Blockchain and Ransomware - Friend or Foe ?

InTech Forums Briefing – Ransomware will impact your business
09 March 2017

Gary Nuttall
Managing Director

Distlytics

Distributed Ledger Analytics
Consultancy & Insight

Agenda

1. Introductions
2. Foe?
3. Targets
4. Vectors
5. Blockchain Primer
6. Friend
7. Q & A

Agenda

1. **Introductions**
2. Foe?
3. Targets
4. Vectors
5. Blockchain Primer
6. Friend
7. Q & A

1 - Introduction: Me

Gary Nuttall MBCS CITP

Managing Director at Distlytics Ltd

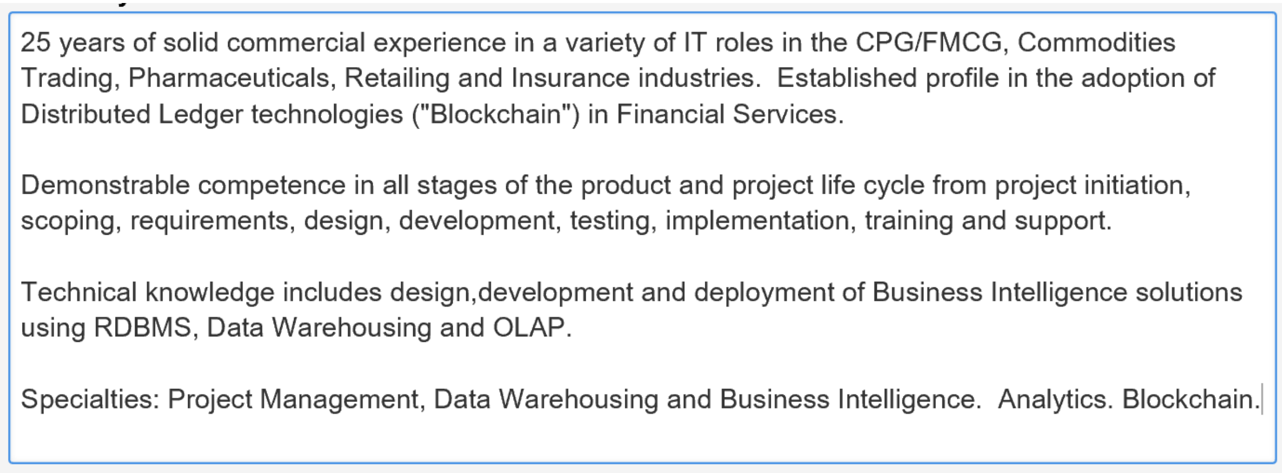
London, United Kingdom | Information Technology and Services

Previous	Chaucer Syndicates Ltd, Trafigura Ltd, E. & J. Gallo Winery Europe
Education	ISEB Diploma in Business Analysis

Distlytics

Distributed Ledger Analytics

Consultancy & Insight

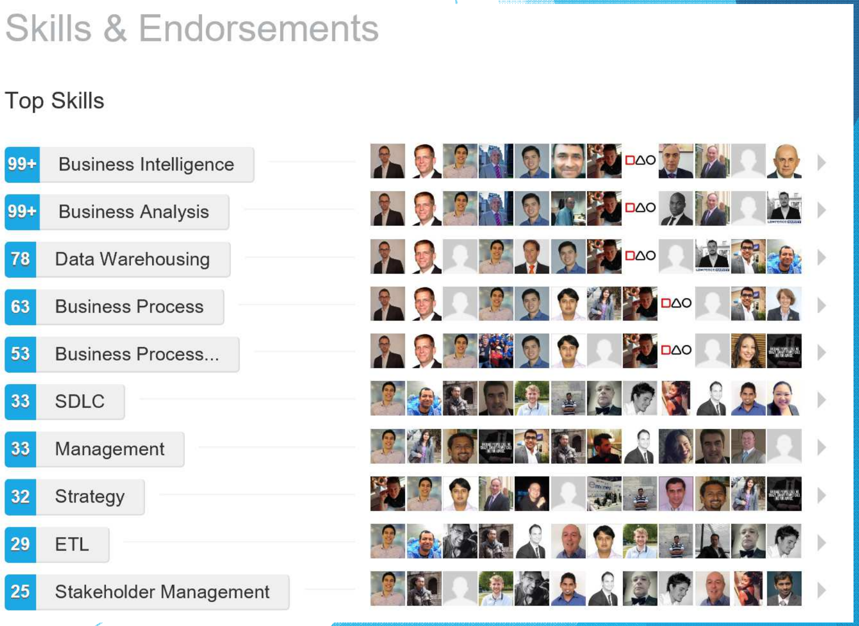


25 years of solid commercial experience in a variety of IT roles in the CPG/FMCG, Commodities Trading, Pharmaceuticals, Retailing and Insurance industries. Established profile in the adoption of Distributed Ledger technologies ("Blockchain") in Financial Services.

Demonstrable competence in all stages of the product and project life cycle from project initiation, scoping, requirements, design, development, testing, implementation, training and support.

Technical knowledge includes design,development and deployment of Business Intelligence solutions using RDBMS, Data Warehousing and OLAP.

Specialties: Project Management, Data Warehousing and Business Intelligence. Analytics. Blockchain.



Skills & Endorsements

Top Skills

99+	Business Intelligence
99+	Business Analysis
78	Data Warehousing
63	Business Process
53	Business Process...
33	SDLC
33	Management
32	Strategy
29	ETL
25	Stakeholder Management

Caveat: Please read the small print…

This presentation reflects my personal views and is not intended to reflect the views of past, current and prospective employers, clients or other agents.

"Prediction is very difficult, especially if it's about the future."

Nils Bohr, Nobel laureate in Physics

1 - Introduction: You

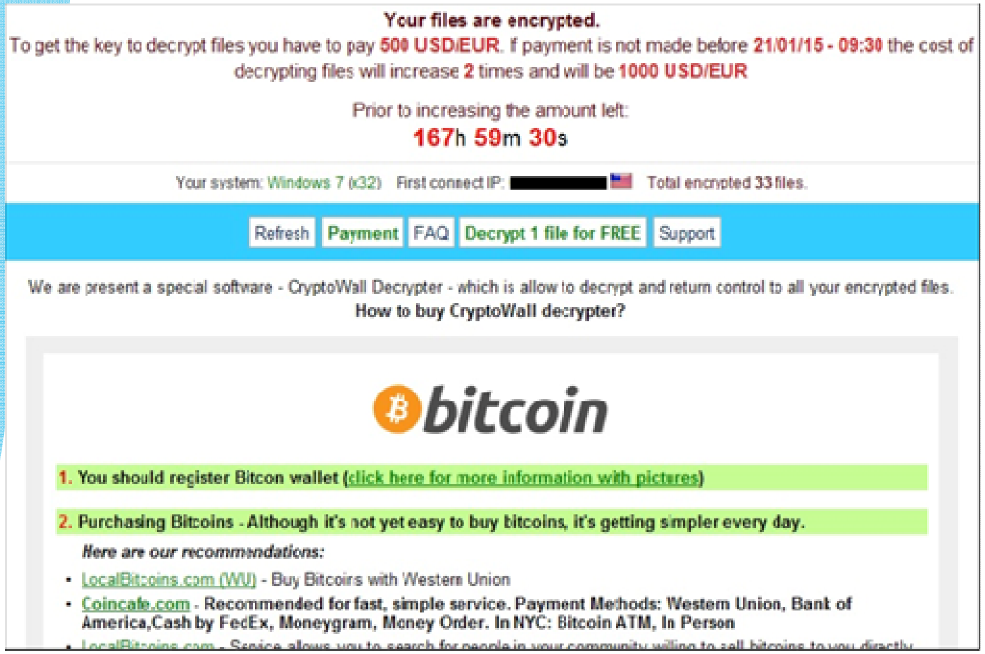
What do you know about Blockchain ?

Are you a Developer, Designer, Manager, Techie, CTO, CISO, Underwriter, Broker, “Business/User” ?

Agenda

1. Introductions
2. **Foe?**
3. Targets
4. Vectors
5. Blockchain Primer
6. Friend
7. Q & A

Foe ?



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **21/01/15 - 09:30** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

167h **59**m **30**s

Your system: Windows 7 (x32) First connect IP: [redacted] Total encrypted 33 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

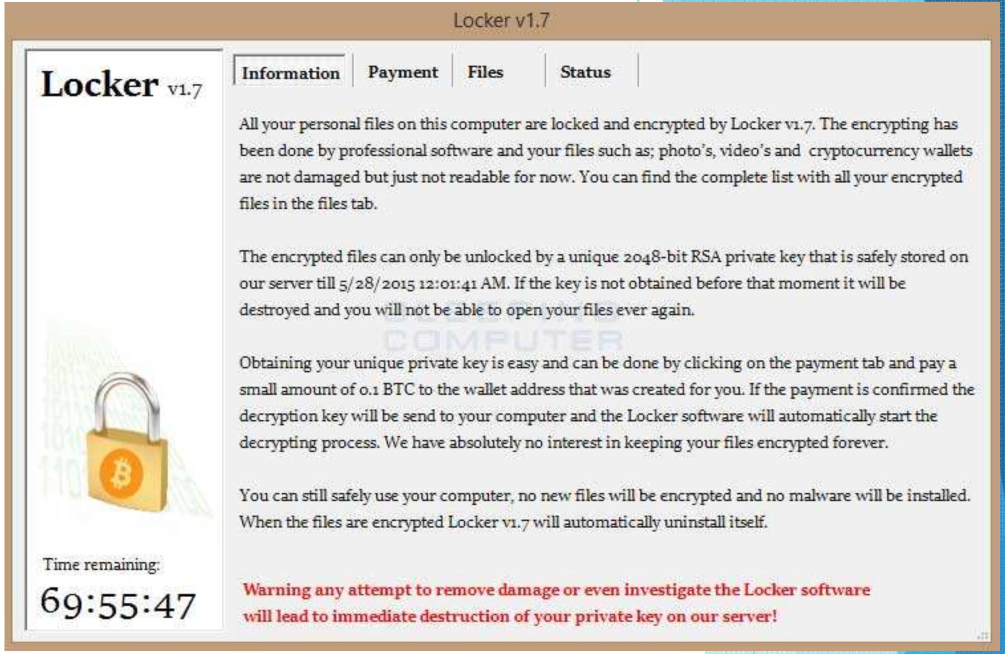
How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.



Locker v1.7

All your personal files on this computer are locked and encrypted by Locker v1.7. The encrypting has been done by professional software and your files such as; photo's, video's and cryptocurrency wallets are not damaged but just not readable for now. You can find the complete list with all your encrypted files in the files tab.

The encrypted files can only be unlocked by a unique 2048-bit RSA private key that is safely stored on our server till 5/28/2015 12:01:41 AM. If the key is not obtained before that moment it will be destroyed and you will not be able to open your files ever again.

Obtaining your unique private key is easy and can be done by clicking on the payment tab and pay a small amount of 0.1 BTC to the wallet address that was created for you. If the payment is confirmed the decryption key will be send to your computer and the Locker software will automatically start the decrypting process. We have absolutely no interest in keeping your files encrypted forever.

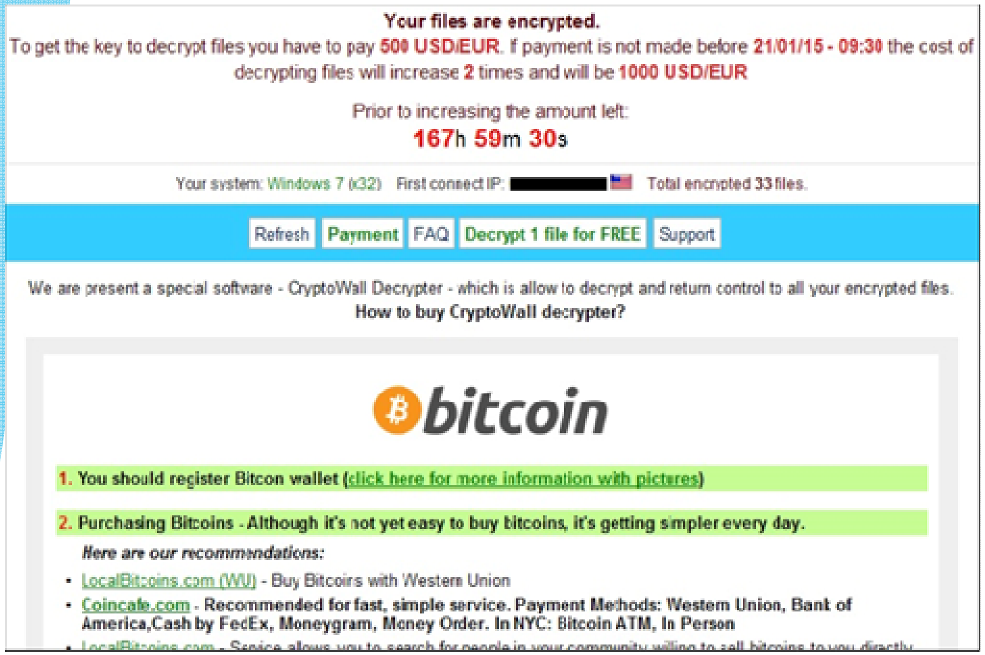
You can still safely use your computer, no new files will be encrypted and no malware will be installed. When the files are encrypted Locker v1.7 will automatically uninstall itself.

Time remaining:

69:55:47

Warning any attempt to remove damage or even investigate the Locker software will lead to immediate destruction of your private key on our server!

Foe ?



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **21/01/15 - 09:30** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:
167h **59**m **30**s

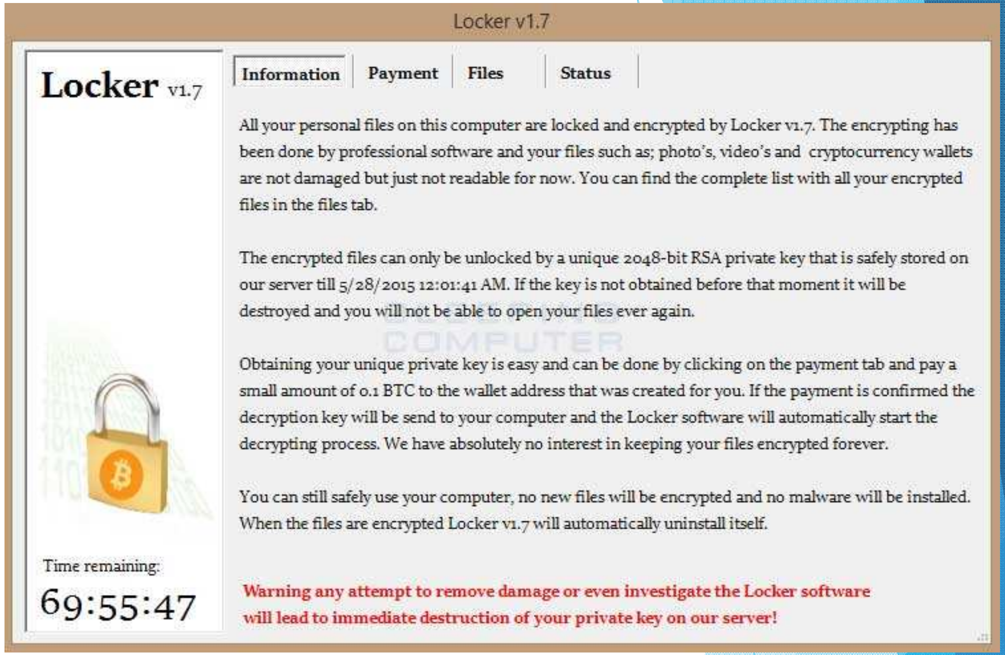
Your system: Windows 7 (x32) First connect IP: [redacted] Total encrypted 33 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

1. **You should register Bitcon wallet (click here for more information with pictures)**
2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly



Locker v1.7

All your personal files on this computer are locked and encrypted by Locker v1.7. The encrypting has been done by professional software and your files such as; photo's, video's and cryptocurrency wallets are not damaged but just not readable for now. You can find the complete list with all your encrypted files in the files tab.

The encrypted files can only be unlocked by a unique 2048-bit RSA private key that is safely stored on our server till 5/28/2015 12:01:41 AM. If the key is not obtained before that moment it will be destroyed and you will not be able to open your files ever again.

Obtaining your unique private key is easy and can be done by clicking on the payment tab and pay a small amount of 0.1 BTC to the wallet address that was created for you. If the payment is confirmed the decryption key will be send to your computer and the Locker software will automatically start the decrypting process. We have absolutely no interest in keeping your files encrypted forever.

You can still safely use your computer, no new files will be encrypted and no malware will be installed. When the files are encrypted Locker v1.7 will automatically uninstall itself.

Time remaining:
69:55:47

Warning any attempt to remove damage or even investigate the Locker software will lead to immediate destruction of your private key on our server!

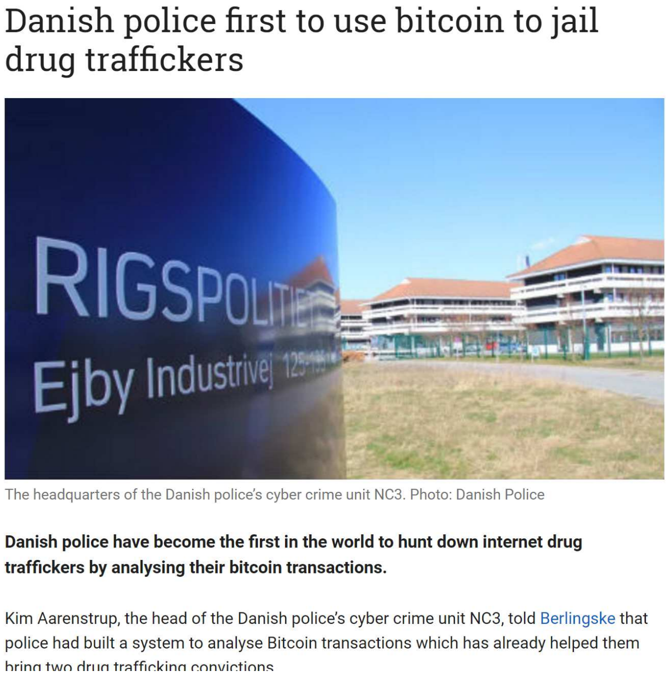
- Off the books
- Untraceable
- Nobody will know ☺
- Preferred payment channel of hackers as it's anonymous

Foe ?

- Off the books
- Untraceable
- Nobody will know ☺
- Preferred payment channel of hackers as it’s anonymous

Foe ?

- Off the books
- Untraceable
- Nobody will know ☺
- Preferred payment channel of hackers as it’s anonymous

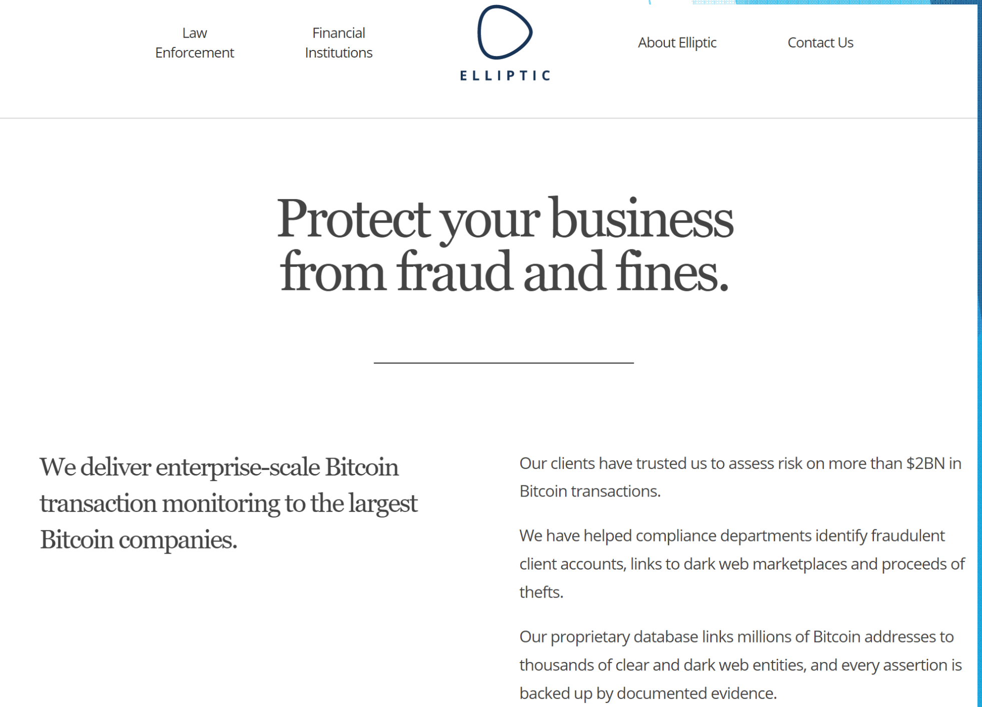


Danish police first to use bitcoin to jail drug traffickers

The headquarters of the Danish police’s cyber crime unit NC3. Photo: Danish Police

Danish police have become the first in the world to hunt down internet drug traffickers by analysing their bitcoin transactions.

Kim Aarenstrup, the head of the Danish police’s cyber crime unit NC3, told Berlingske that police had built a system to analyse Bitcoin transactions which has already helped them bring two drug trafficking convictions



Protect your business from fraud and fines.

We deliver enterprise-scale Bitcoin transaction monitoring to the largest Bitcoin companies.

Our clients have trusted us to assess risk on more than $2BN in Bitcoin transactions.

We have helped compliance departments identify fraudulent client accounts, links to dark web marketplaces and proceeds of thefts.

Our proprietary database links millions of Bitcoin addresses to thousands of clear and dark web entities, and every assertion is backed up by documented evidence.

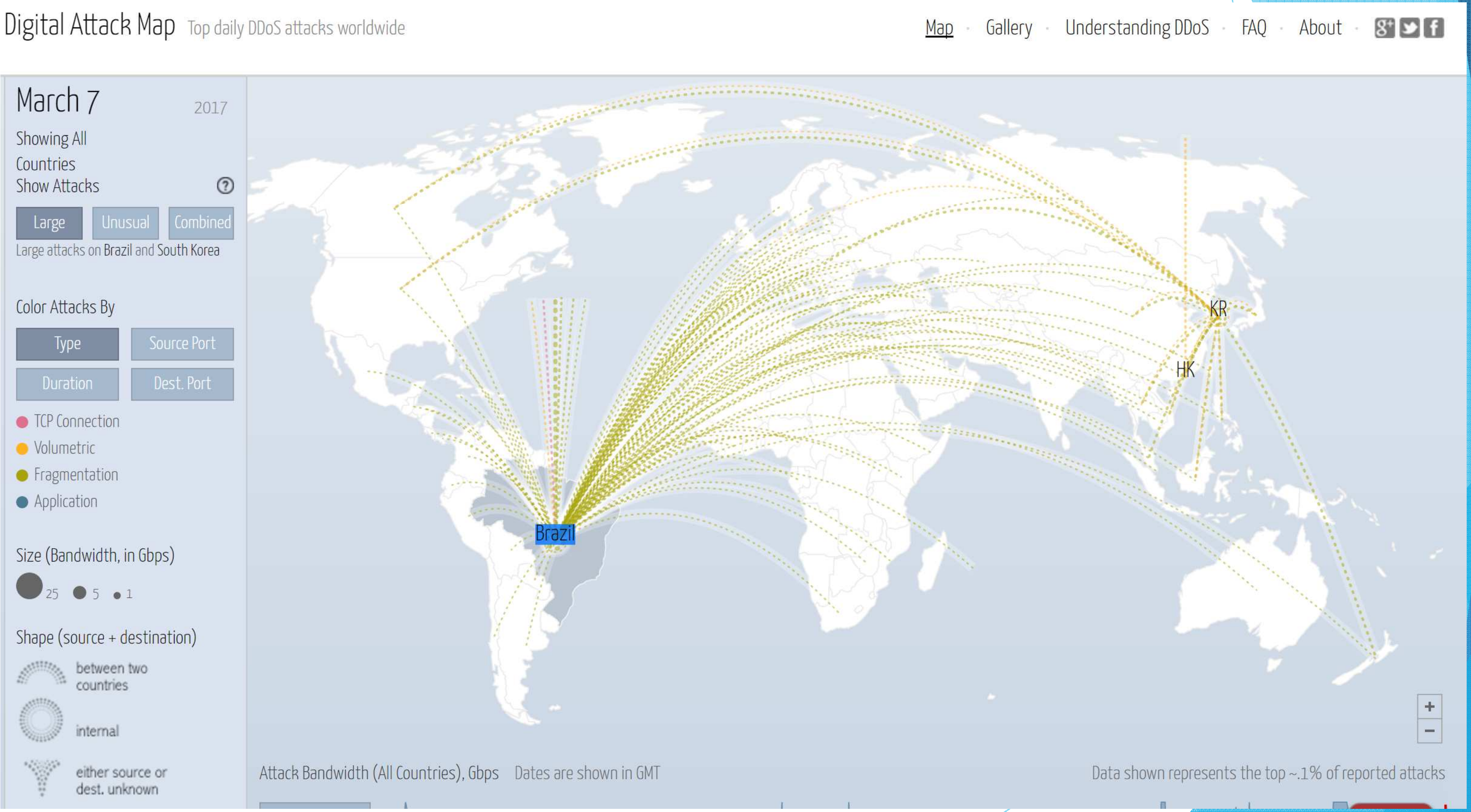
Agenda

1. Introductions
2. Foe?
3. **Targets**
4. Vectors
5. Blockchain Primer
6. Friend
7. Q & A

3 – Targets - DDoS

```
Sorry – System is unavailable
Please try again later
```

3 – Targets - DDoS



Digital Attack Map Top daily DDoS attacks worldwide

Map · Gallery · Understanding DDoS · FAQ · About

March 7 2017

Showing All Countries

Show Attacks

Large | Unusual | Combined

Large attacks on Brazil and South Korea

Color Attacks By

Type | Source Port | Duration | Dest. Port

- ● TCP Connection
- ● Volumetric
- ● Fragmentation
- ● Application

Size (Bandwidth, in Gbps)

● 25 ● 5 ● 1

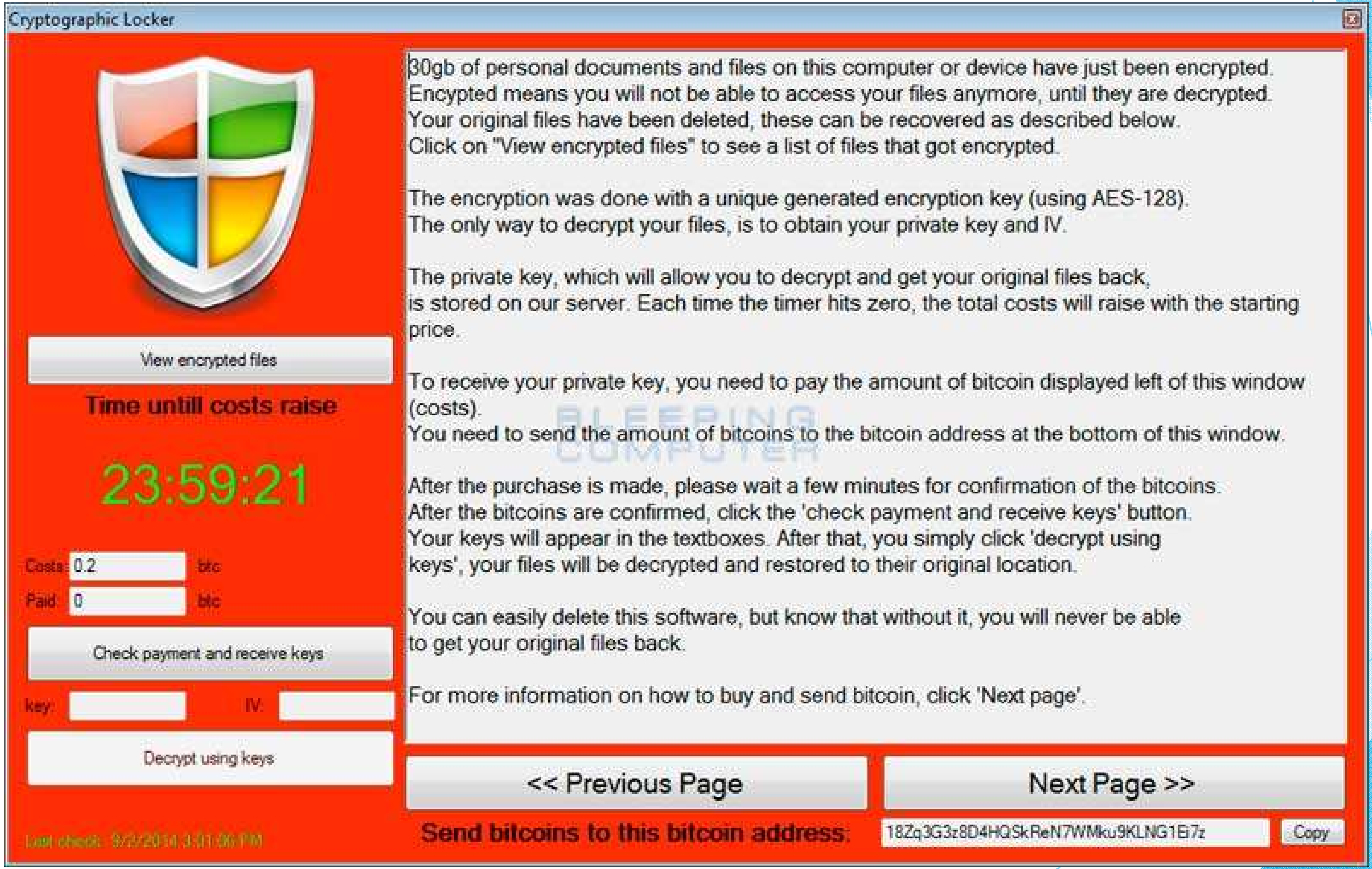
Shape (source + destination)

- between two countries
- internal
- either source or dest. unknown

Attack Bandwidth (All Countries), Gbps Dates are shown in GMT

Data shown represents the top ~.1% of reported attacks

3 – Targets – Data Encryption



30gb of personal documents and files on this computer or device have just been encrypted.
Encrypted means you will not be able to access your files anymore, until they are decrypted.
Your original files have been deleted, these can be recovered as described below.
Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-128).
The only way to decrypt your files, is to obtain your private key and IV.

The private key, which will allow you to decrypt and get your original files back, is stored on our server. Each time the timer hits zero, the total costs will raise with the starting price.

To receive your private key, you need to pay the amount of bitcoin displayed left of this window (costs).
You need to send the amount of bitcoins to the bitcoin address at the bottom of this window.

After the purchase is made, please wait a few minutes for confirmation of the bitcoins.
After the bitcoins are confirmed, click the 'check payment and receive keys' button.
Your keys will appear in the textboxes. After that, you simply click 'decrypt using keys', your files will be decrypted and restored to their original location.

You can easily delete this software, but know that without it, you will never be able to get your original files back.

For more information on how to buy and send bitcoin, click 'Next page'.

Time untill costs raise

23:59:21

Costs: 0.2 btc

Paid: 0 btc

key:

IV:

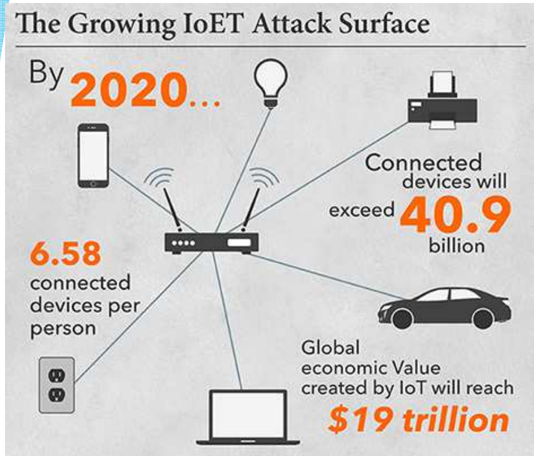
Last check: 9/2/2014 3:01:36 PM

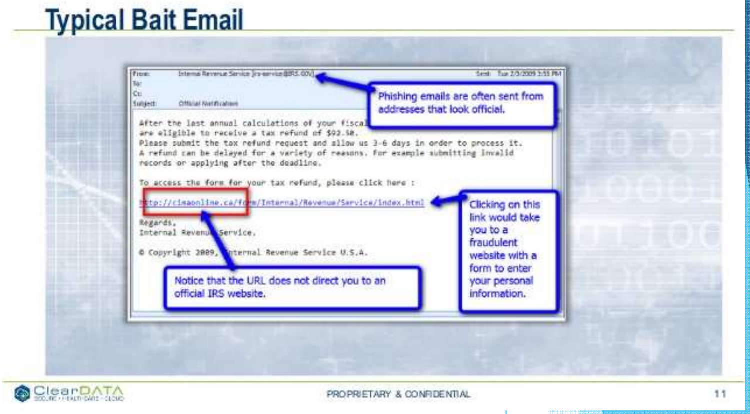
Send bitcoins to this bitcoin address: 18Zq3G3z8D4HQSkReN7WMku9KLNG1Ei7z

Agenda

1. Introductions
2. Foe?
3. Targets
4. **Vectors**
5. Blockchain Primer
6. Friend
7. Q & A

Vectors


The Growing IoET Attack Surface
By 2020...
Connected devices will exceed 40.9 billion
6.58 connected devices per person
Global economic Value created by IoT will reach $19 trillion



Typical Bail Email

From: Internal Revenue Service [irs-service@IRS.GOV] Sent: Tue 2/3/2009 3:55 PM
To:
Cc:
Subject: Official Notification

```
After the last annual calculations of your fiscal
are eligible to receive a tax refund of $92.50.
Please submit the tax refund request and allow us 3-6 days in order to process it.
A refund can be delayed for a variety of reasons. For example submitting invalid
records or applying after the deadline.

To access the form for your tax refund, please click here :

http://cimaonline.ca/form/Internal/Revenue/Service/index.html

Regards,
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.
```

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

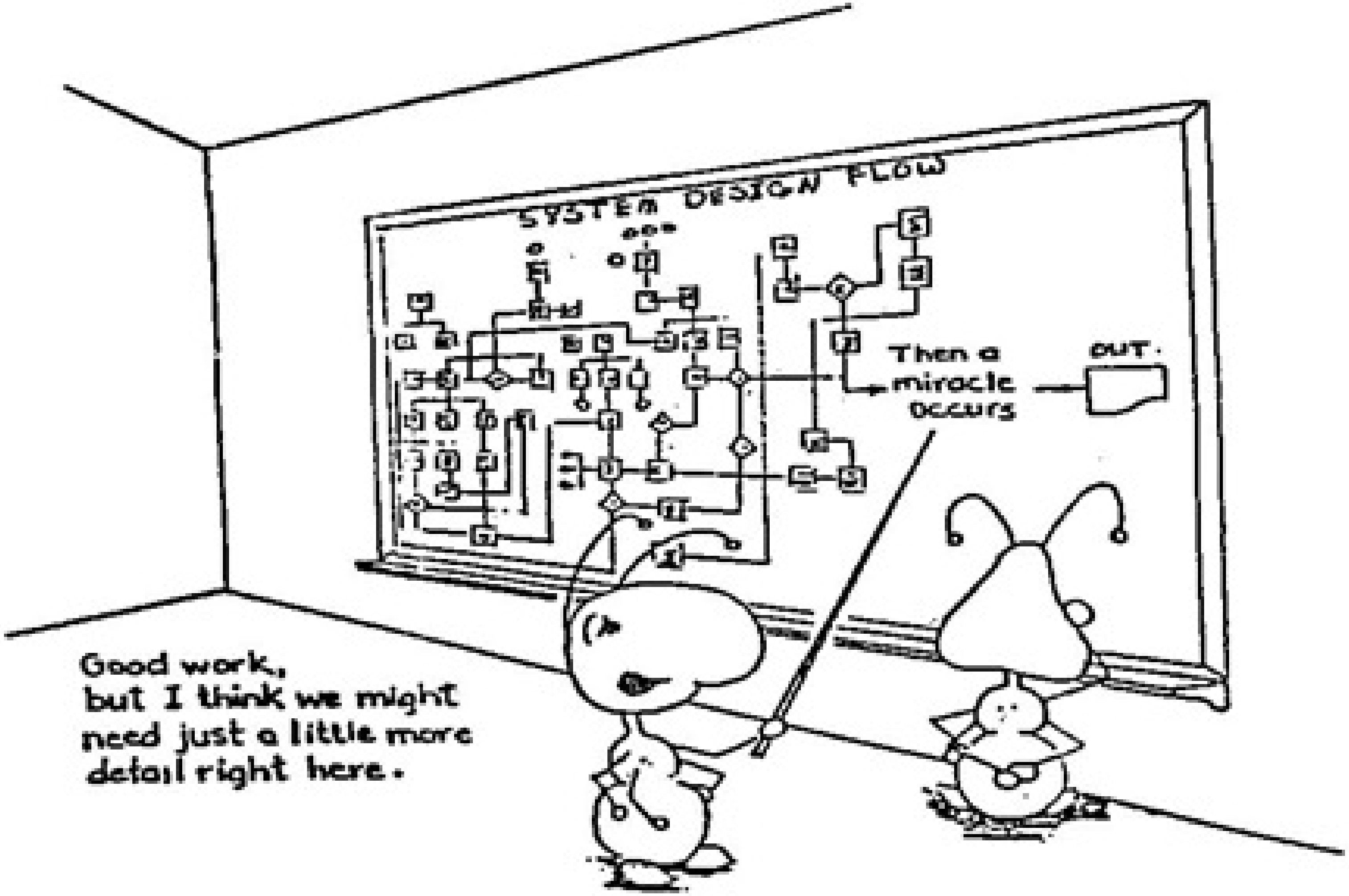
Notice that the URL does not direct you to an official IRS website.

ClearDATA SECURE · HEALTHCARE · CLOUD PROPRIETARY & CONFIDENTIAL 11

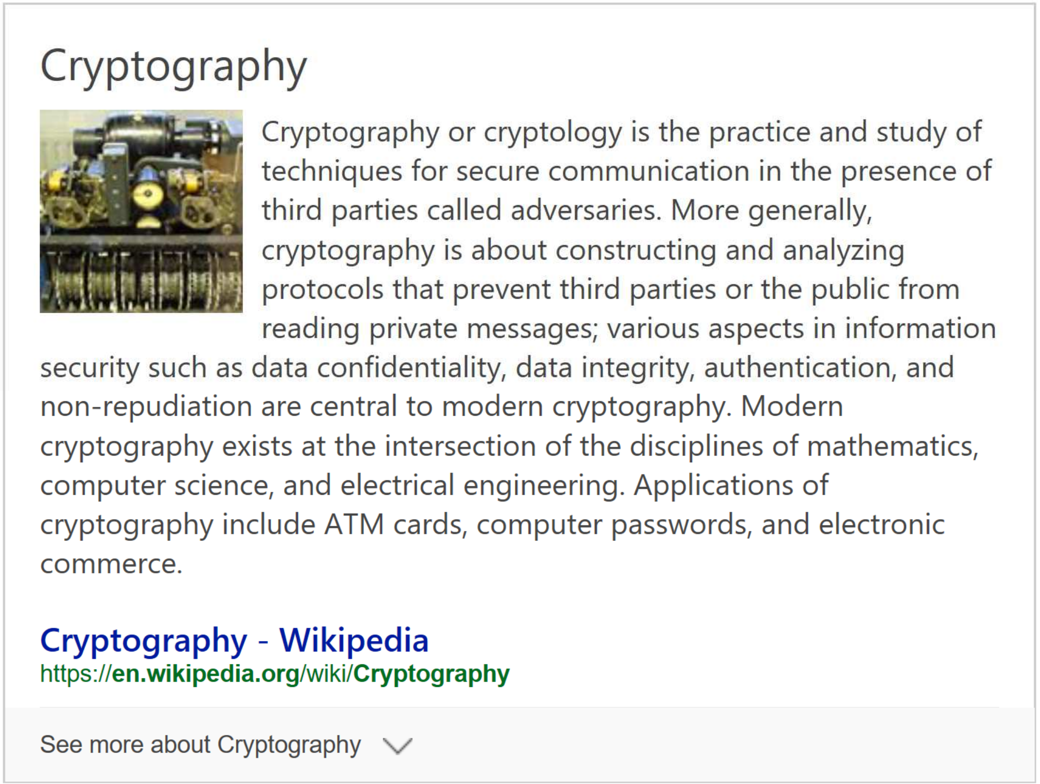
Agenda

1. Introductions
2. Foe?
3. Targets
4. Vectors
5. **Blockchain Primer**
6. Friend
7. Q & A

5 – Blockchain Primer


SYSTEM DESIGN FLOW
Then a miracle occurs
OUT.
Good work, but I think we might need just a little more detail right here.

5 – Blockchain Primer – Cryptography & Hashing

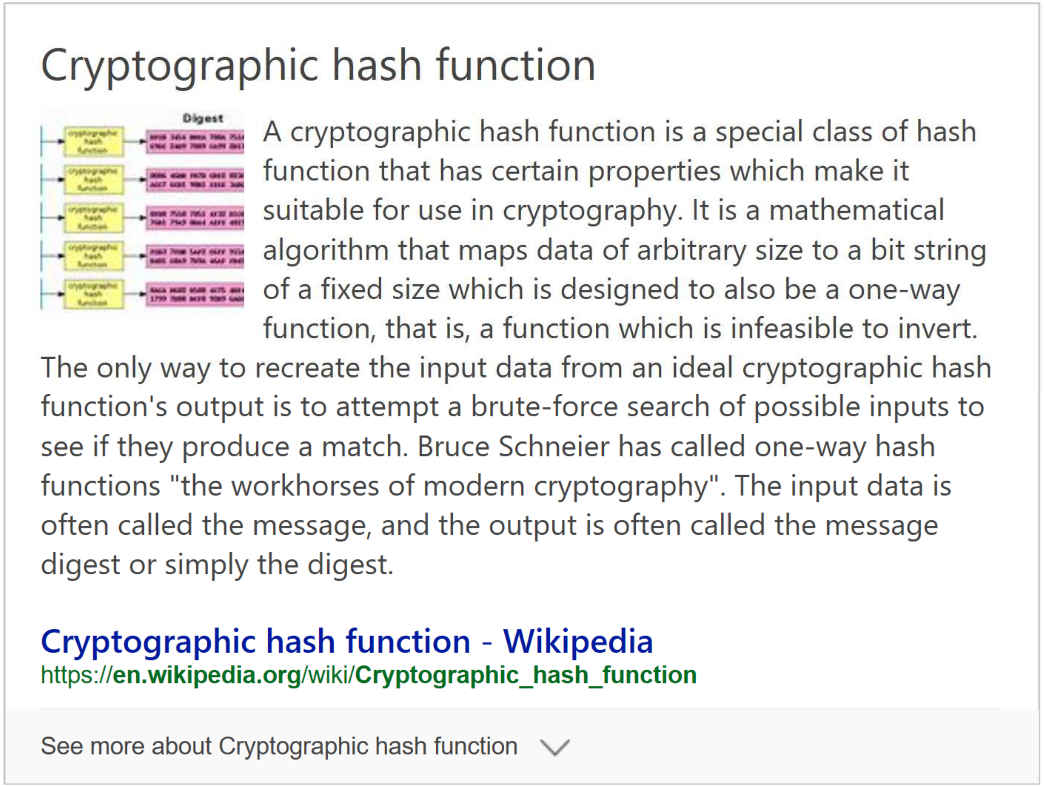


Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography - Wikipedia
https://en.wikipedia.org/wiki/Cryptography

See more about Cryptography



Cryptographic hash function

A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size which is designed to also be a one-way function, that is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match. Bruce Schneier has called one-way hash functions "the workhorses of modern cryptography". The input data is often called the message, and the output is often called the message digest or simply the digest.

Cryptographic hash function - Wikipedia
https://en.wikipedia.org/wiki/Cryptographic_hash_function

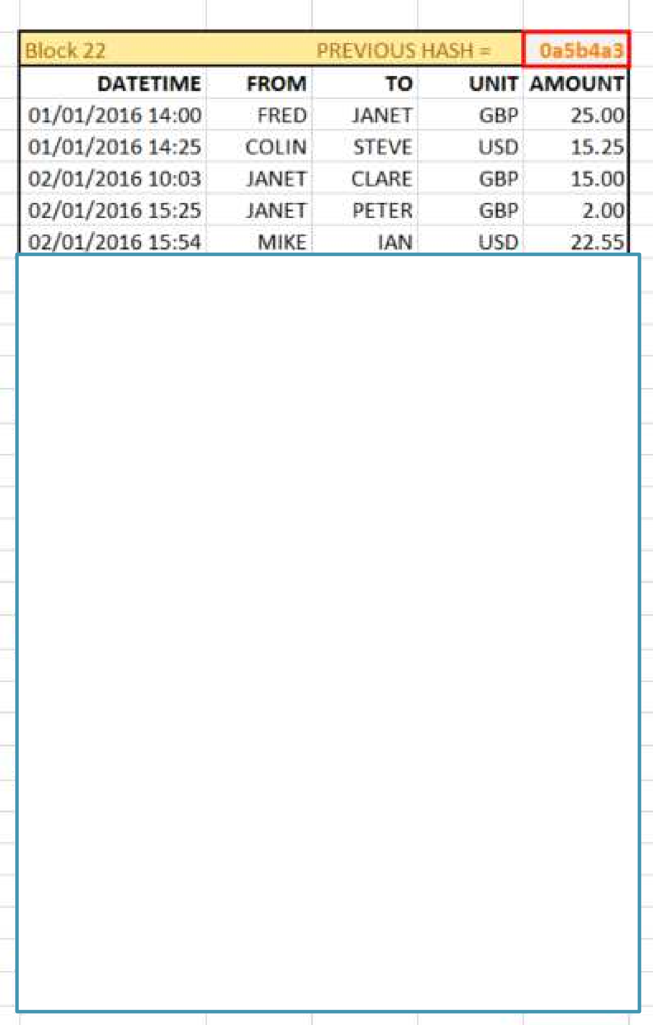
See more about Cryptographic hash function

Mathematics to keep things secure & secret

Mathematics to provide a unique signature

5 – Blockchain Primer –Blockchain(s)

Imagine a physical ledger, with pages in it



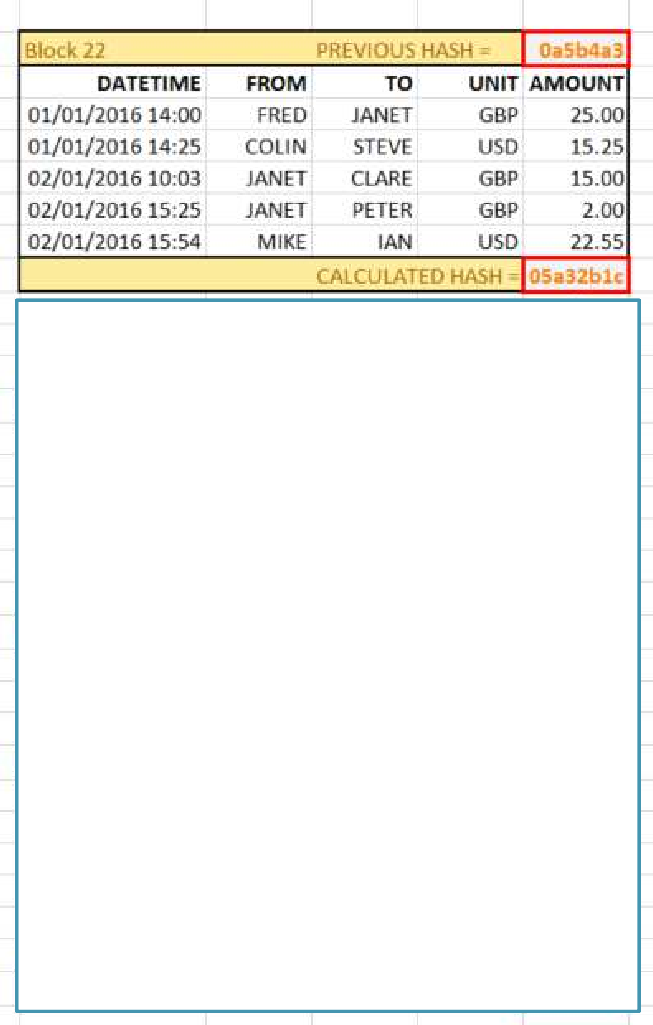
Block 22		PREVIOUS HASH =		0a5b4a3
DATETIME	FROM	TO	UNIT	AMOUNT
01/01/2016 14:00	FRED	JANET	GBP	25.00
01/01/2016 14:25	COLIN	STEVE	USD	15.25
02/01/2016 10:03	JANET	CLARE	GBP	15.00
02/01/2016 15:25	JANET	PETER	GBP	2.00
02/01/2016 15:54	MIKE	IAN	USD	22.55

`

5 – Blockchain Primer –Blockchain(s)

Imagine a physical ledger, with pages in it

At the bottom of the page you enter the **hash** for that page



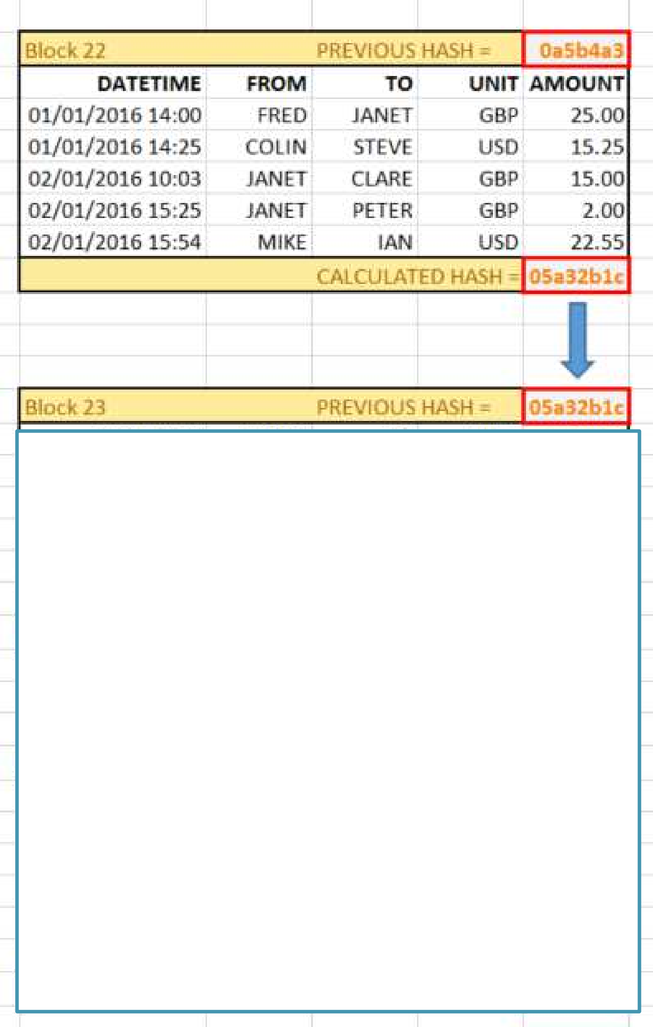
Block 22		PREVIOUS HASH =			0a5b4a3
DATETIME	FROM	TO	UNIT	AMOUNT	
01/01/2016 14:00	FRED	JANET	GBP	25.00	
01/01/2016 14:25	COLIN	STEVE	USD	15.25	
02/01/2016 10:03	JANET	CLARE	GBP	15.00	
02/01/2016 15:25	JANET	PETER	GBP	2.00	
02/01/2016 15:54	MIKE	IAN	USD	22.55	
		CALCULATED HASH =			05a32b1c

5 – Blockchain Primer –Blockchain(s)

Imagine a physical ledger, with pages in it

At the bottom of the page you enter the hash for that page

At the top of the next page, you start with the hash from the previous page. This means that when you hash the page it includes the hash from the previous page.



Block 22		PREVIOUS HASH =		0a5b4a3
DATETIME	FROM	TO	UNIT	AMOUNT
01/01/2016 14:00	FRED	JANET	GBP	25.00
01/01/2016 14:25	COLIN	STEVE	USD	15.25
02/01/2016 10:03	JANET	CLARE	GBP	15.00
02/01/2016 15:25	JANET	PETER	GBP	2.00
02/01/2016 15:54	MIKE	IAN	USD	22.55
		CALCULATED HASH =		05a32b1c

Block 23		PREVIOUS HASH =		05a32b1c

5 – Blockchain Primer –Blockchain(s)

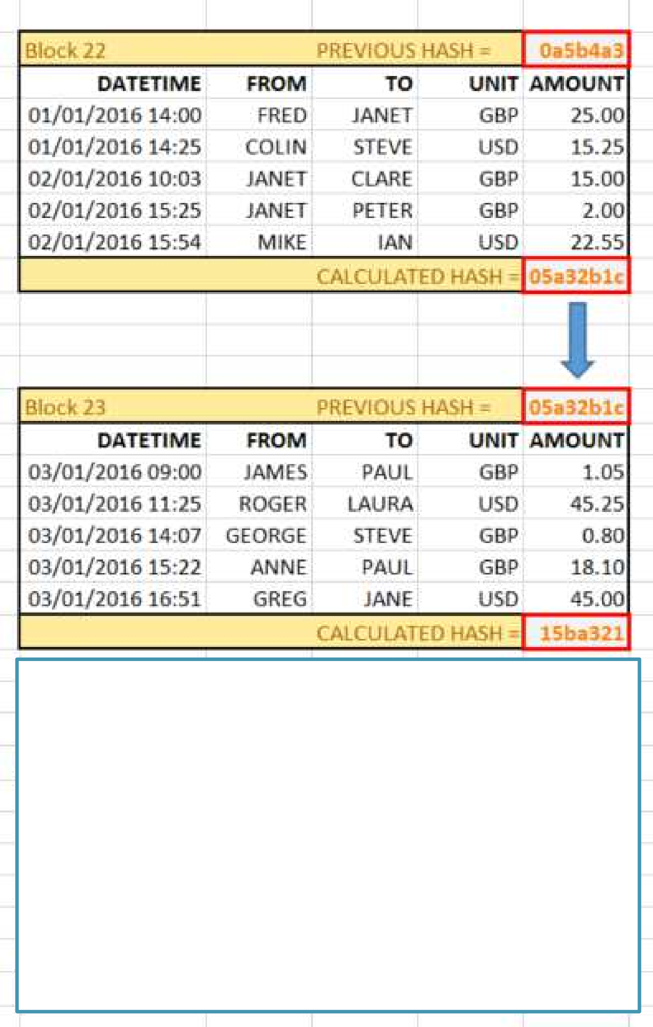
Imagine a physical ledger, with pages in it

At the bottom of the page you enter the hash for that page

At the top of the next page, you start with the hash from the previous page

So, the data is held in **BLOCKS** which are **CHAIN**ed together

BLOCKCHAIN!



Block 22			PREVIOUS HASH =	0a5b4a3
DATETIME	FROM	TO	UNIT	AMOUNT
01/01/2016 14:00	FRED	JANET	GBP	25.00
01/01/2016 14:25	COLIN	STEVE	USD	15.25
02/01/2016 10:03	JANET	CLARE	GBP	15.00
02/01/2016 15:25	JANET	PETER	GBP	2.00
02/01/2016 15:54	MIKE	IAN	USD	22.55
			CALCULATED HASH =	05a32b1c

Block 23			PREVIOUS HASH =	05a32b1c
DATETIME	FROM	TO	UNIT	AMOUNT
03/01/2016 09:00	JAMES	PAUL	GBP	1.05
03/01/2016 11:25	ROGER	LAURA	USD	45.25
03/01/2016 14:07	GEORGE	STEVE	GBP	0.80
03/01/2016 15:22	ANNE	PAUL	GBP	18.10
03/01/2016 16:51	GREG	JANE	USD	45.00
			CALCULATED HASH =	15ba321

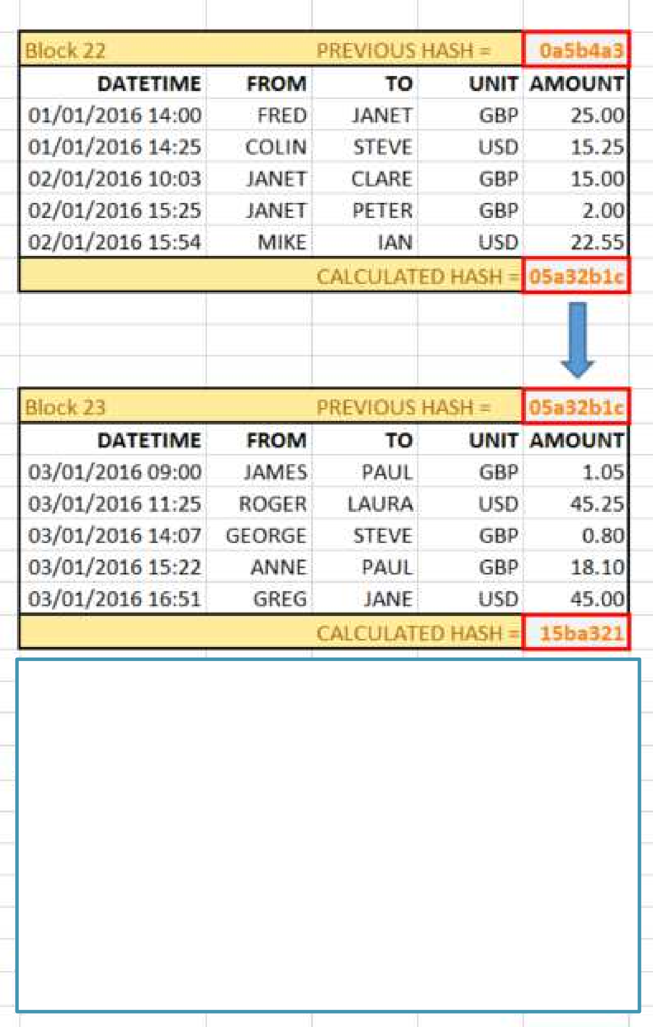
5 – Blockchain Primer –Blockchain(s)

Imagine a physical ledger, with pages in it

At the bottom of the page you enter the hash for that page

At the top of the next page, you start with the hash from the previous page

So, the data is held in **BLOCKS** which are **CHAIN**ed together



Block 22			PREVIOUS HASH =	0a5b4a3
DATETIME	FROM	TO	UNIT	AMOUNT
01/01/2016 14:00	FRED	JANET	GBP	25.00
01/01/2016 14:25	COLIN	STEVE	USD	15.25
02/01/2016 10:03	JANET	CLARE	GBP	15.00
02/01/2016 15:25	JANET	PETER	GBP	2.00
02/01/2016 15:54	MIKE	IAN	USD	22.55
			CALCULATED HASH =	05a32b1c

Block 23			PREVIOUS HASH =	05a32b1c
DATETIME	FROM	TO	UNIT	AMOUNT
03/01/2016 09:00	JAMES	PAUL	GBP	1.05
03/01/2016 11:25	ROGER	LAURA	USD	45.25
03/01/2016 14:07	GEORGE	STEVE	GBP	0.80
03/01/2016 15:22	ANNE	PAUL	GBP	18.10
03/01/2016 16:51	GREG	JANE	USD	45.00
			CALCULATED HASH =	15ba321

5 – Blockchain Primer –Blockchain(s)

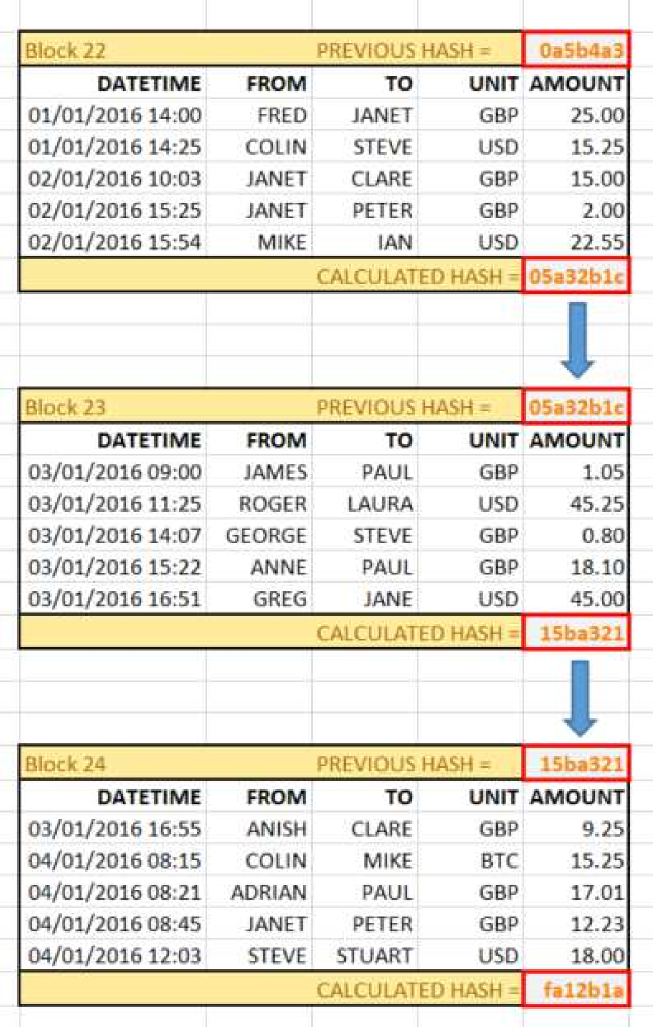
Imagine a physical ledger, with pages in it

At the bottom of the page you enter the hash for that page

At the top of the next page, you start with the hash from the previous page

So, the data is held in BLOCKS which are CHAINed together

Now VERY difficult to change an earlier entry as all of the hashes on all pages would need to be recalculated

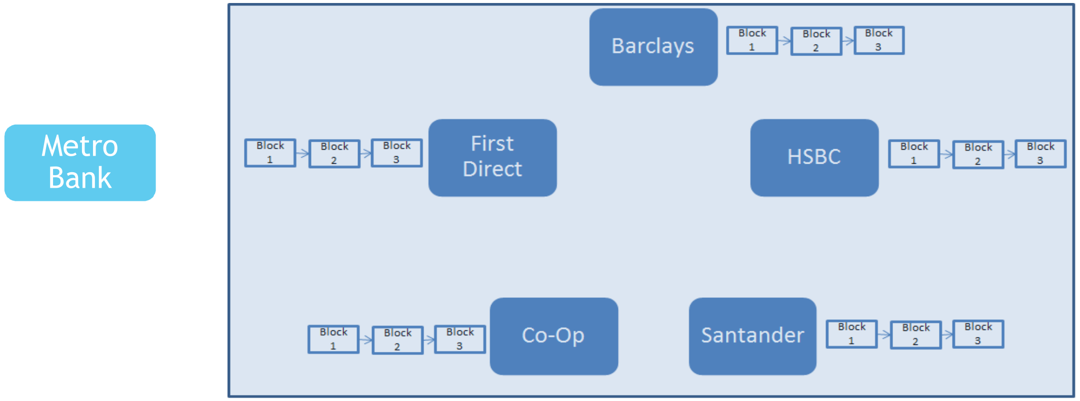


Block 22		PREVIOUS HASH =		0a5b4a3
DATETIME	FROM	TO	UNIT	AMOUNT
01/01/2016 14:00	FRED	JANET	GBP	25.00
01/01/2016 14:25	COLIN	STEVE	USD	15.25
02/01/2016 10:03	JANET	CLARE	GBP	15.00
02/01/2016 15:25	JANET	PETER	GBP	2.00
02/01/2016 15:54	MIKE	IAN	USD	22.55
		CALCULATED HASH =		05a32b1c

Block 23		PREVIOUS HASH =		05a32b1c
DATETIME	FROM	TO	UNIT	AMOUNT
03/01/2016 09:00	JAMES	PAUL	GBP	1.05
03/01/2016 11:25	ROGER	LAURA	USD	45.25
03/01/2016 14:07	GEORGE	STEVE	GBP	0.80
03/01/2016 15:22	ANNE	PAUL	GBP	18.10
03/01/2016 16:51	GREG	JANE	USD	45.00
		CALCULATED HASH =		15ba321

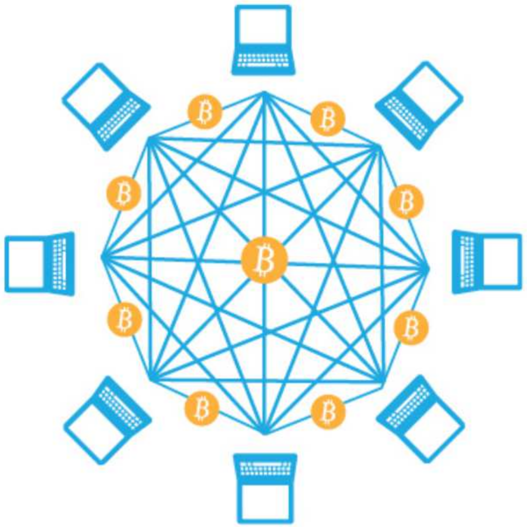
Block 24		PREVIOUS HASH =		15ba321
DATETIME	FROM	TO	UNIT	AMOUNT
03/01/2016 16:55	ANISH	CLARE	GBP	9.25
04/01/2016 08:15	COLIN	MIKE	BTC	15.25
04/01/2016 08:21	ADRIAN	PAUL	GBP	17.01
04/01/2016 08:45	JANET	PETER	GBP	12.23
04/01/2016 12:03	STEVE	STUART	USD	18.00
		CALCULATED HASH =		fa12b1a

You can restrict access only to members…



…Giving a Private, Permissioned Ledger

You can provide open access to everybody…



… but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

Graphic: Deloitte University Press | DUPress.com

…Giving a Public, Unpermissioned Ledger

So, back to the definition….

It’s a write-only database
That everyone has an identical copy of

With all entries timestamped
And the data is cryptographically secured

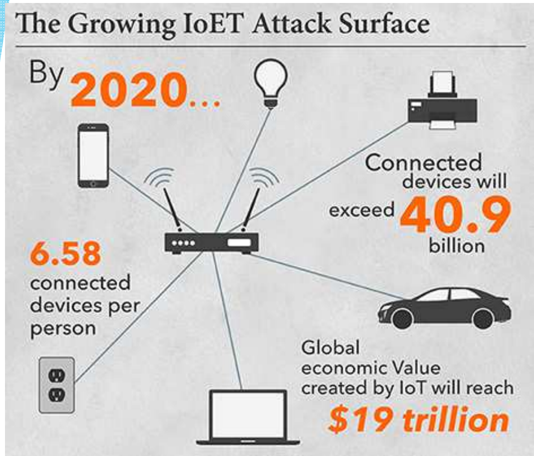
Which means:

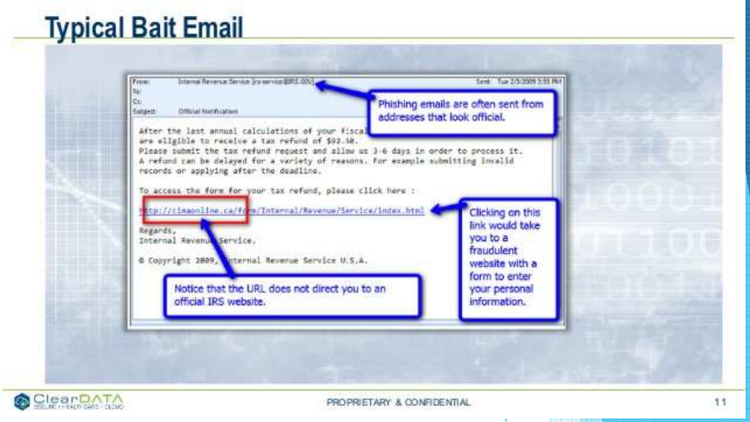
- **A complete history of all transactions - great audit trail**
- **Everyone has a copy of the same thing - No need for reconciliation**
- **It’s highly distributed - Makes it cyber-resistant**
- **Data is cryptographically secured - overcomes security issues**

Agenda

1. Introductions
2. Foe?
3. Targets
4. Vectors
5. Blockchain Primer
6. **Friend**
7. Q & A

Vectors


The Growing IoET Attack Surface
By 2020...
Connected devices will exceed 40.9 billion
6.58 connected devices per person
Global economic Value created by IoT will reach $19 trillion



Typical Bait Email

From: Internal Revenue Service [irs-service@IRS.GOV]
To:
Cc:
Subject: Official Notification
Sent: Tue 2/3/2009 3:55 PM

```
After the last annual calculations of your fiscal
are eligible to receive a tax refund of $92.50.
Please submit the tax refund request and allow us 3-6 days in order to process it.
A refund can be delayed for a variety of reasons. For example submitting invalid
records or applying after the deadline.

To access the form for your tax refund, please click here :

http://cimaonline.ca/form/Internal/Revenue/Service/index.html

Regards,
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.
```

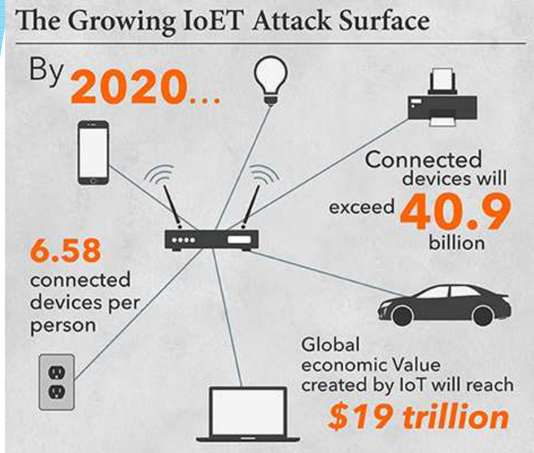
Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.

ClearDATA PROPRIETARY & CONFIDENTIAL 11

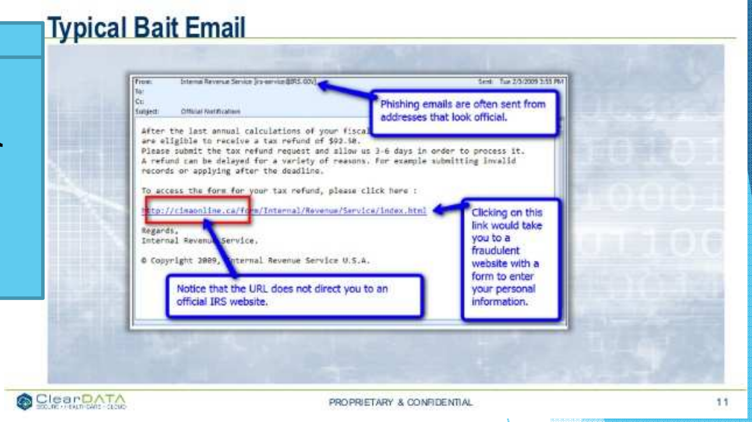
Friend


The Growing IoET Attack Surface
By 2020...
Connected devices will exceed 40.9 billion
6.58 connected devices per person
Global economic Value created by IoT will reach $19 trillion

Verified Devices

Firmware O/S

Secure eMail Verified authenticity



Typical Bait Email

From: Internal Revenue Service [irs-service@IRS.GOV]

Sent: Tue 2/3/2009 3:55 PM

To:

Cc:

Subject: Official Notification

After the last annual calculations of your fiscal

are eligible to receive a tax refund of $92.50.

Please submit the tax refund request and allow us 3-6 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here :

http://cimaonline.ca/form/Internal/Revenue/Service/index.html

Regards,

Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.

ClearDATA SECURE • HEALTHCARE • CLOUD

PROPRIETARY & CONFIDENTIAL

11

Blockchain:
Decentralised
Distributed
Encrypted

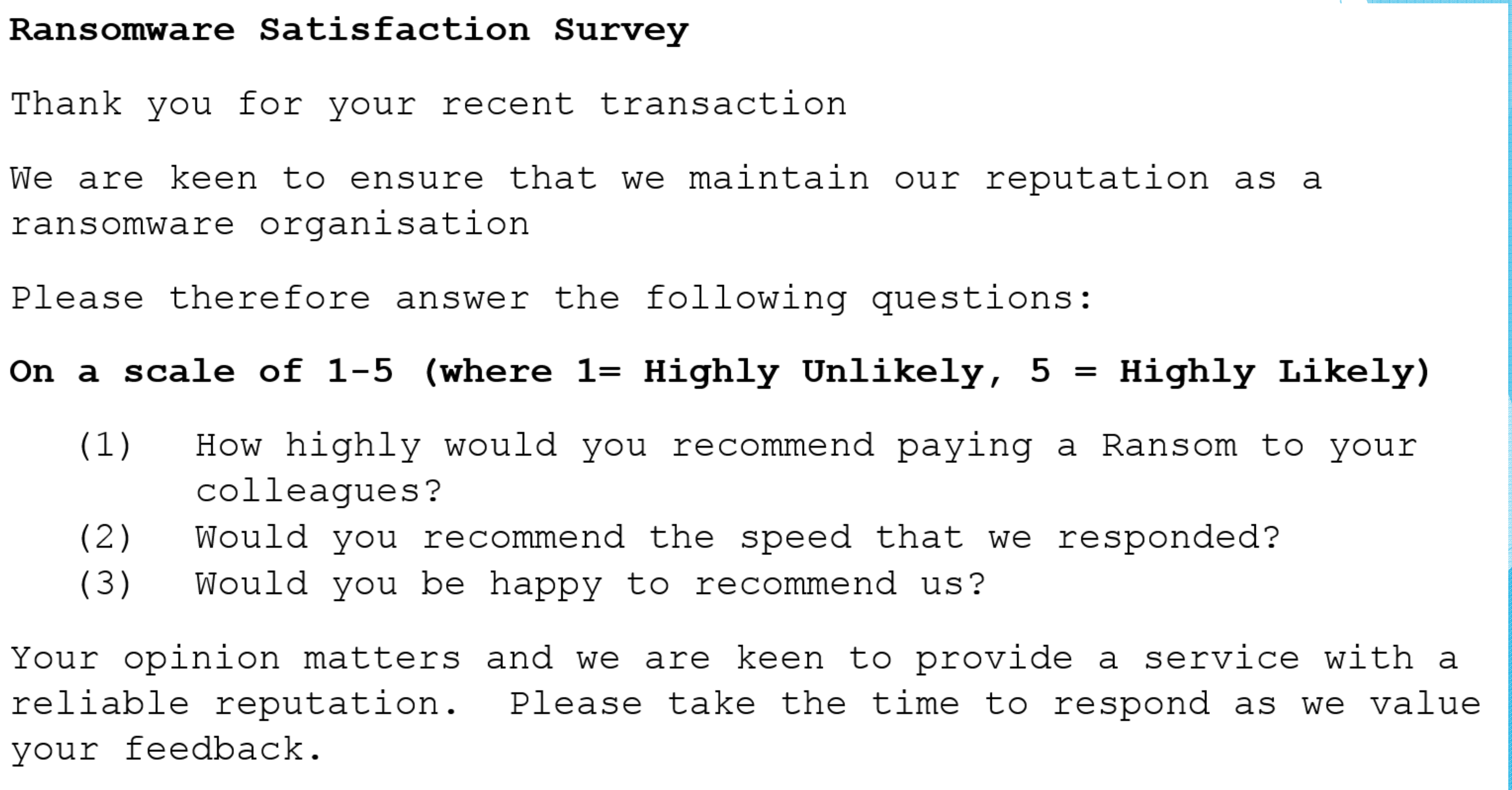
Digital Certificate Management/ OCSP

Identity
Authentication
Authorisation
Accreditation

Agenda

1. Introductions
2. Foe?
3. Targets
4. Vectors
5. Blockchain Primer
6. Friend
7. **Q & A**

Q & A



Ransomware Satisfaction Survey

Thank you for your recent transaction

We are keen to ensure that we maintain our reputation as a ransomware organisation

Please therefore answer the following questions:

On a scale of 1-5 (where 1= Highly Unlikely, 5 = Highly Likely)

(1) How highly would you recommend paying a Ransom to your colleagues?
(2) Would you recommend the speed that we responded?
(3) Would you be happy to recommend us?

Your opinion matters and we are keen to provide a service with a reliable reputation. Please take the time to respond as we value your feedback.

www.linkedin.
www.linked
www.link

Q & A

Thank you!

Gary Nuttall contact details:
eMail: gnuttall@distlytics.com

Twitter: @GPN01

LinkedIn:uk.linkedin.com/in/garynuttall
Web: www.Distlytics.com

Distlytics

Distributed Ledger Analytics
Consultancy & Insight