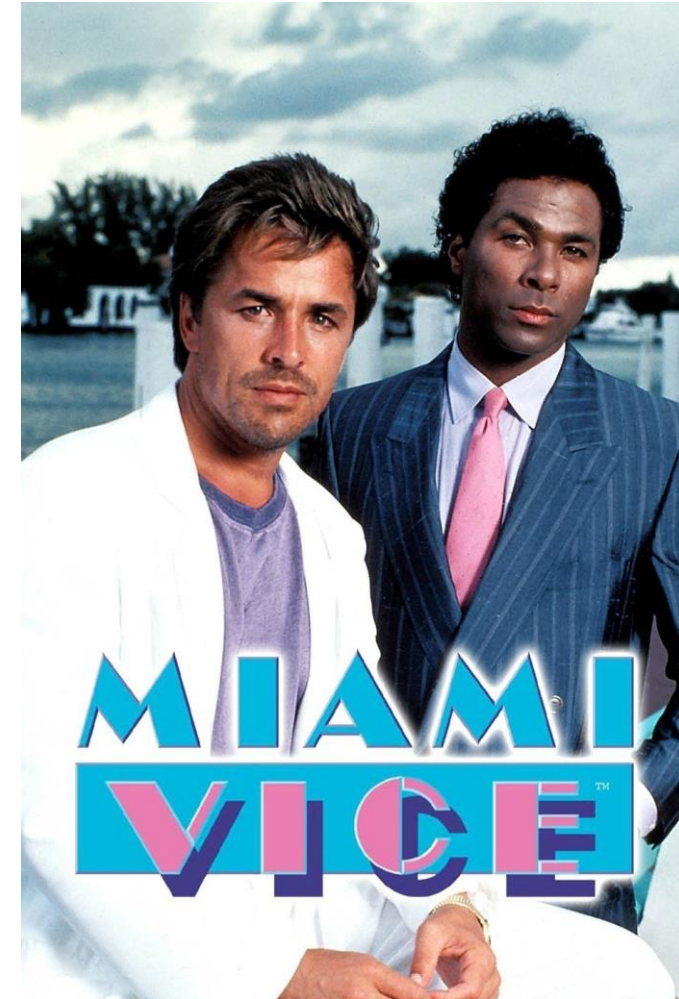


# About Me



Institute  
and Faculty  
of Actuaries

# About Me



Institute  
and Faculty  
of Actuaries

# My Career



10 Years



18 Years



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



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

- Items that can be bartered and are widely accepted.



# Money is: A Unit of Account

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



# Money is: A Store of Value

- 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
- Derives trust from known established mathematical properties.

The image shows a chalkboard with several mathematical formulas written in white chalk. The formulas are related to probability distributions and their derivatives. The most prominent formula is the derivative of the natural logarithm of a normal distribution's probability density function with respect to its mean parameter  $\mu$ . Other formulas include the derivative of the log-likelihood function with respect to the mean parameter, and the derivative of the moment-generating function with respect to the mean parameter.

$$\frac{\partial}{\partial \mu} \ln f_{\mu, \sigma^2}(\xi_1) = \frac{(\xi_1 - \mu)}{\sigma^2} f_{\mu, \sigma^2}(\xi_1) - \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(\xi_1 - \mu)^2}{2\sigma^2}\right\}$$
$$\int_{\mathcal{R}_n} T(x) \cdot \frac{\partial}{\partial \theta} f(x, \theta) dx = M\left(T(\xi) \cdot \frac{\partial}{\partial \theta} \ln L(\xi, \theta)\right)$$
$$\int_{\mathcal{R}_n} T(x) \cdot \left(\frac{\partial}{\partial \theta} \ln L(x, \theta)\right) \cdot f(x, \theta) dx = \int_{\mathcal{R}_n} T(x) \left(\frac{\partial \ln L(x, \theta)}{\partial \theta}\right) f(x, \theta) dx$$
$$\frac{\partial}{\partial \theta} M T(\xi) = \frac{\partial}{\partial \theta} \int_{\mathcal{R}_n} T(x) f(x, \theta) dx = \int_{\mathcal{R}_n} T(x) \frac{\partial f(x, \theta)}{\partial \theta} dx$$

# What do Bitcoins look like?

1454A2geTxaJwF8eqry7oLEcdomgDSj6Zx



## Public Key (“Address”)

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

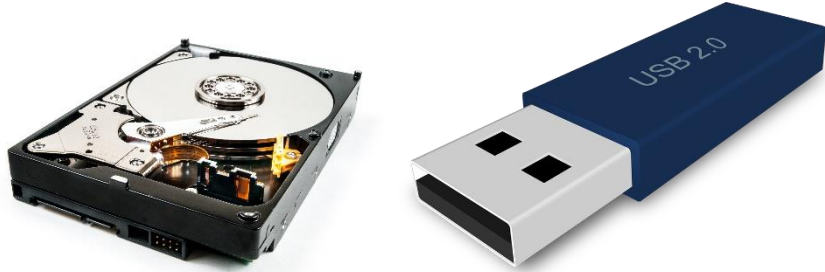
5JHkYd4mYkTsCsF5axnFj573PG6tqpeJ39Rz2M33vwBka4S1hu6



## Private Key

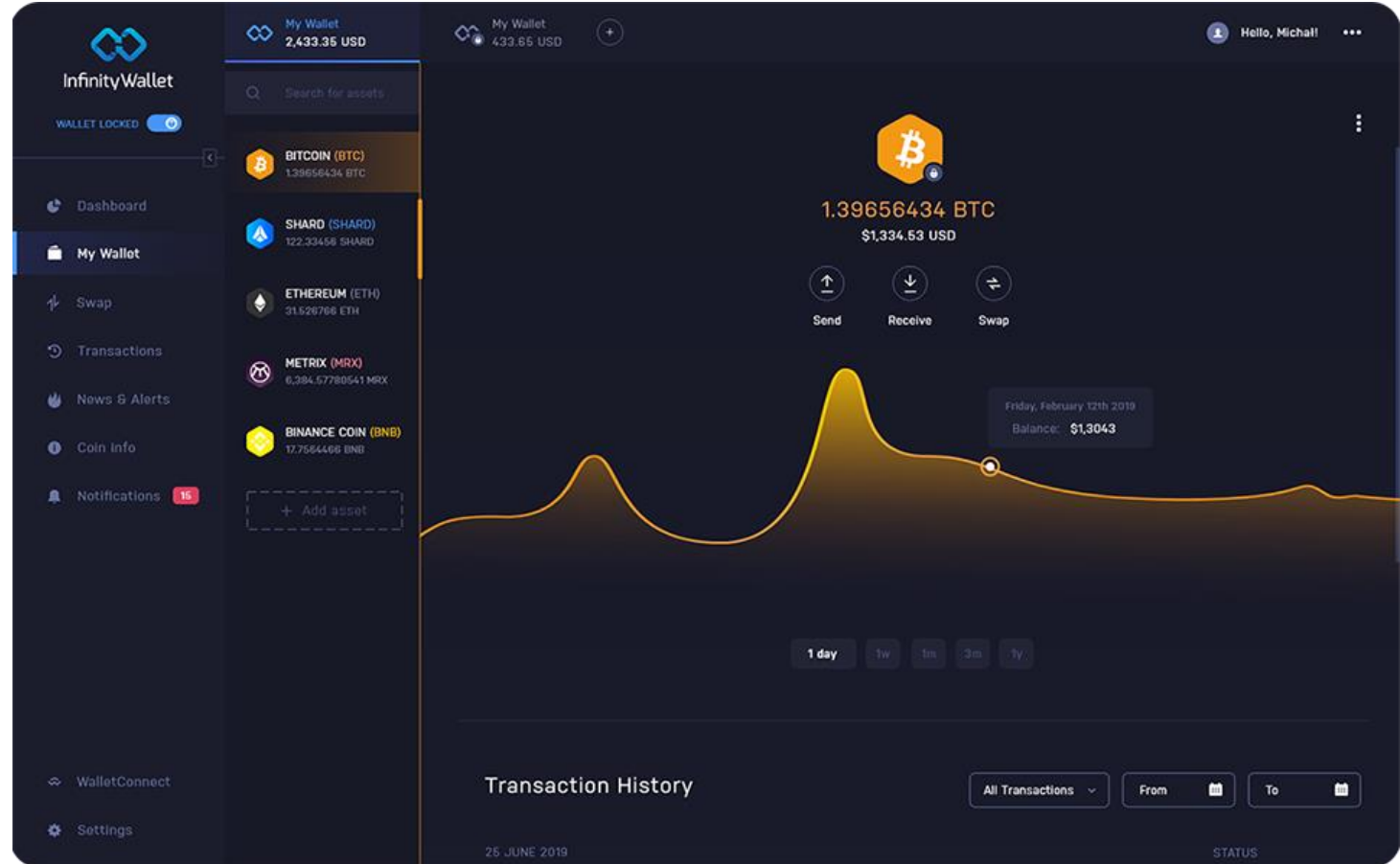
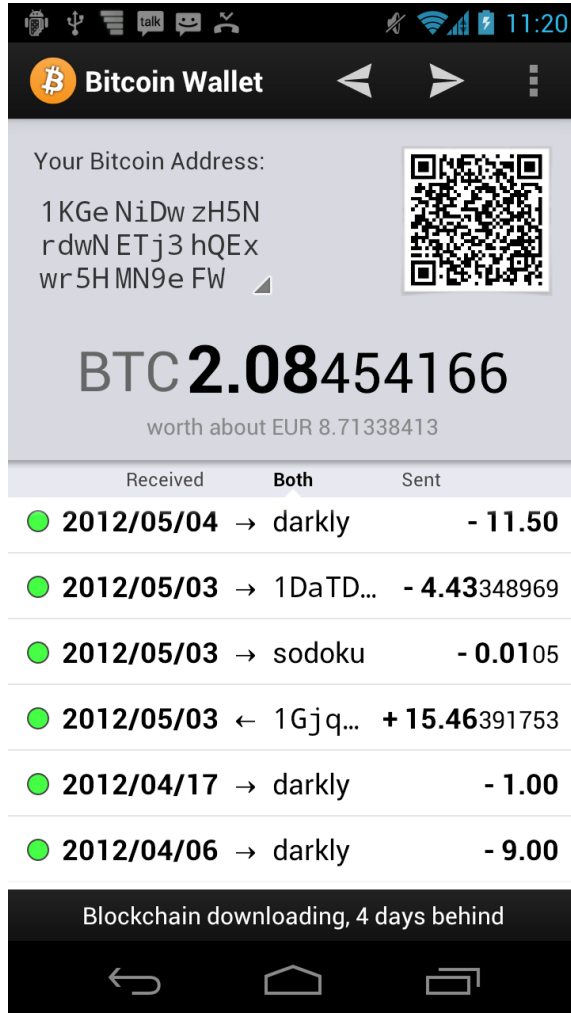
51 characters starting with **5**  
Required to transfer value from the address

# What do Bitcoins look like?

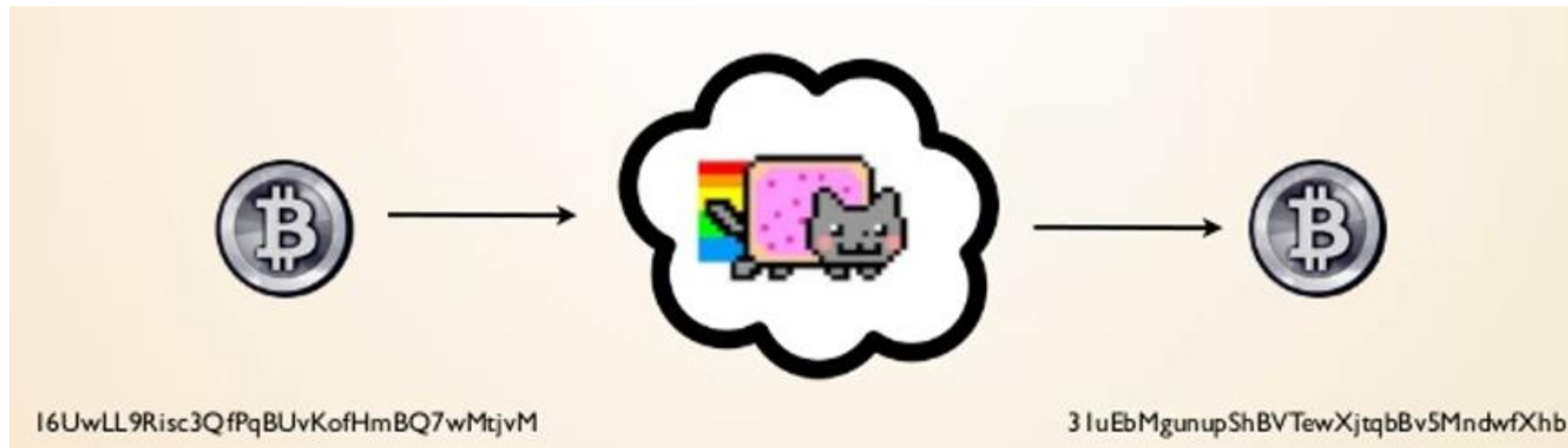
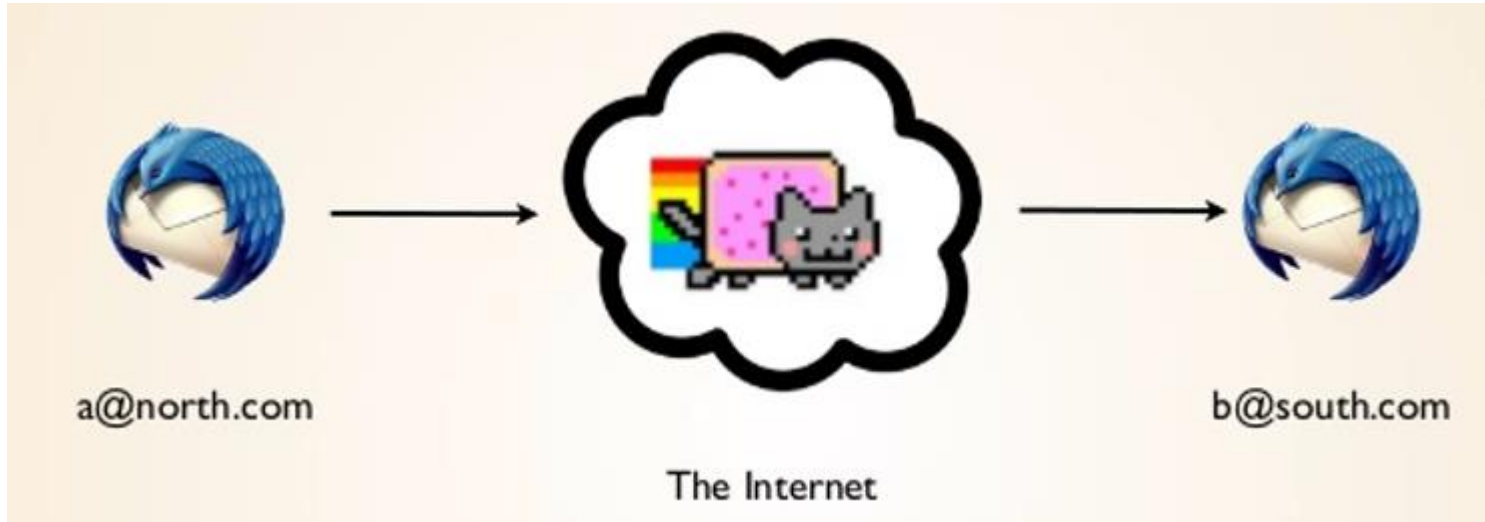




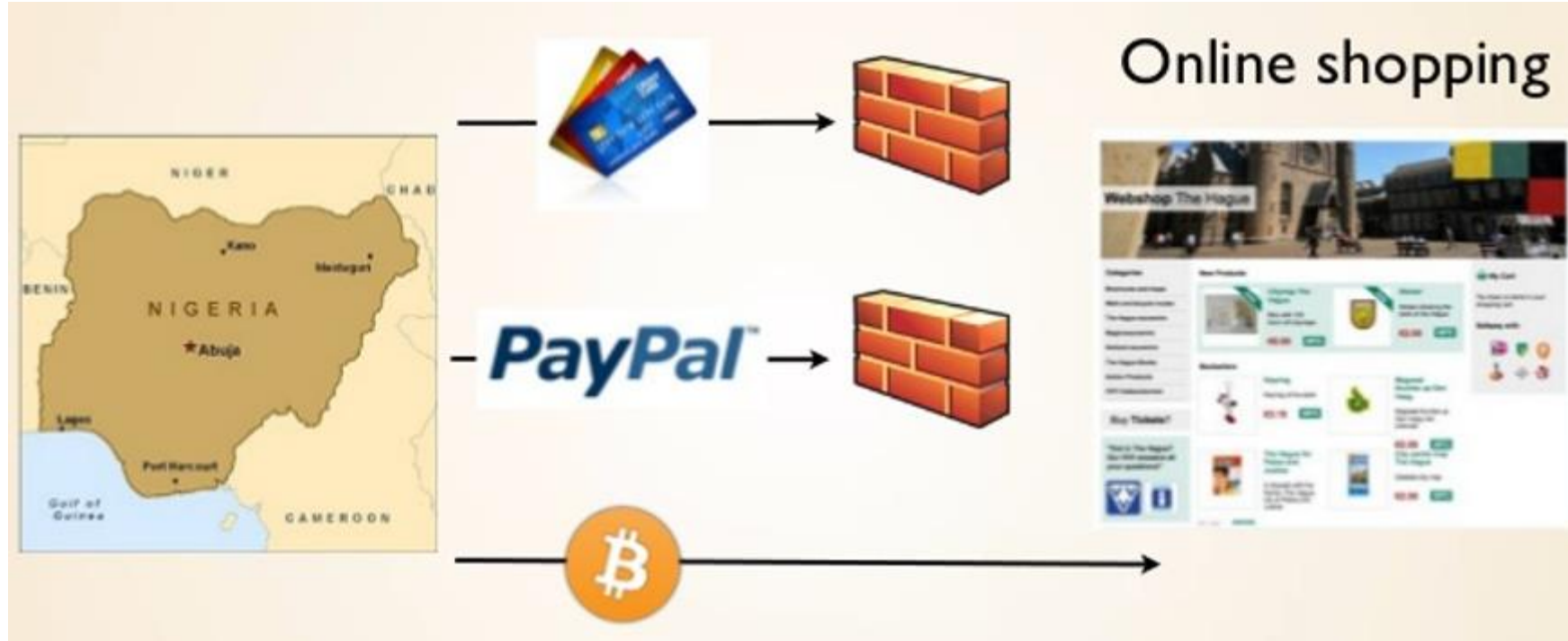
# What does a Bitcoins Wallet look like?



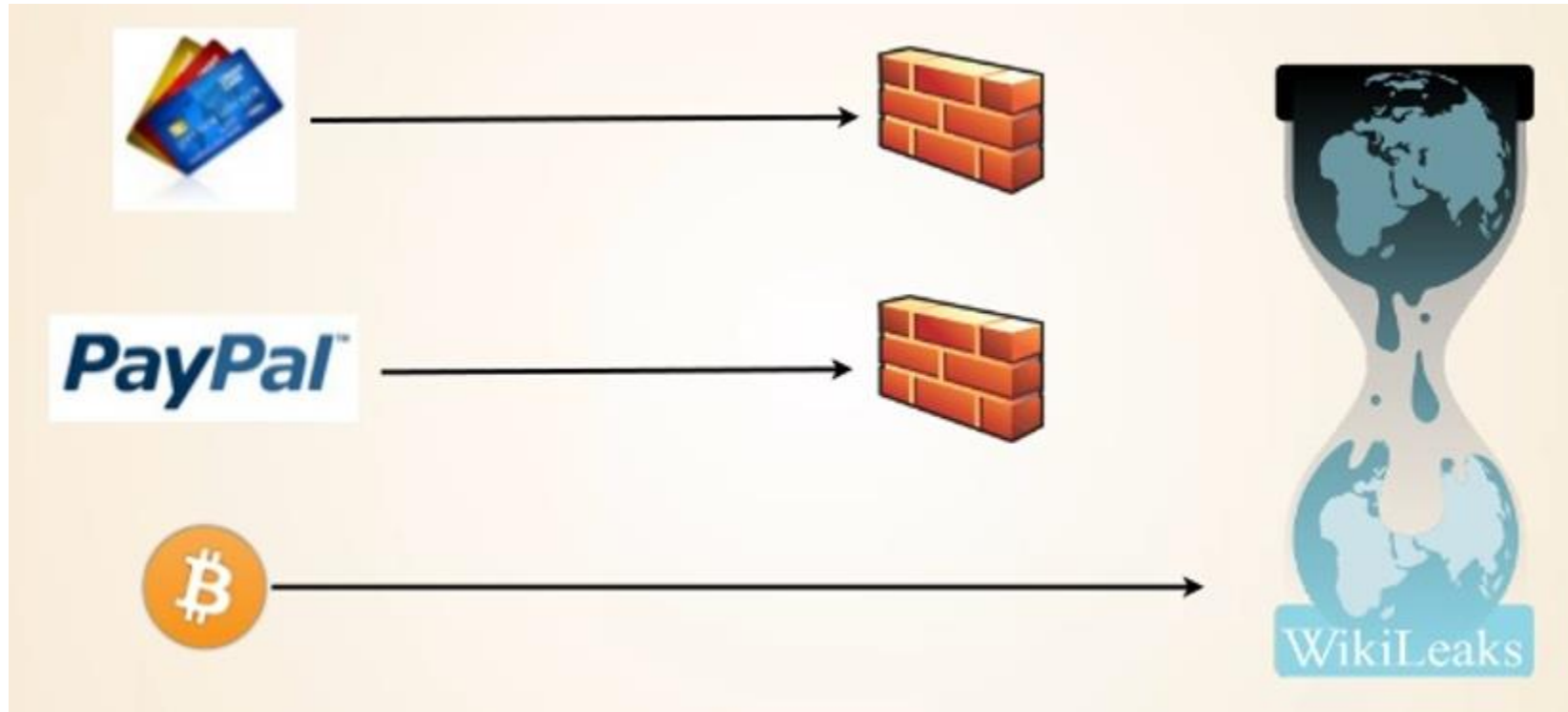
# Bitcoin is like email



# Bitcoin is truly International



# Bitcoin is difficult to block



# Bitcoin is cheaper than wire transfer



# Bitcoin is a ledger

DATE 1953	PAR- TICU- LARS	L.K.S INITIALS	DR.	CR.	DR. OR CR.	BALANCE	DATE 1953	PAR- TICU- LARS	L.K.S INITIALS	DR.	CR.	DR. OR CR.	BALANCE
Feb 23		Janin		41.52		41.52	June 30	Janin			20.97		20.97
March 17				24.85		116.37	July 4			1.00			
19			5.00				12 10				101.92		
			13.25							5.00			
23 July			56				18			50.00			
23			10.00				27 July			75			
24			17.75				Aug 29			2.95			
			10.85				Nov 29				25.00		
April 1			6.00				Dec 3				100.00		
			10.00							350.00			
12			17.00				8			10.00			
16 10				150.00			12			17.00			
19			128.80							45.00			
25			10.00				14 10				496.98		
28 July			1.00							21.80			
30 Oct 1953			1.06				Oct 1953			167.71			
				32.00			21			50.00			
June 7			10.00				21			20.00			
13			20.00				27			23.67			
24 10							Jan 5/6			28.10			
26 on note			120.82			20.97	10 10				946.69		965.99

BLOCKCHAIN info
 
[Home](#)
[Charts](#)
[Stats](#)
[Markets](#)
[API](#)
[Wallet](#)

## Home

Welcome to Blockchain More...

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
433904	4 minutes	2412	23,658.69 BTC	F2Pool	1,000
433903	11 minutes	2637	31,614.91 BTC	AntPool	998.21
433902	30 minutes	2190	28,647.85 BTC	85,214,105.80	934.43
433901	47 minutes	2067	15,586.04 BTC	AntPool	998.19
433900	53 minutes	2239	11,471.28 BTC	BW.COM	998.09
433899	57 minutes	2417	28,010.53 BTC	BW.COM	998.2

### Latest Transactions

72b4844e0fa18ccc2ca41	< 1 minute	2.3246805 BTC
8ce535065a3398701b0241cb0...	< 1 minute	10.74666309 BTC
98c7d4320d7d75276f2e079bf...	< 1 minute	0.0060822 BTC
f4c8f01e1aca3bc1535b984bc...	< 1 minute	0.41773383 BTC
badf023645d4bf958539e53b7...	< 1 minute	0.00530779 BTC
b1a654c295b94cfc71f701a3...	< 1 minute	7.81056045 BTC
d6f84f5ea565041f9eae053be...	< 1 minute	1.85028794 BTC
5bacbae73d0d4f85712c17394...	< 1 minute	0.3242867 BTC
94e3620f02549a8e597350a5e...	< 1 minute	11.40987309 BTC

### Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Search

### NEWS

- Magnr - Bitcoin Trading Platform | Trade with Leverage**  
Magnr ← 1 minute ago  
Big numbers don't mean big money  
[/r/btc 1 minute ago](#)  
Learn from Kore's downfall, support many clients!  
[/r/btc 10 minutes ago](#)
- Joe Weisenthal on Twitter: Yuan vs. Bitcoin**  
[/r/bitcoin 10 minutes ago](#)
- MasterCard Rolls Out Selfie Payments Decreasing Privacy One Step Further**  
CoinTelegraph 15 minutes ago
- The First Service Allowing Russian Online Shops To Accept Bitcoin**  
[/r/bitcoin 26 minutes ago](#)
- Russian deputy finance minister: Bitcoin poses no threat to Russia's financial system**  
[/r/bitcoin 35 minutes ago](#)

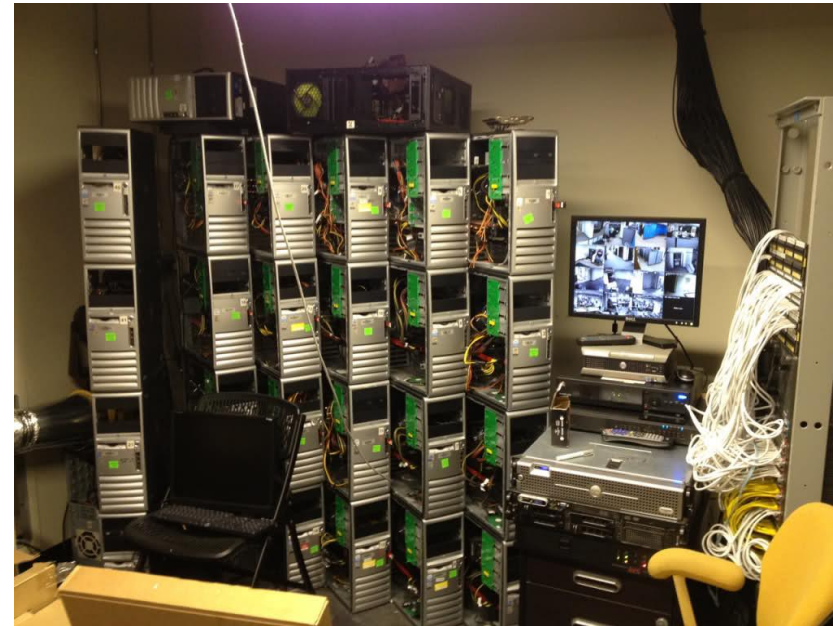


Institute and Faculty of Actuaries

# Where do Bitcoins come from?

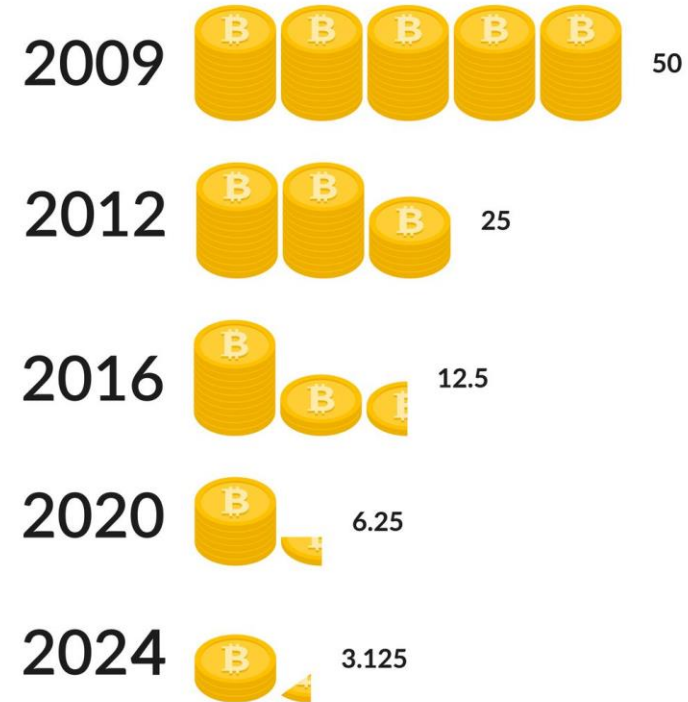


**Miners** - Generate new coins by solving maths problems



# 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

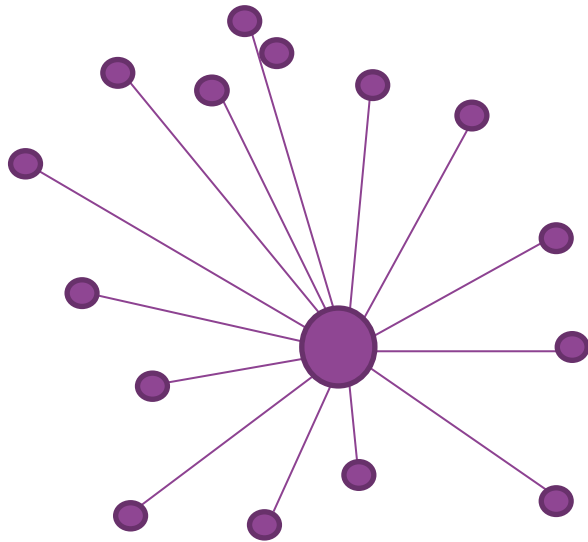
Oct 10, 9:51:25 AM UTC · Disclaimer

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



- 10 Oct 2022

# A Decentralised Currency



**CENTRALISED**

## Problem

Central point of failure

Expensive to secure

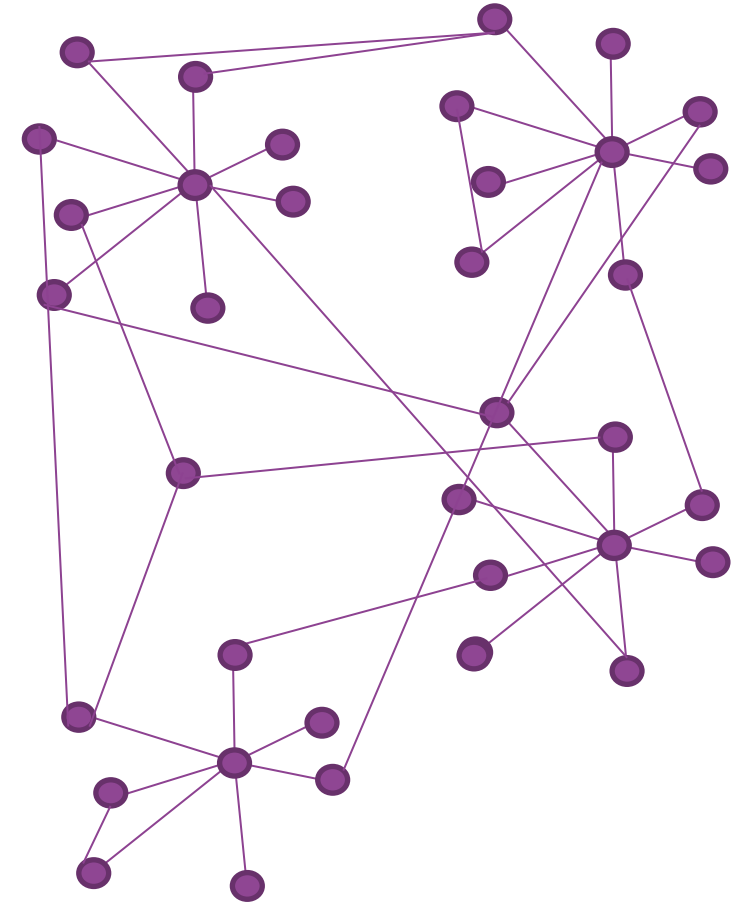
Trust who is in charge

## Solution

Decentralised network

Shared security cost

Trust a fixed set of rules



**DECENTRALISED**

# How to Get Bitcoin?

- ATM



- In Person exchange

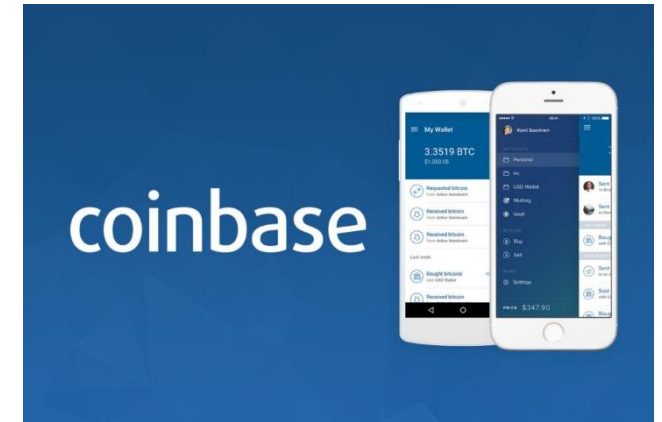


- Bank Transfer



Bank  
Transfer

- Crypto Exchange



# Difficulties 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

# 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



COCAINE



HEROIN



METHAMPHETAMINES

and other drugs paid for by Bitcoins.

Between

Feb  
2011

'Silk Road' has carried out over **\$1.2 billion** worth of business

Jul  
2013

# 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**

# 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	

# Interactive Questions

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



Institute  
and Faculty  
of Actuaries



## Interactive Questions

Who carries out  
cyber attacks?

Nation states

Hacking / Crime groups

 Youngsters and lone-actors

## 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.



## Interactive Questions

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

- Training
- Cyber Essentials
- Backups
- Planning

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



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



# 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)

# 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 (and is backup data available?);
  - (ii) The risks (inc reputation) 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

## 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](mailto:richard@brainstormsecurity.com)



020 8058 0047



[www.brainstormsecurity.com](http://www.brainstormsecurity.com)

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



Institute  
and Faculty  
of Actuaries



Institute  
and Faculty  
of Actuaries

# Thank you



**#GiroConf22**