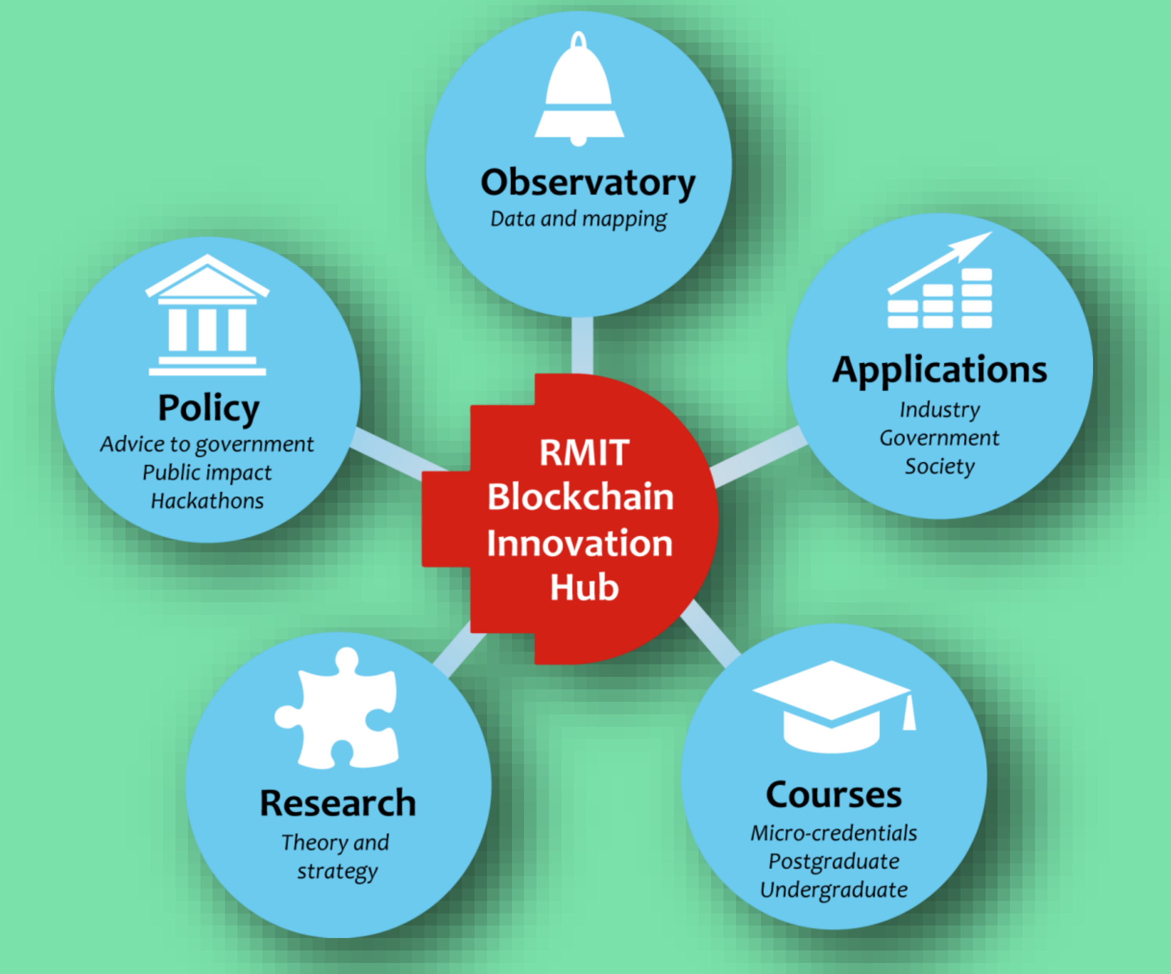
Lurking in the Dark Web: Bitcoin and Criminal Entrepreneurs

Dr Aaron M. Lane
Graduate School of Business and Law
RMIT Blockchain Innovation Hub
RMIT University

Lisanne Adam
Graduate School of Business and Law
RMIT University

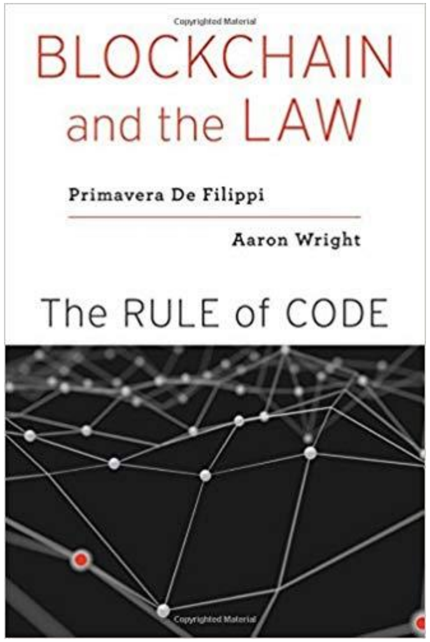
RMIT Blockchain Innovation Hub

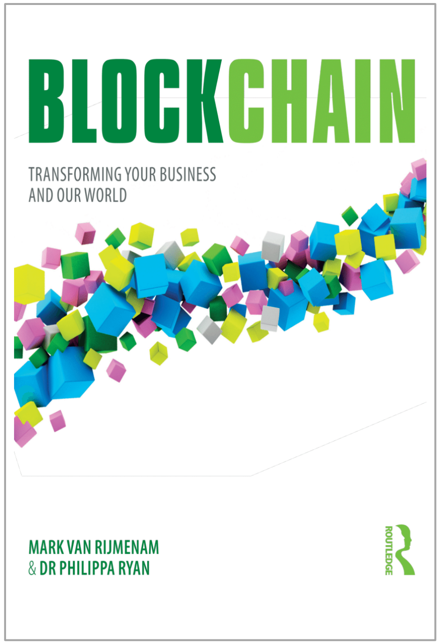


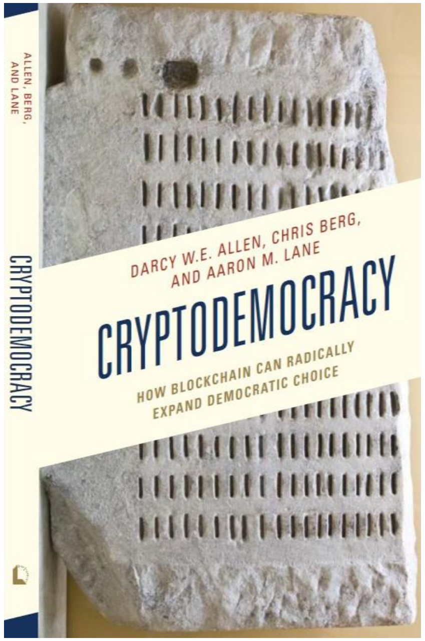
sites.rmit.edu.au/blockchain-innovation-hub/

RMIT
UNIVERSITY

Lawyers are researching in blockchain (with some help from economists)




BLOCKCHAIN
TRANSFORMING YOUR BUSINESS AND OUR WORLD
MARK VAN RIJMENAM & DR PHILIPPA RYAN
ROUTLEDGE


ALLEN, BERG, AND LANE
CRYPTODEMOCRACY
DARCY W.E. ALLEN, CHRIS BERG, AND AARON M. LANE
CRYPTODEMOCRACY
HOW BLOCKCHAIN CAN RADICALLY EXPAND DEMOCRATIC CHOICE

Outline

What we are going to cover today:

- Provide an brief explainer of **blockchain technology and cryptocurrency.**
- Provide a **summary of the first Australian cases.**
- Provide a **thematic analysis of the criminal cases.**
- Consider whether the theory of “**Institutional Cryptoeconomics”** is helpful for explaining the prevalence and motivation of criminal offenders.
- Conclude with **observations** for future cases.

What we are not going to cover today:

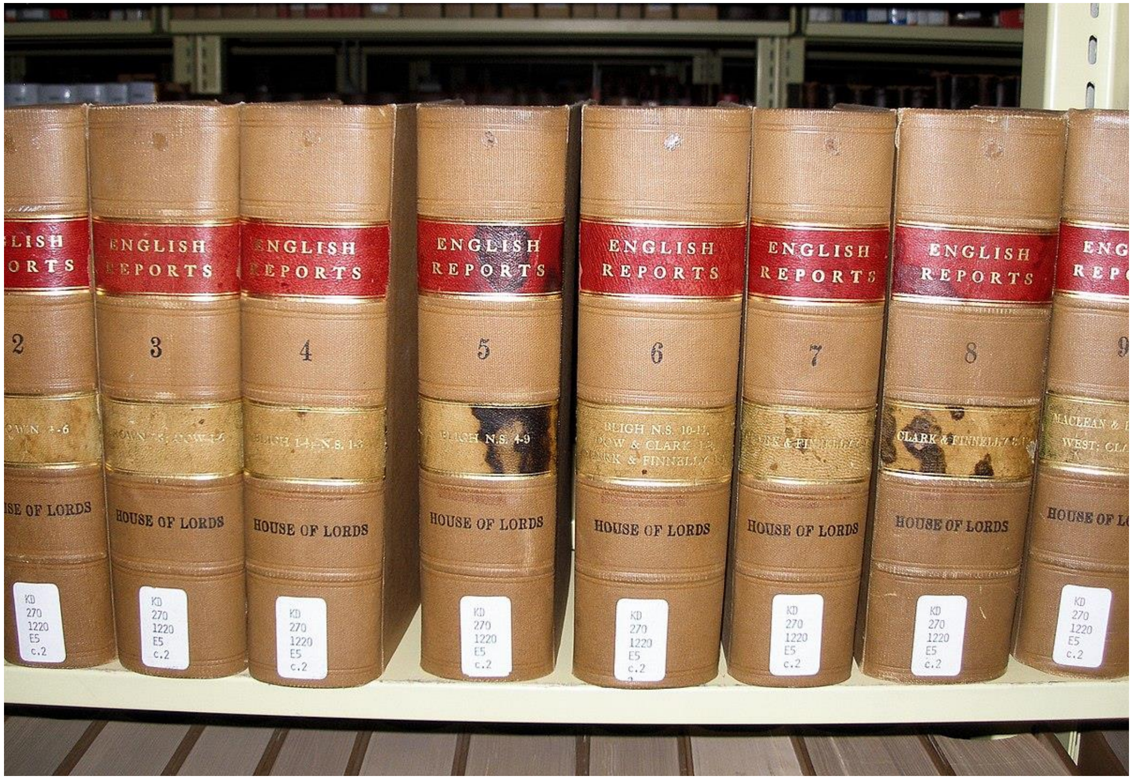
- Explain the gory technical details.
- Provide investment advice about your cryptocurrency portfolio.
- Give you legal advice on your ICO.

RMIT UNIVERSITY

What is blockchain?

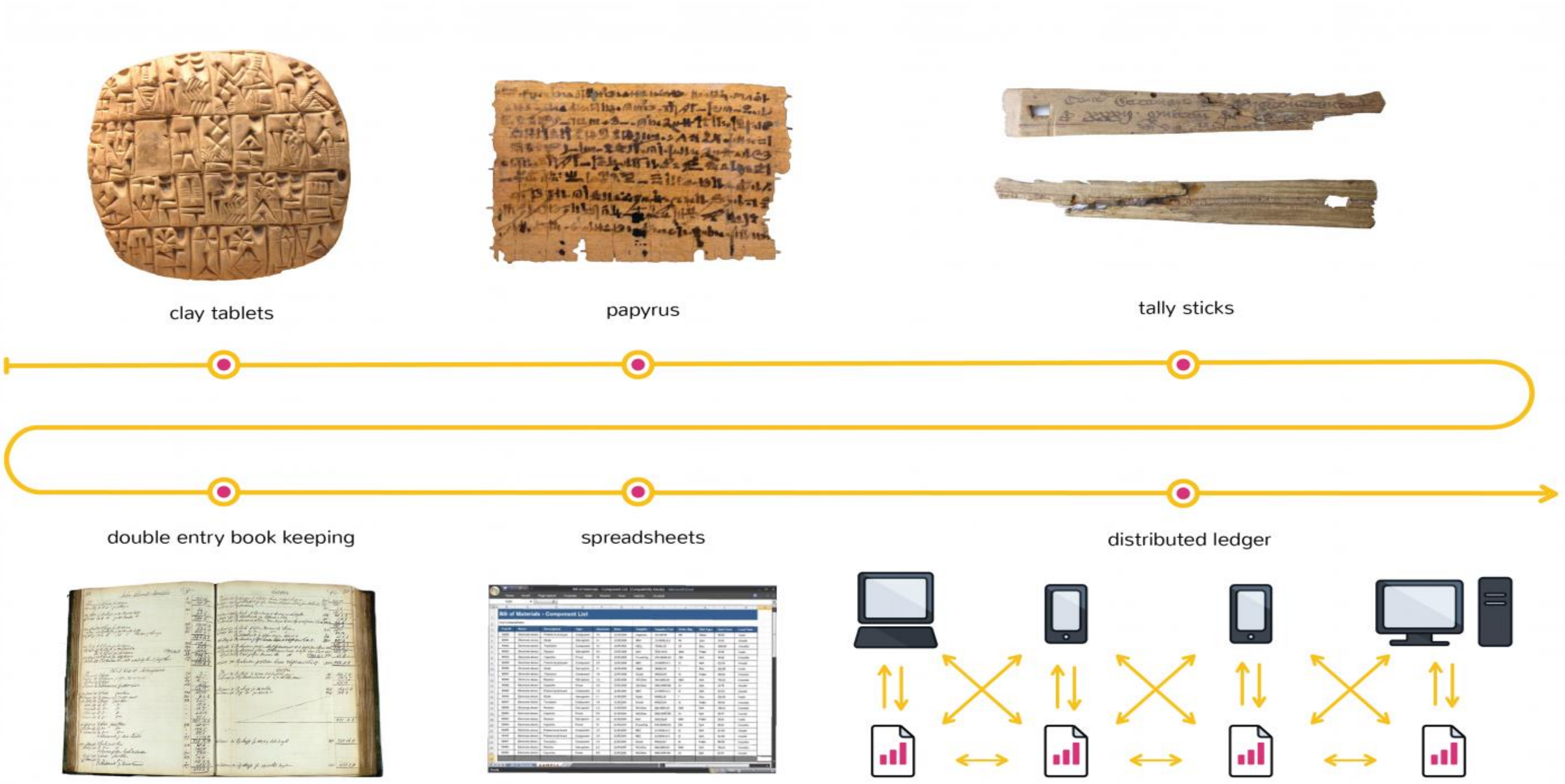
Ledgers record important social facts.

The law is made up of ledgers.



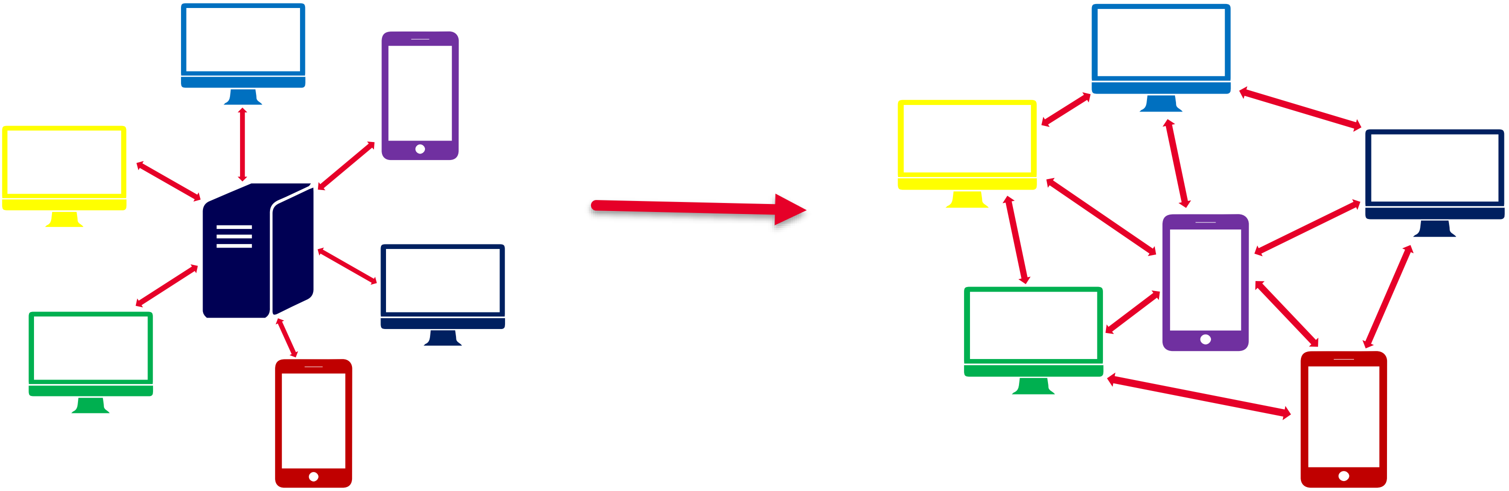
RMIT UNIVERSITY

When ledgers change, society changes.



What is blockchain?

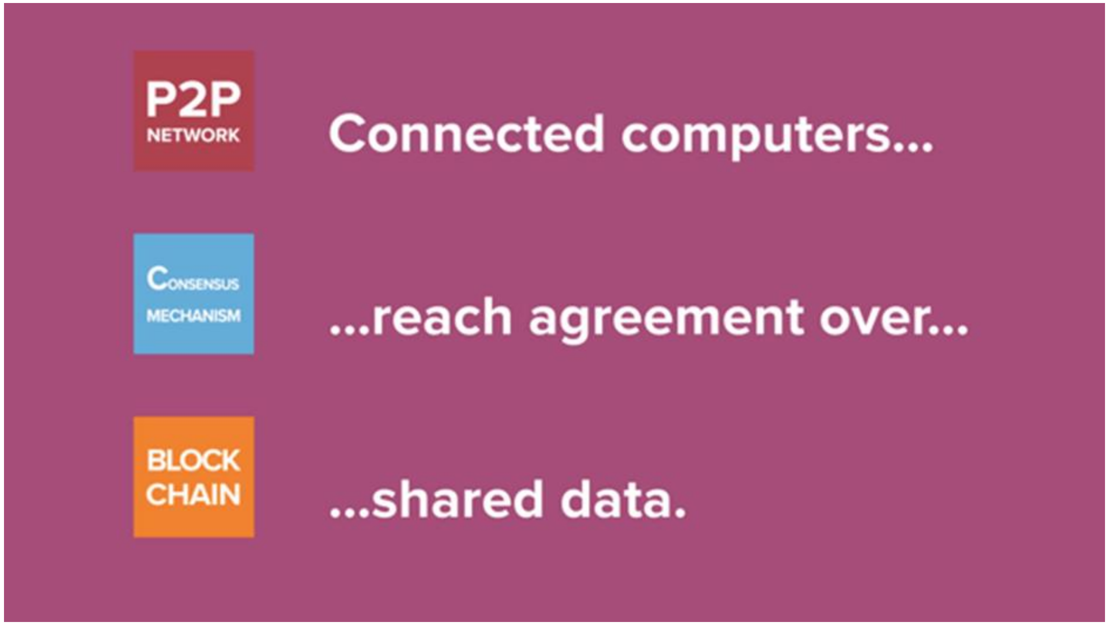
- The blockchain is a decentralised, distributed ledger
- The challenge with a distributed ledger is ensuring everyone agrees what the ledger says



Distributed ledger with central, trusted server

Distributed ledger with distributed consensus mechanism

Blockchain in three steps.



P2P NETWORK

Connected computers...

CONSENSUS MECHANISM

...reach agreement over...

BLOCK CHAIN

...shared data.

A Primer: OK, so what is Bitcoin?

Two dreams about digital currency

- **Native currency for the internet**:
  - “The phrase ‘*the cheque is in the e-mail’*, will soon be as common as its snail-mail equivalent” – *The Age*, 14 February 1995

- **Seceding from the state**:
  - “Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions” – Timothy C. May, *The Crypto Anarchist Manifesto,* 1988.

Prior attempts

DigiCash: Founded in Amsterdam, 1990, bankrupt in 1998

PayPal: Founded in 1998, originally conceived as native digital currency for Palm Pilots

E-Gold: Founded in 1996, 100% backed by gold, shut down by legal action in 2009

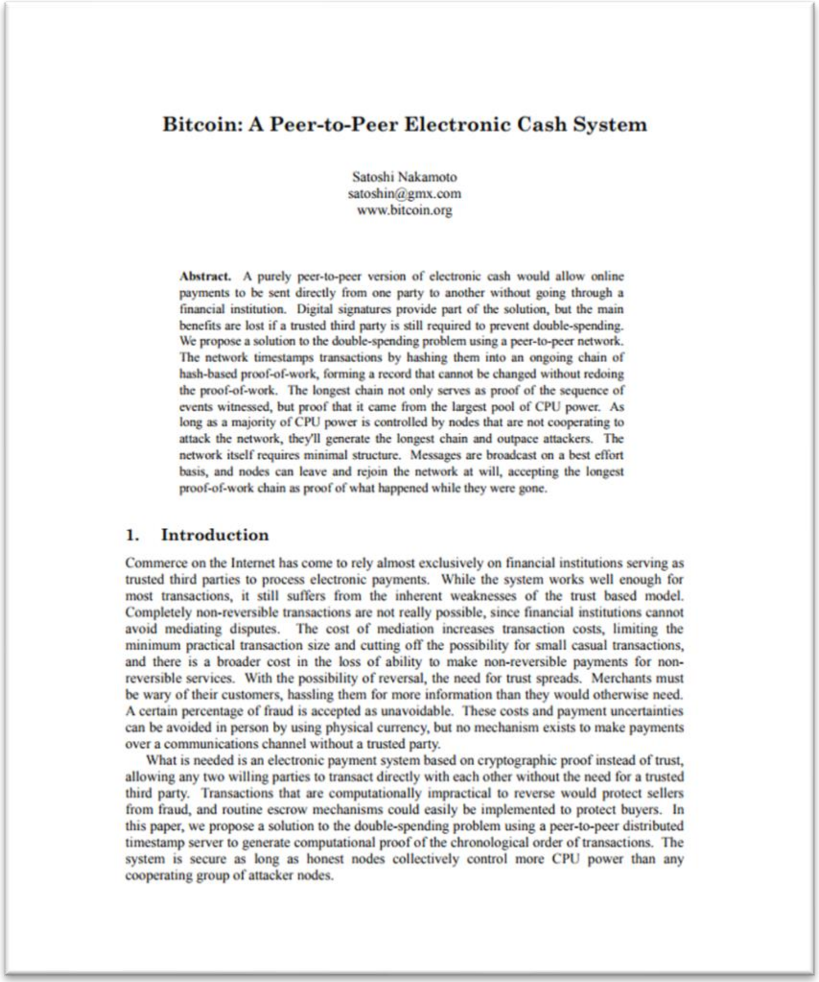
But digital currencies are hard

- **The ‘double spend’ problem**
  - It is trivially easy to copy digital currency
  - Users might try to buy two goods with one currency unit (similar to a counterfeiting problem with physical currency)
- **The Byzantine Generals’ problem**
  - How do we come to consensus over shared facts?
- **Previous digital currencies solved this with centralization**
  - A trusted source verifies transactions and checks for double spending
- **Centralization has its own problems**
  - How trusted is the trusted source?
  - Single point is a security weakness
  - Single entity can be targeted by lawmakers / regulators

Bitcoin solves the double spend problem

- Bitcoin network begun in January 2009
  - “a purely peer-to-peer version of electronic cash ... based on cryptographic proof instead of trust”

- Who is **Satoshi Nakamoto?**
  - Nakamoto (probably) holds around 1 million Bitcoin, the equivalent of AUD$5.4 billion (as of 5 March 2019)



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

The Bitcoin blockchain

- **Bitcoin** is a digital currency powered by a **blockchain**
- Blockchains consist of five complementary technologies that give it its properties of:

Secure:

Asymmetric cryptography and **cryptographic hash functions**

Ledger:

Append-only databases

Distributed:

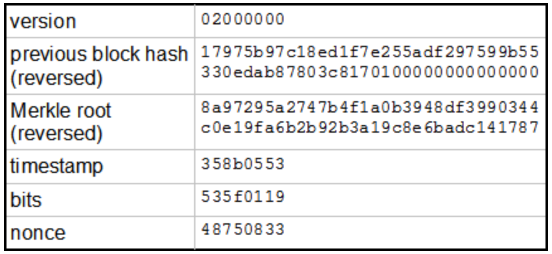
Peer to peer networking

Incentive compatible:

Game theory

Consistent:

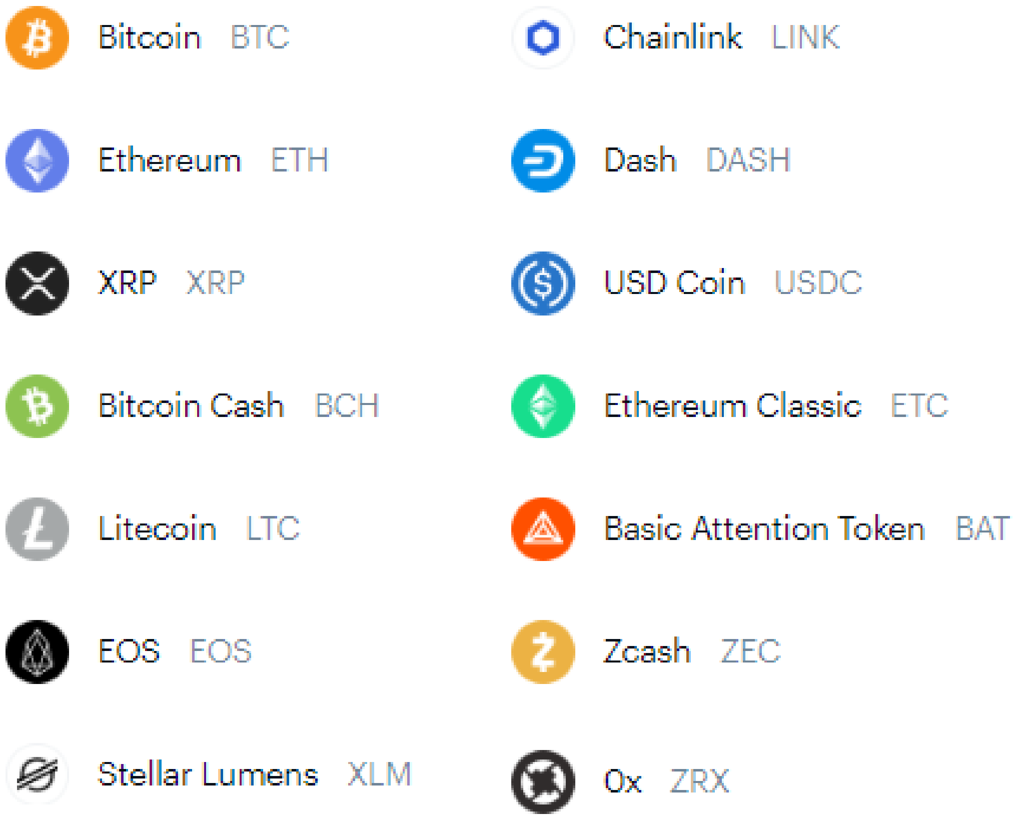
Consensus algorithms



version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833

In 2009, Cryptocurrency = Bitcoin

In 2019, Cryptocurrency =



Bitcoin	BTC
Ethereum	ETH
XRP	XRP
Bitcoin Cash	BCH
Litecoin	LTC
EOS	EOS
Stellar Lumens	XLM
Chainlink	LINK
Dash	DASH
USD Coin	USDC
Ethereum Classic	ETC
Basic Attention Token	BAT
Zcash	ZEC
0x	ZRX

…..plus many more!

A first look at the first wave of cases

Study motivation

- **Bitcoin** has been **described as the “a criminal's laundromat for cleaning money”** (Hyman 2017)
- **Bitcoin is stereotypically associated with cyber crime** with law enforcement experts claiming that it is “**the currency of choice for cybercriminals”** (Brown 2016)
- **Bitcoin** is also the **digital currency of choice** for those wanting to purchase **illegal goods** from **silk road** (Martin 2014; Phelps and Watt 2014; Kethineni et al. 2018).
- **Bitcoin** is one element of a “**cryptomarket**” (Martin 2014)
- More generally, legal scholars have suggested that a **more rigorous approach to doctrinal analysis** is needed – drawing on scientific systematic reviews (Baude et al. 2017; Snel and De Moraes 2018).

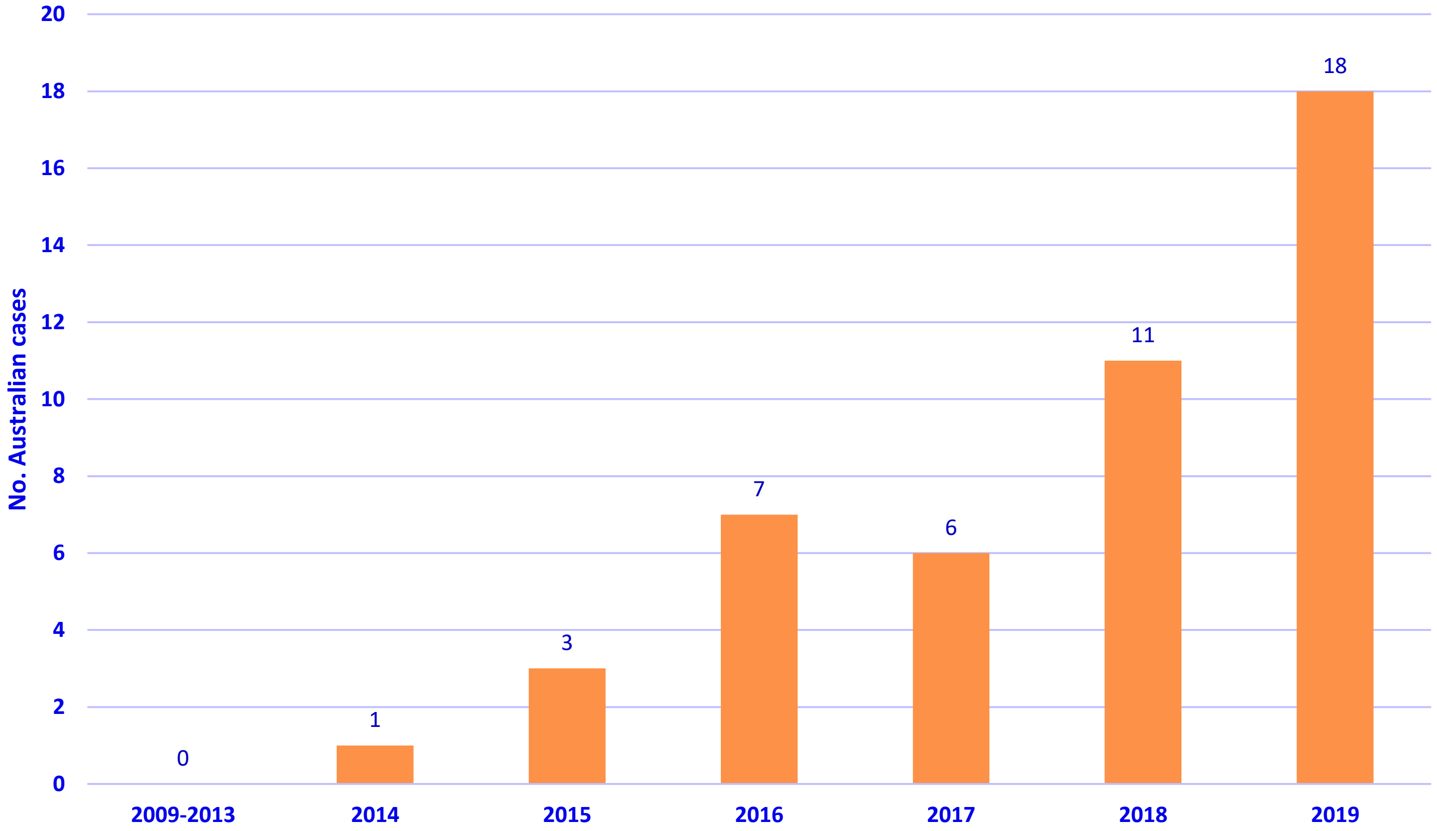
Study design

- **Search of Austlii case database** with a supplementary search conducted using Thomson Reuters Westlaw database**.**
- **Jan 2009 to November 2019** (inclusive)
- Included **all Australian jurisdictions**
- **Search terms:**
  - “Bitcoin”
  - “Ethereum”
  - “Cryptocurrenc*” or “Crypto Currenc*”
  - “Blockchain”
  - “Distributed Ledger”

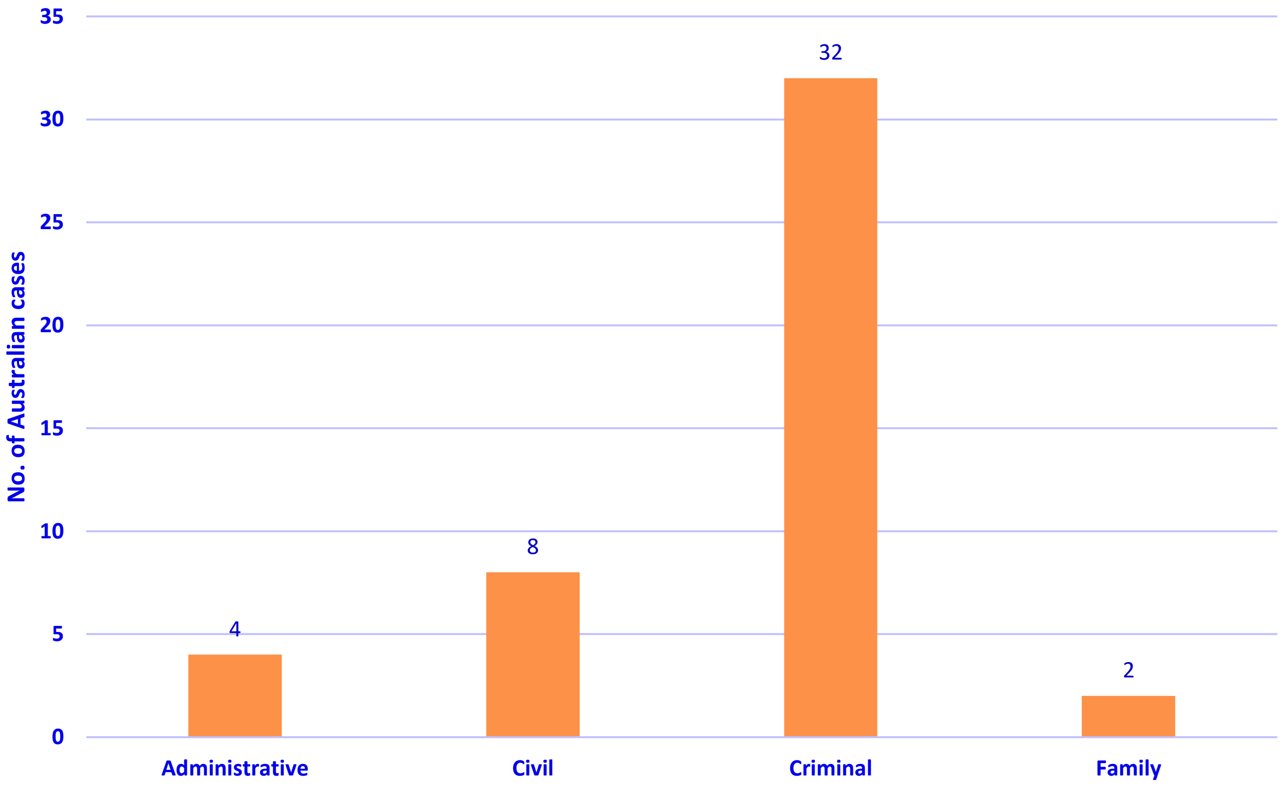
Results:

- 46 reported cases included
- 1 reported case excluded (spelling error of solicitor’s name…!)

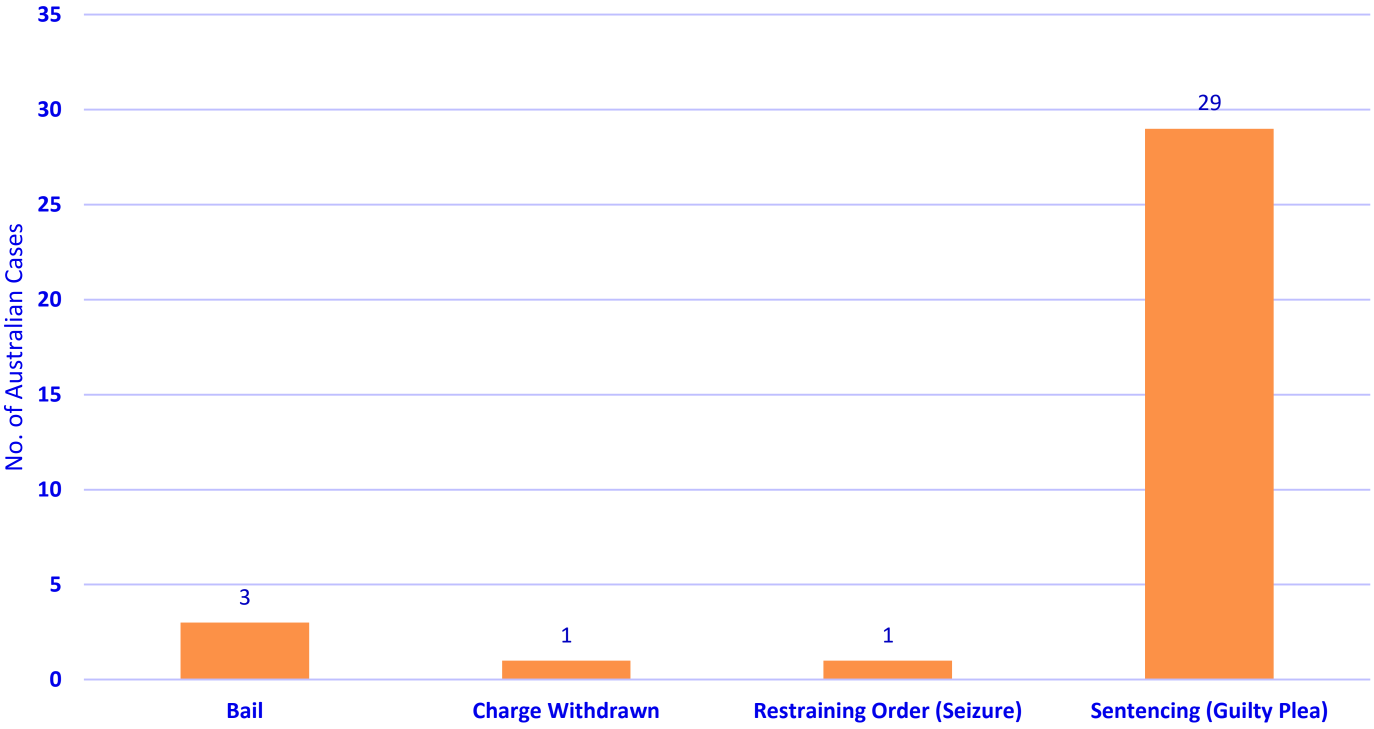
Summary Statistics, cases by year



Summary Statistics, cases by primary matter type



Summary Statistics, breakdown of criminal matters



NB: figures include two administrative cases that refer to previous criminal matters

High-level findings

- The number of cases involving bitcoin or cryptocurrency as part of the factual matrix has increased over time.
- The case research confirms that criminals looking to import drugs or weapons were among the first cohort of cryptocurrency users in Australia.
- The majority of reported criminal cases involve guilty pleas. The case review reveals that offending was caught using “traditional” policing methods.
- In the criminal context, courts have held that use of cryptocurrencies can contribute to the level of sophistication of the offence – becoming an aggravating factor in sentencing.
- Holding cryptocurrency does not appear to be a significant factor in considering the grant of bail.

Theme 1: Sentencing

Does the use of cryptocurrency evidence a sophistication of offending?

Dark Web and Border Controlled Substances

- Purchase or importation of drugs (*N* 24)
- Use of marketplaces on the dark web (*N* 16)
- Firearms (*N* 1)
- Child abuse materials (*N* 1)
- Using cryptocurrency for payment
- Shipping addresses other than residential address
- False identities.

Bitcoin or cryptocurrency on itself is not an aggravating factor. However, this case analysis demonstrates that the use of cryptocurrency in conjunction with the up mentioned factors, contributes to the level of sophistication of the criminal enterprise.

Sophisticated Criminal Entrepreneurs

- ‘Sophisticated’ offenders often had an organisational scheme to import border-controlled substances.

- Often used false identities, a range of shipping addresses, bitcoin and purchased off the dark web.

- New method of drug trafficking not the ‘traditional’ model and the use of this ‘new model’ should be seen as an aggravating feature giving its secretive nature and undetectability (*R v Cooley* [2017] SASCFC 64 [71]).

- “If I pause there for a moment, it causes me some distress that you can press a button on a computer and order such drugs from overseas, and then they come into the country the way they do. It is far too easy. But still, that is what is happening, and that is what you did” (*DPP v Ragauskas* [2016] VCC 1232[65]).

Some examples

Sentence appeal: ***Tran v The State of Western Australia* [2019] WASCA 50** [2]:

…There is no merit in the submission that the learned sentencing judge erred in finding that the appellant's offending was sophisticated and brazen. The appellant attempted to conceal his activities by using the darknet and by making payments via Bitcoin, plainly with the intention of making his wrongdoing more difficult to detect. These measures may be properly characterised as sophisticated.

Sentence appeal: ***Dunning v Tasmania* [2018] TASCCA** [10]:

…Some factors which are relevant to the need for general deterrence in this case include the quantity of the drug involved, in particular the amphetamine, the grave social consequences which would flow from the dissemination of that drug in that quantity, the difficulty of detecting the crime, which depended upon effective and comprehensive surveillance of the enormous volume of postal articles coming into the country, and your use of covert websites and digital currency to complete the transaction.

Sentence appeal: ***Edmonds v The Queen* [2019] NTCCA 1** [28]:

…the use of Bitcoin and the dark web in order to purchase the drugs elevated the gravity of the offending because it demonstrated a degree of sophistication (of a sort), and it gave rise to obvious and intended difficulties in detecting the activity”

RMIT UNIVERSITY

‘Unsophisticated’ offenders

- This category of offenders often involved individuals that purchased the drugs for their own consumption and had these drugs shipped to their residential addresses.

- Degree of naivety relevant when assessing offence gravity (in particular seriousness of the offence)

- In these cases, the majority of the defendants plead guilty.

Examples

***R v NE* [2015] ACTSC 352** [25]:

On the other hand, for the first relevant importation NE used his own home address. He applied for the post office box in his own name and the packaging, including those that went later to his friend’s post office box, were all addressed to him in his own name. He also used his own mobile phone. This showed a degree of naïvety or unsophistication in the enterprise.

***DPP v Gould* [2016] VCC 22** [26]:

Your counsel submitted that the importations were unsophisticated. You did not expect the drugs to arrive after you ordered them on the internet. Your counsel also submitted that your trafficking was naïve, without you understanding the seriousness of what you were doing or perhaps even that it constituted trafficking, given the motivation and the absence of a profit motive. These propositions were not challenged by the prosecution and I accept that there is a valid point to be made.

Protect the offender from prisoners that are interested in his skillset

***The Queen v Meginess* [2019] NTCA 5 [12]:**

His Honour expressed concern that a term of actual imprisonment could adversely affect the respondent's prospects of rehabilitation and risk his **falling into the company of 'new friends' who could take advantage of the respondent's skill and experience in accessing the dark web and using bitcoin to purchase dangerous drugs**. His Honour expressed the view that it was in the interests of the community primarily, that the respondent not be sent to prison.

Crown argued the sentence was manifestly inadequate. Sentence aggregated to three years imprisonment.

Theme 2: Bail

Is an accused’s possession of cryptocurrencies relevant for deciding a grant of bail?

Bail applications

- The study findings show three bail applications.

- In all three cases, bail was refused.

- In all three cases, the Court determined that the Crown had a strong case against the accused (NB: onus on was on the applicant – different tests applied in different jurisdictions).

- Offence gravity (in particular; seriousness of offence) in relation to sophistication and deception relevant by considering bail applications.

Bitcoin and technical skill increases flight risk

***RE Brendan Baker* [2018] ACTMC 27 [23]-[24]:**

> “Constable Hawke said that she is aware that if the applicant is released he will have access to funds and is well supported financially in that regard. Constable Hawke suggested there is intelligence evidence to suggest that the applicant purchased significant bitcoin or crypto currency for the purposes of importing the drugs.
>
> There is no indication as to where that crypto currency is at the present time and given the restraints on the applicant’s assets the concern is that he will access the crypto currency for the purposes of escape.”

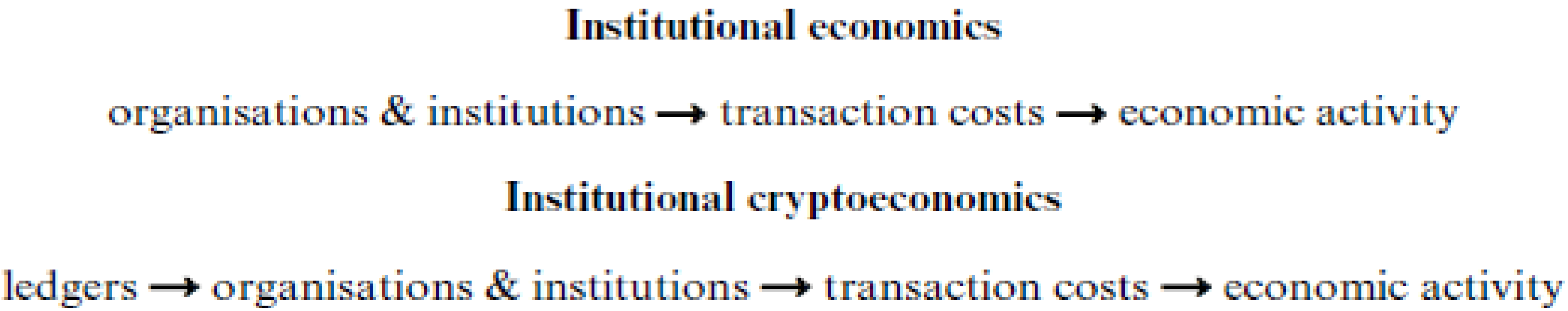
This argument did not appear to be accepted by the Court as SM Hunter stated at [53] that “I consider risk of flight is a low level risk which could be mitigated by conditions.”

Concluding Observations

RMIT UNIVERSITY

Applying Institutional Cryptoeconomics

- Although the **Law and Economics of crime** has typically focussed on **optimal criminal sanctions** (e.g. Becker 1968; Posner 2014), **crime can be understood** as **economic exchange** (e.g. Dick 1995).
- Here, we apply **Institutional Cryptoeconomics** (Berg, Davidson and Potts 2019) understand why cryptocurrencies are an attractive payment method.



Institutional economics

organisations & institutions → transaction costs → economic activity

Institutional cryptoeconomics

ledgers → organisations & institutions → transaction costs → economic activity

Applying Institutional Cryptoeconomics

Proposition:

- **Blockchain does not create better drugs or weapons, instead as an institutional technology** it lowers the transaction costs of committing crime by industrialising trust and limiting opportunism.

Predictions:

- as blockchain lowers the transaction costs of exchange generally, **more crime is shifted to digital environment**
- as blockchain lowers the costs of enforcement, **crime is less violent.** This is consistent with the "gentrification hypothesis" – i.e. the potential "crypto markets are displacing potentially violent drug market norms in favour of more cordial relationships between market participants" (Martin 2018).

Observations for Future Cases

Evidentiary Issues

- This study presents mostly guilty pleas – in the future contested hearings are likely.
- There is a live question about the admissibility of “block explorer” evidence and the use of services for investigative purposes (see: *R v Adams* (No 5)).

Discharging the Stereotype

- If Bitcoin and cryptocurrencies are seen with suspicion then this raises an issue for the presumption of innocence**.**

Professional Development

- Advocates will need to be technology literate in order to seek appropriate court orders, review expert witness reports, and understand the commercial and legal significance of transactions.

Questions and Feedback

RMIT
Blockchain
Innovation
Hub

RMIT
UNIVERSITY