MALAWI INTERNET GOVERNANCE FORUM
2019 CAPITAL HOTEL – 17-18 DECEMBER 2019

ONE WORLD. ONE NET. ONE VISION

CRYPTOCURRENCIES & BITCOIN

Sunduzwayo Madise
BSc, LLB (Hons), LLM, PGAHE, PhD
Fellow of the Higher Education Academy (UK)
Commonwealth Fellow
NORHED Post-Doc Researcher
(mfundisi)
Dean of Law - University of Malawi
smadise@cc.ac.mw

Early evolution

Commercial Law Clinic

21 Nov 2019

Faculty of Law

Structure of presentation

1. Virtual currencies and the birth of cryptocurrencies
2. The old silk road
3. The new Silk road
4. Challenges of regulating cryptocurrencies

Main characteristics/functions of money

- Medium of exchange
- Store of value
- Unit of account

Challenges of regulating emerging forms of money

The underlying question for the regulation of new forms of money is the extent to which they create new or different risks.

UNIVERSITY OF MALAWI

Virtual currency

*“a type of **unregulated**, **digital money**, which is **issued** and usually controlled by its **developers**, and used and accepted among the members of a **specific virtual community**.”*

The European Central Bank in 2012 :

VIRTUAL CURRENCY

- **Digital representation** of value - **neither** issued by a central bank or public authority
- Used a **means of exchange** - can be transferred, stored or traded electronically.
- Digitally traded as, and **functions as money**, **but is not legal tender**.
- Not issued by **fiat** - **no state guarantee**
- Operates as money on the basis that it is accepted by the community which uses it – **social tender**
- **Decentralised currency**

UNIVERSITY OF MALAWI

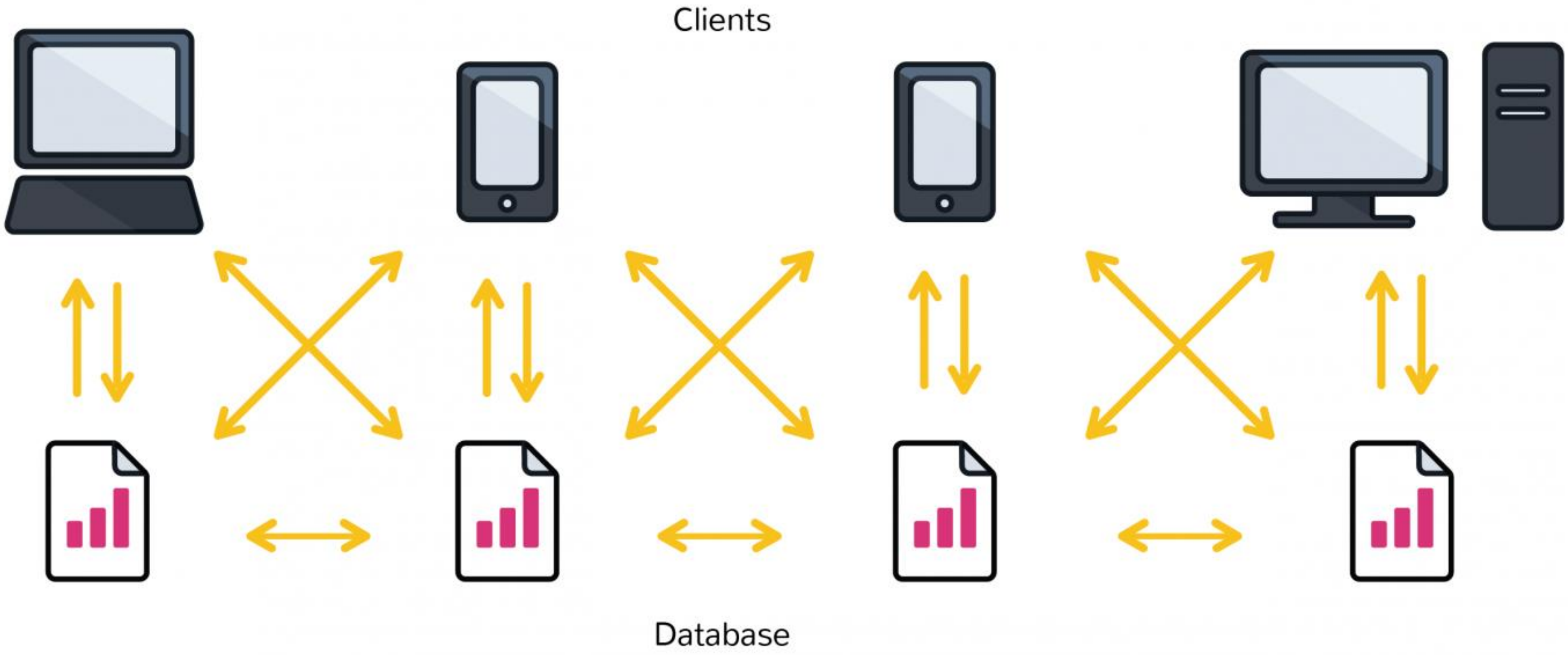
Decentralised currency

- Its value is represented by the currency’s “**coin**”
- Coin is an **encrypted** piece of **computer code** that is **difficult to reproduce**, but **easy to verify**.
- The “coin” has **two “keys”:**
  - a public key that anchors it to its hosting **blockchain** or **publicly distributed ledger**, and
  - a **private key** that **infers ownership** and is held in the “coin’s” **owner wallet**.

Decentralised currency

- A bank-less currency is **free** of national monetary policies.
- For residents of countries that have destabilized fiat currencies, can serve as **a stabilizing agent** and an alternative.
- **Insulates** from **bank failures** and collapses, as well as **exuberant bank fees** and **aggressive bank policies**.
- **Borderless payments** - allows for **seamless** and **cheap international payments** despite current **limits** on transnational fiat payments.
- **Immune** to inflation or deflation [but can be volatile].
- The only requirement for using decentralized currencies is the ability to obtain and use a wallet. A attractive to the **underbanked/unbanked**.
- **Not subject** to geographically-based exchange rates - goods and services bought with decentralized currency will not be devalued due to tariffs or unfavorable changes in national monetary values.
- A real-world demonstration of **blockchain technology**

Blockchain Technology



Cryptocurrency

- A **decentralised virtual currency**, based on a **mathematical formula** that is protected by **cryptography**.
- Cryptography ensures that the digital currency is **secure and protected** from being interfered with by **third parties**.
- Also prevents the **duplicate** or **multiple** uses of the same currency – **double spending** – ***time stamp***
- Estimated to be close to two thousand (and counting) cryptocurrencies in operation.
- Most famous cryptocurrency is **Bitcoin**

- Once you send money via a cryptocurrency there is no going back.
- The transaction is absolutely permanent and unalterable as it added to the blockchain.
- It is also generally anonymous as there is not central system and transactions are not actually connected with a personal identity.
- Proponents argue that :
  - It cuts out 3rd parties like banks [that have for too long manipulated the financial arena]
  - Allows for global transactions in areas of the world where access to banks or small loans are limited.
  - Removes the necessity of having hard currency in bills in cash.

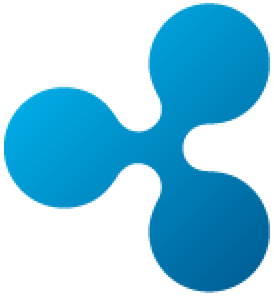
Cryptocurrencies

Litecoin

Ethereum

Zcash

Dash



Ripple

Monero

Neo

Bitcoin

Cardano

Bitcoin

- **No actual coins** in Bitcoin
- Bought using fiat money.
- Can be exchanged via special Bitcoin exchanges
- Some vendors accept payment in Bitcoin
- Used and accepted as tender in the Bitcoin **ecosystem**

Bitcoin

- Bitcoin has been shrouded in mystery ever since its introduction.
- **Satoshi Nakamoto** the so-called creator of Bitcoin announced the “Peer-to-Peer Electronic Cash System” on October 31, 2009
- However, Satoshi Nakamoto, a presumed **pseudonym**, has never actually been identified.
- As part of the implementation, Nakamoto also devised the first **blockchain** database.
- Nakamoto was the first to solve the **double-spending** problem for digital currency using a **peer-to-peer network**.

Bitcoin 101

- **Anonymity** is one of the reasons for security concerns regarding the trading of cryptocurrency.
- Virtual currencies have created a **decentralized** cash system that completely cuts out the **middleperson**, - currency sent online, directly, from one user to another.
- Traditionally, these “middlepersons” have been **banks**
- With cryptocurrency, instead of having a central entity like a bank that would manage in-going and outgoing expenditures, **peer-to-peer networks** of computers act as managers of these expenditures.
- If **X** (the sender) sends cryptocurrency to **Y** (the receiver), this cryptocurrency would be sent from **X’s** computer and then blasted out to the entire network.
- **Y**, the receiver of the currency, would have a **key** or **code** to access the currency

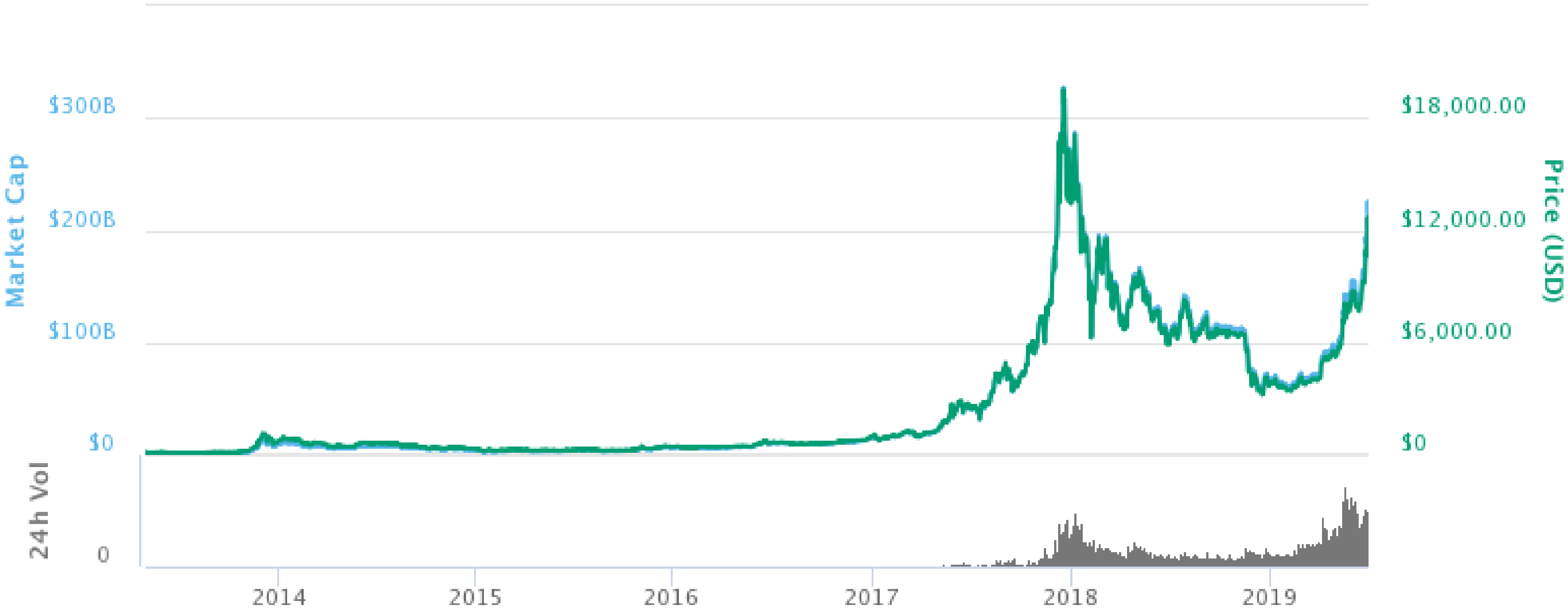
- **But** before the transaction can be completed a verification process needs to take place.
- This is to ensure that transactions cannot be duplicated.
- This is done by what industry members call "**mining**" done by "**miners**."
- "Miners" check the transactions to make sure it is not a **counterfeit** or **duplicate transaction**.
- Mining takes a ton of computer power
- These independent "miners" invest some of their own-person computer power [and time] and in return they receive cryptocurrency, such as, Bitcoin.
- This is the only way **valid** Bitcoins can be created.
- Otherwise they have to be bought

- **But** before the transaction can be completed a verification process needs to take place.
- This is to ensure that transactions cannot be duplicated.
- This is done by what industry members call "**mining**" done by "**miners**."
- "Miners" check the transactions to make sure it is not a **counterfeit** or **duplicate transaction**.
- Mining takes a ton of computer power
- These independent "miners" invest some of their own-person computer power [and time] and in return they receive cryptocurrency, such as, Bitcoin.
- This is the only way **valid** Bitcoins can be created.
- Otherwise they have to be bought

Bitcoin

- Has a 21 million ceiling (*Does this give it certainty of value?*)
- Bitcoins are **mathematically mined** using a computer
- **Time stamp** to avoid double spending
- **Irreversible transactions** – *vendors love this*
- Allows **anonymity** (similar to cash in a way)
- **Silk Road – *That is where it all happens! Anything and everything goes***

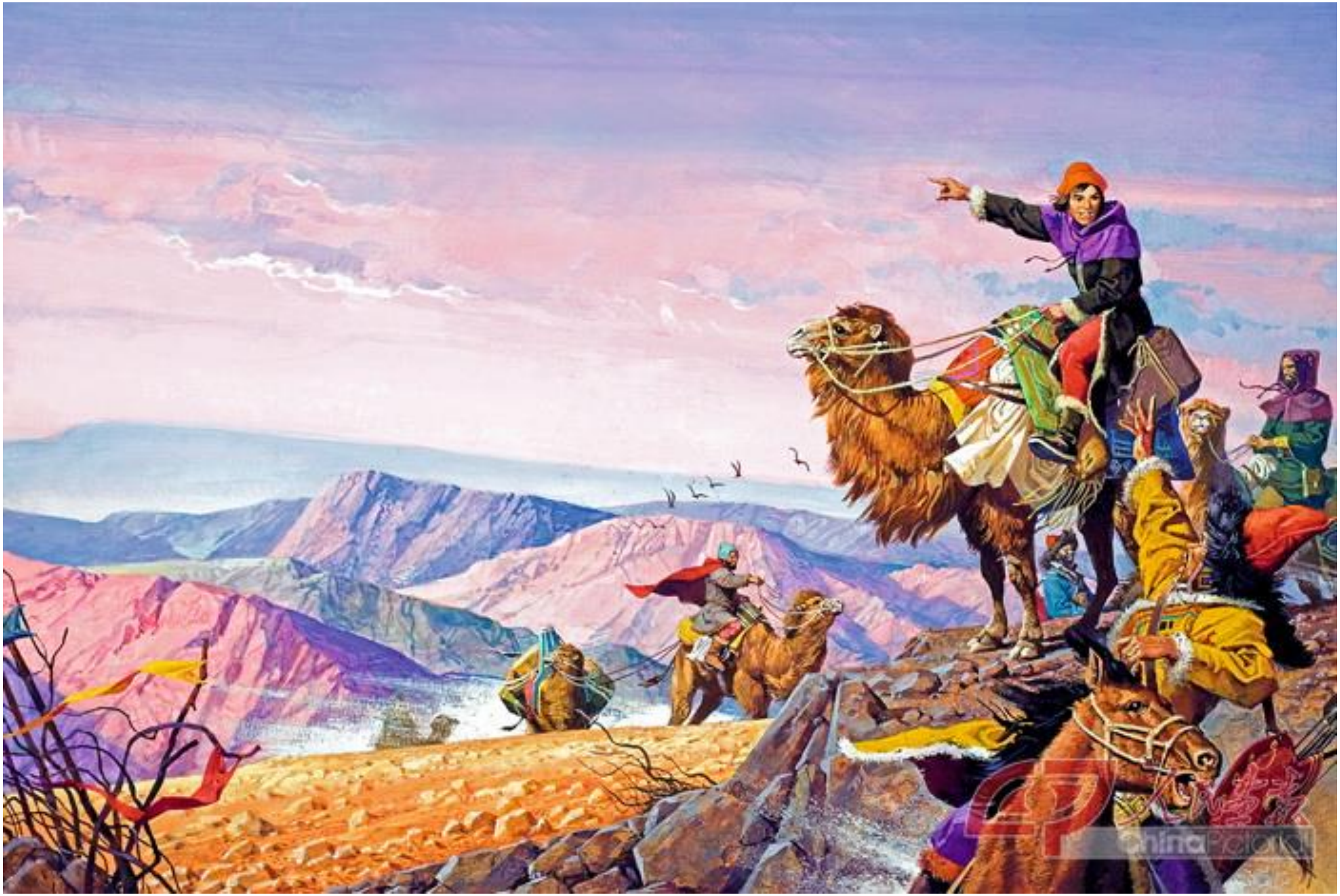
Bitcoin value over the years …



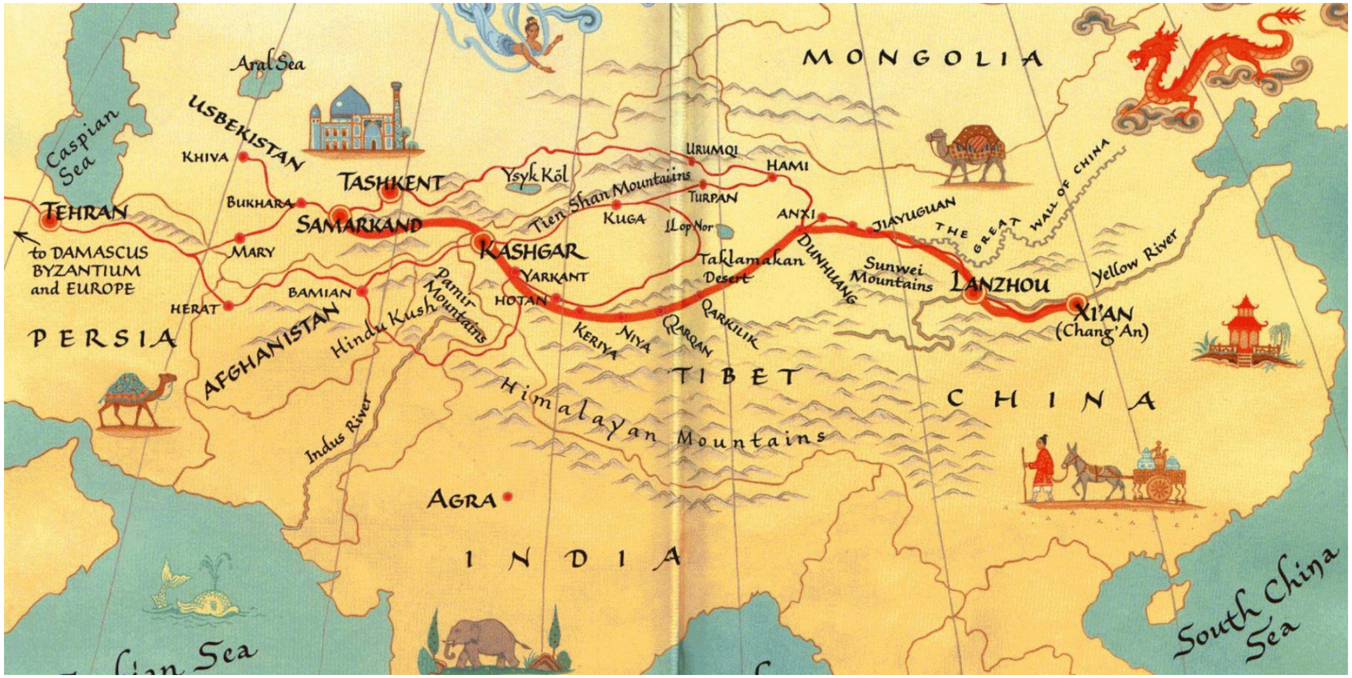
Bitcoin

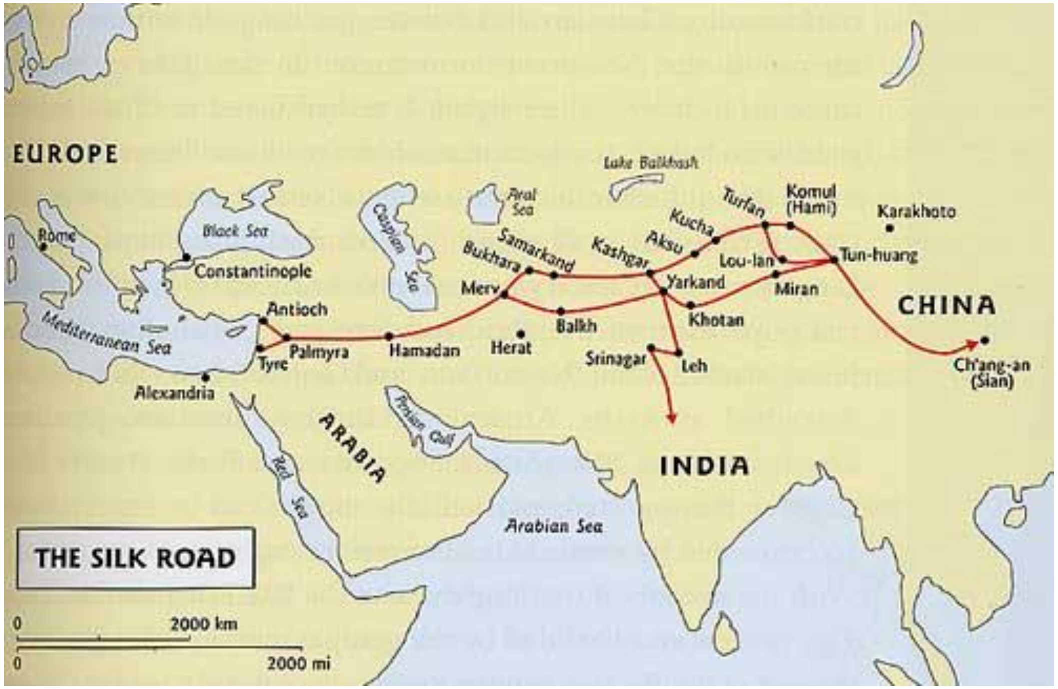
- Normally operations in the digital domain always leave a trace or a footprint.
- However, thanks to cryptography, Bitcoin allow users to trade with “a high degree of anonymity”.
- In this respect, Bitcoin **mimics** cash.
- Because of this, Bitcoins have become **attractive to criminals** including those dealing in **illicit financing**.
- [Recent] ***Ransomware*** attack - hackers got into the systems of several global institutions, including the UK’s **National Health Service** (NHS), threatening to permanently lock data unless a ransom was paid in Bitcoins

Silk Road



Silk Road

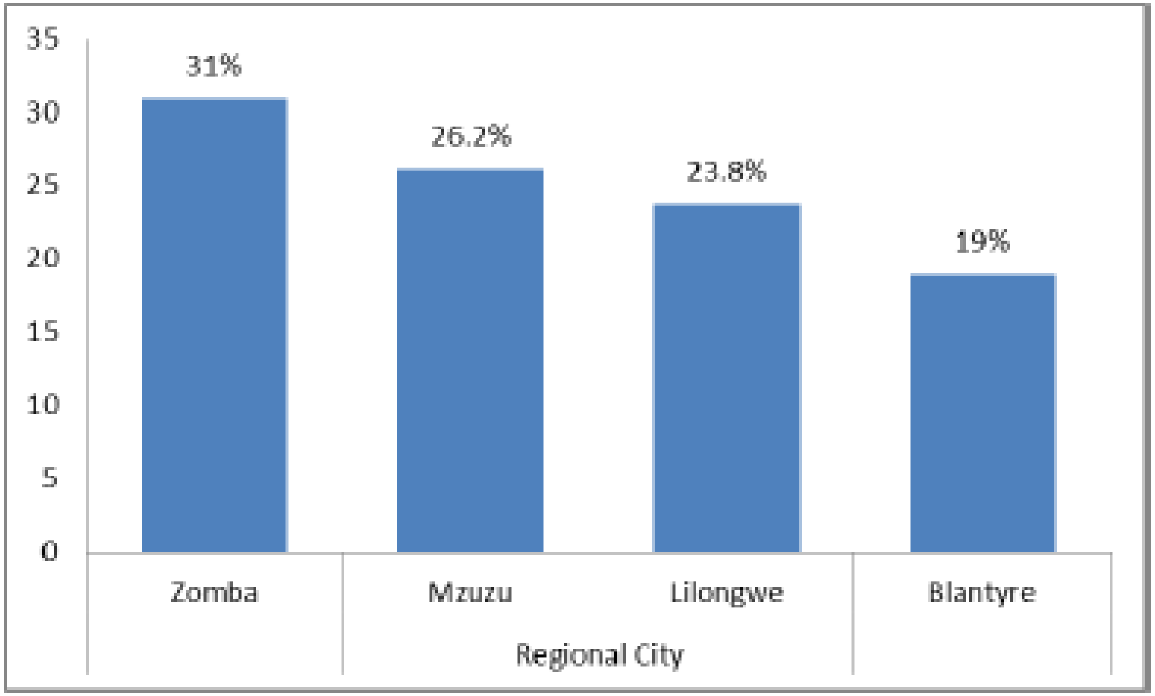

Aral Sea
Caspian Sea
USBEKISTAN
KHIVA
TASHKENT
BUKHARA
SAMARKAND
TEHRAN
to DAMASCUS BYZANTIUM and EUROPE
MARY
HERAT
BAMIAN
PERSIA
AFGHANISTAN
Hindu Kush
Pamir Mountains
Ysyk Köl
Tien Shan Mountains
KASHGAR
YARKANT
HOTAN
KERIYA
NIYA
QARQAN
QARKILIK
KUGA
URUMQI
TURPAN
HAMI
Lop Nor
Taklamakan Desert
ANXI
DUNHUANG
JIAYUGUAN
THE GREAT WALL OF CHINA
Sunwei Mountains
LANZHOU
XI'AN (Chang'An)
Yellow River
MONGOLIA
TIBET
CHINA
Himalayan Mountains
Indus River
AGRA
INDIA
South China Sea
Sea


EUROPE
Lake Balkhash
Aral Sea
Caspian Sea
Black Sea
Rome
Constantinople
Mediterranean Sea
Antioch
Tyre
Palmyra
Alexandria
Hamadan
Merv
Bukhara
Samarkand
Balkh
Herat
Kashgar
Aksu
Kucha
Turfan
Komul (Hami)
Karakhoto
Lou-lan
Tun-huang
Yarkand
Miran
Khotan
Srinagar
Leh
CHINA
Ch'ang-an (Sian)
ARABIA
Persian Gulf
Red Sea
Arabian Sea
INDIA
THE SILK ROAD
0
2000 km
0
2000 mi

Cryptocurrencies in Malawi?

- Research by Thangalimodzi (2019) ~ 400 respondents (cities)
- 88% - Bitcoin (plus Bitcoin Cash)
- 10.5% of respondents use cyrptocurrencies
- 84% are male

INVESTMENT BY REGIONS



Graph by Thangalimodzi (2019)

Cryptocurrency
is here to stay

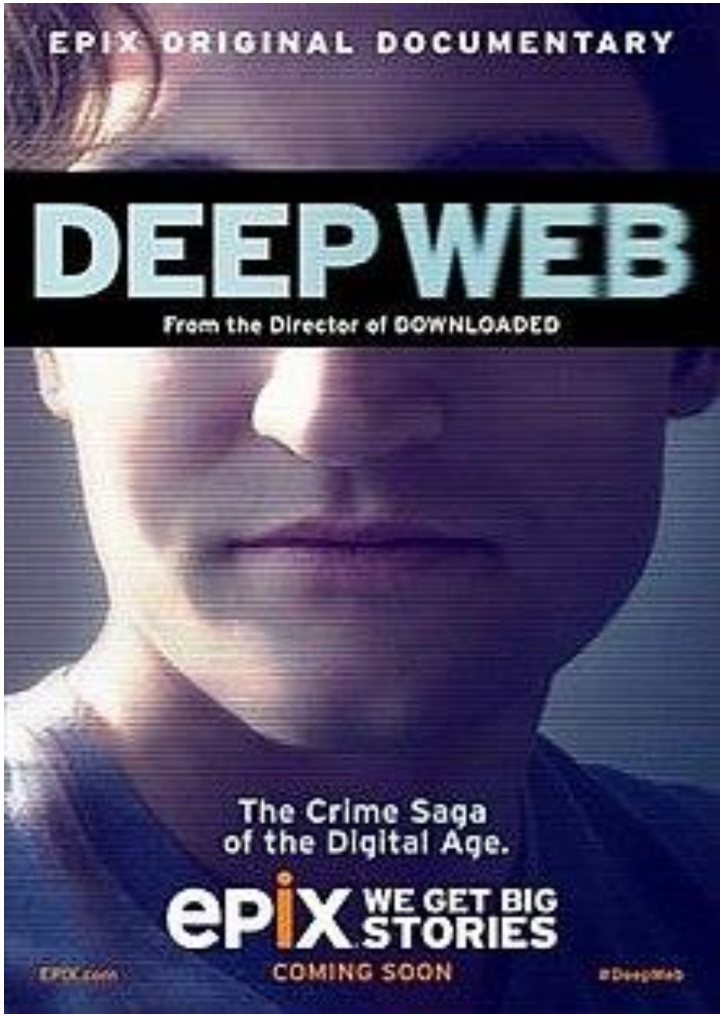
Welcome to the Dark Side

Enter the dark web …

- The dark web is part of the internet that you cannot access it through Google.
- Needs **special software** to access it.
- Allows you to surf the web while **encrypting your identification** as you go so your **IP address is unreadable**.
- One of the most popular software programs used to access the dark web is called **TOR**
- TOR was created by the **US government**.
- Not not all activities on the dark web are nefarious.
- TOR is **still supported** by the US government
  - plays a role in **state security**
  - allows **journalists to connect secretly** with sources and has even been used by dissidents of authoritarian regimes to share information.

New Silk Road – The Dark Web

- Silk Road - **online black market -** the first modern **darknet** market
- Best known as a platform for **selling illegal drugs**.
- Part of the **dark web –** operating as a **hidden service**
- Launched in February 2011 - Provided **anonymity** (securely without potential traffic monitoring) to online users
- Site had 10,000 products 4 sale by vendors - **70% of were drugs**
- Shut down by the FBI in 2013 - arrested Ross Ulbricht under charges of being the site's pseudonymous founder "**Dread Pirate Roberts**".
- 2013, **Silk Road 2.0** came online - run by former Silk Road operators
- Also shut down - alleged operator was arrested in 2014
- Following closure of Silk Road 2.0, **Diabolus Market** renamed itself to '**Silk Road 3 Reloaded**' – brand capitalisation.
- Had multiple cryptocurrency support [with similar listing restrictions to the original Silk Road market.]
- Now ‘deemed; defunct …

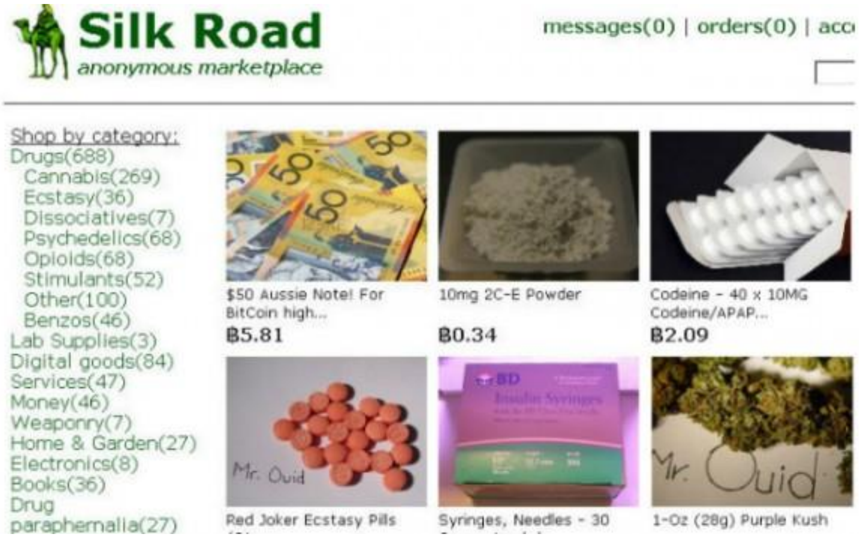

EPIX ORIGINAL DOCUMENTARY
DEEP WEB
From the Director of DOWNLOADED
The Crime Saga of the Digital Age.
epix WE GET BIG STORIES
EPIX.com
COMING SOON
#DeepWeb

Deep Web

-2015 documentary film, chronicling events surrounding Silk Road, Bitcoin and politics of the dark web.

Gives the inside story of the arrest of Ross Ulbricht

New Silk Road – The Dark Web



Silk Road
anonymous marketplace

messages(0) | orders(0) | acc

Shop by category:
- Drugs(688)
  - Cannabis(269)
  - Ecstasy(36)
  - Dissociatives(7)
  - Psychedelics(68)
  - Opioids(68)
  - Stimulants(52)
  - Other(100)
  - Benzos(46)
- Lab Supplies(3)
- Digital goods(84)
- Services(47)
- Money(46)
- Weaponry(7)
- Home & Garden(27)
- Electronics(8)
- Books(36)
- Drug paraphernalia(27)

$50 Aussie Note! For BitCoin high...
฿5.81

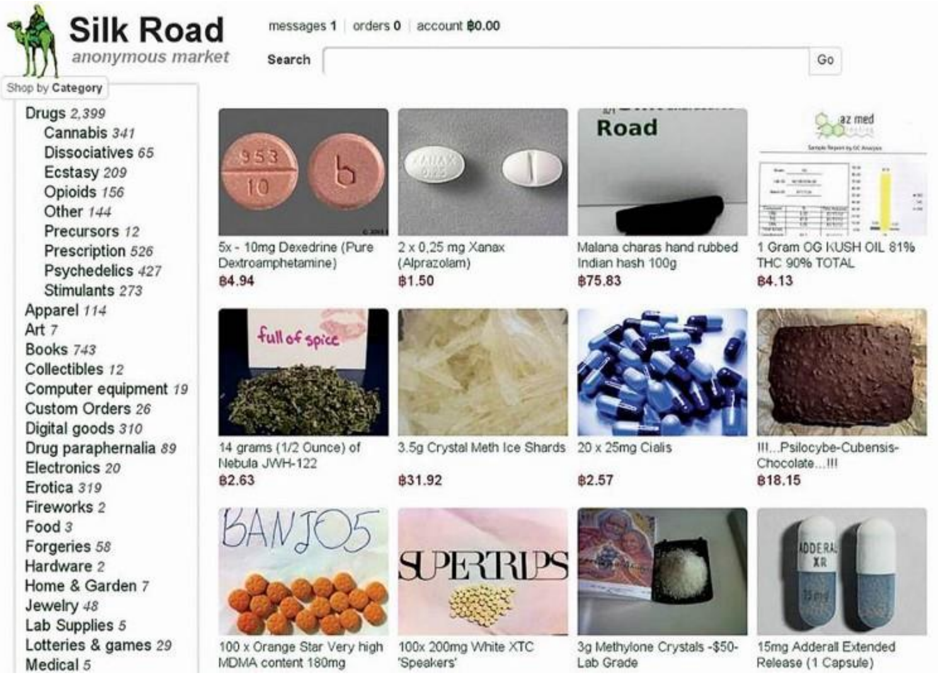
10mg 2C-E Powder
฿0.34

Codeine - 40 x 10MG Codeine/APAP...
฿2.09

Red Joker Ecstasy Pills

Syringes, Needles - 30

1-Oz (28g) Purple Kush



Silk Road
anonymous market

messages 1 | orders 0 | account ฿0.00

Search [ ] Go

Shop by Category
- Drugs 2,399
  - Cannabis 341
  - Dissociatives 65
  - Ecstasy 209
  - Opioids 156
  - Other 144
  - Precursors 12
  - Prescription 526
  - Psychedelics 427
  - Stimulants 273
- Apparel 114
- Art 7
- Books 743
- Collectibles 12
- Computer equipment 19
- Custom Orders 26
- Digital goods 310
- Drug paraphernalia 89
- Electronics 20
- Erotica 319
- Fireworks 2
- Food 3
- Forgeries 58
- Hardware 2
- Home & Garden 7
- Jewelry 48
- Lab Supplies 5
- Lotteries & games 29
- Medical 5

5x - 10mg Dexedrine (Pure Dextroamphetamine)
฿4.94

2 x 0,25 mg Xanax (Alprazolam)
฿1.50

Malana charas hand rubbed Indian hash 100g
฿75.83

1 Gram OG KUSH OIL 81% THC 90% TOTAL
฿4.13

14 grams (1/2 Ounce) of Nebula JWH-122
฿2.63

3.5g Crystal Meth Ice Shards
฿31.92

20 x 25mg Cialis
฿2.57

!!!...Psilocybe-Cubensis-Chocolate...!!!
฿18.15

100 x Orange Star Very high MDMA content 180mg

100x 200mg White XTC 'Speakers'

3g Methylone Crystals -$50- Lab Grade

15mg Adderall Extended Release (1 Capsule)

Regulatory challenges

UNIVERSITY OF MALAWI

Cryptocurrency and money

- Regulators like to deny that cryptocurrency is money
- They prefer the term **crypto assets**.
- Their view is supported by the failure of classic cryptocurrencies to achieve mainstream adoption due to their price volatility.
- No matter what they are called, cryptocurrencies are as close to money as you can get
- So central bankers & regulatory agencies will soon have to step up their game and find a way to regulate them

[RECAP] Main characteristics/functions of money

- Medium of exchange
- Store of value
- Unit of account

Regulatory challenges

Existing or new regime?

- In most jurisdictions the **natural tendency** is to use an **existing** regime.
- This allows regulators to respond quickly and be consistent
- Most jurisdictions use rules from **existing** laws applicable to cryptocurrency payment and to tokens (actual currency).
- This is where regulators might be overlooking something.
- As a new form of money, cryptocurrencies [may] need a **new** regulatory regime – new law and a new way of regulating

Regulatory challenges

Can we rely on intermediaries?

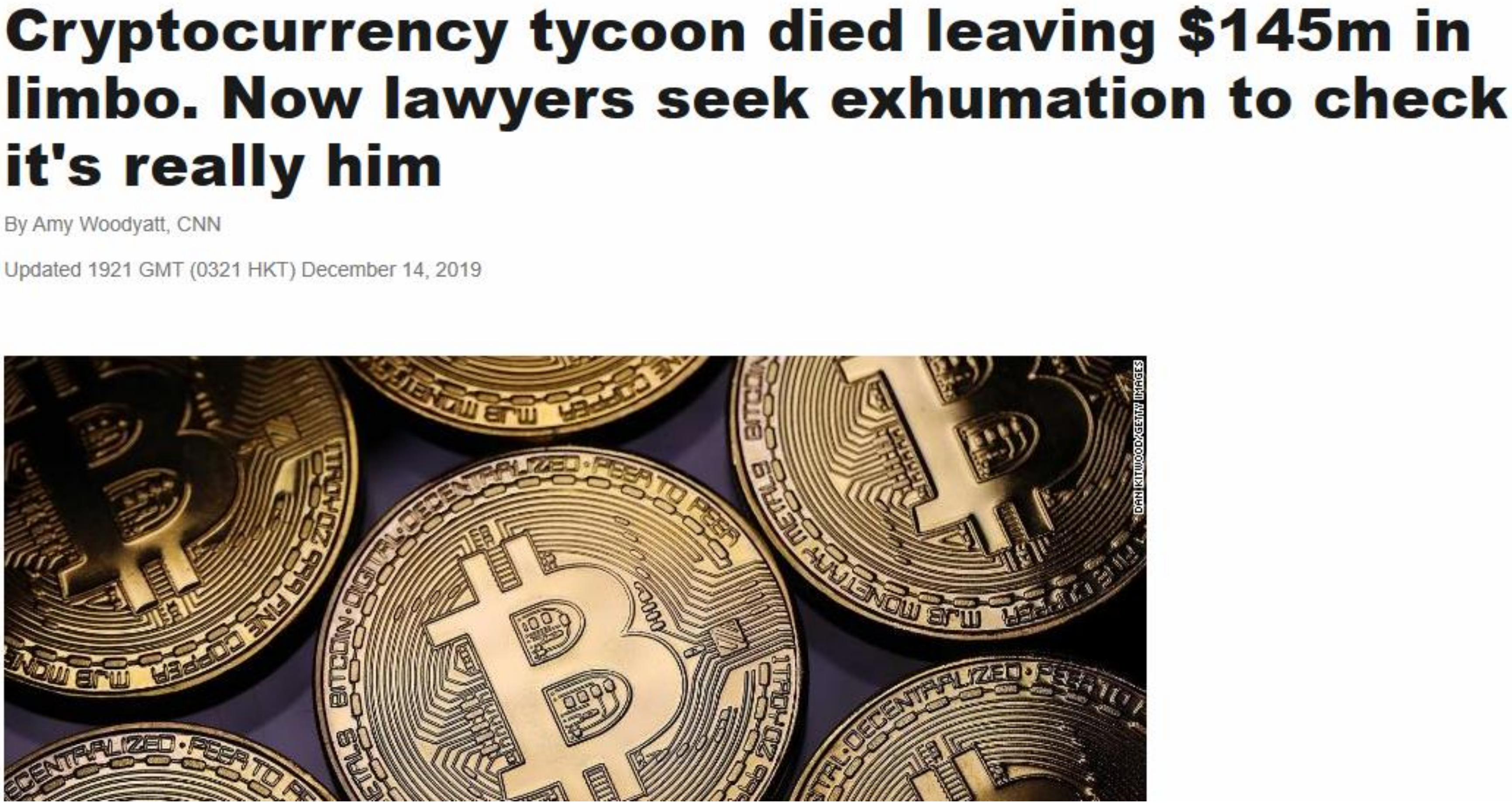
- Core component of [securities] regulation is about regulating the intermediaries.
- Some regulations exist for investor protection.
- Some put the intermediaries in a gatekeeping role at the onboarding process to help prevent criminal activities including money laundering and terrorist financing.
- But what if the platform is distributed, with investors agreeing on trades on their own and using the platform to settle?
- If investors self-custody using their own wallets, **how** do we regulate that?

UNIVERSITY OF MALAWI

Regulatory challenges

- Can we really restrict investors?
- The regulator's mindset
- Fraud?
- *The Blockchain Revolution*

UNIVERSITY OF MALAWI



Cryptocurrency tycoon died leaving $145m in limbo. Now lawyers seek exhumation to check it's really him

By Amy Woodyatt, CNN

Updated 1921 GMT (0321 HKT) December 14, 2019

CryptoTycoon goes to the grave with currency secrets in his crypt – where is the money?

- Cold wallets good to prevent hacking and tracing but …
- Evidence that being secretive can backfire?

UNIVERSITY OF MALAWI

Final thoughts – what is money?

- Can a decentralised currency survive without state guarantee? What will hold its value?
- Are these not another set of Ponzi scheme? Bitcoin especially?
- Extra-territorial challenges on regulation