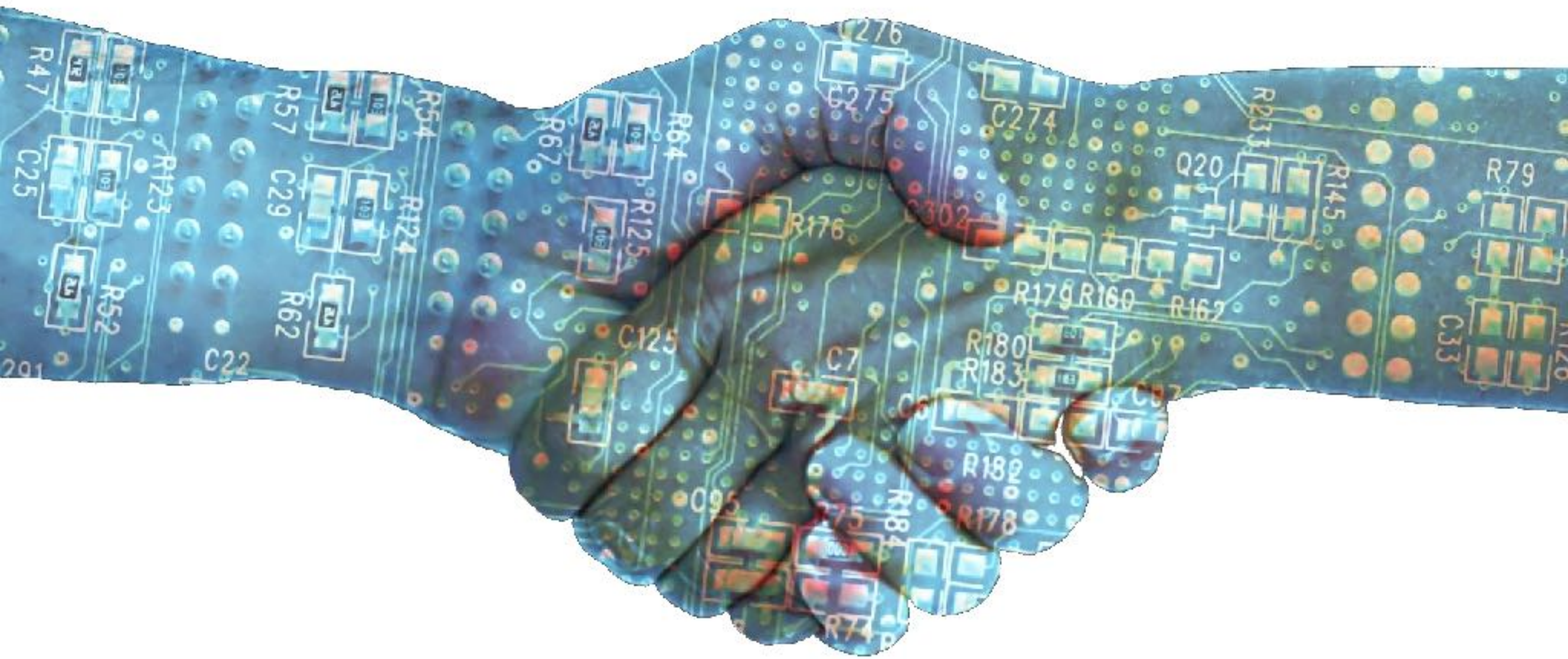
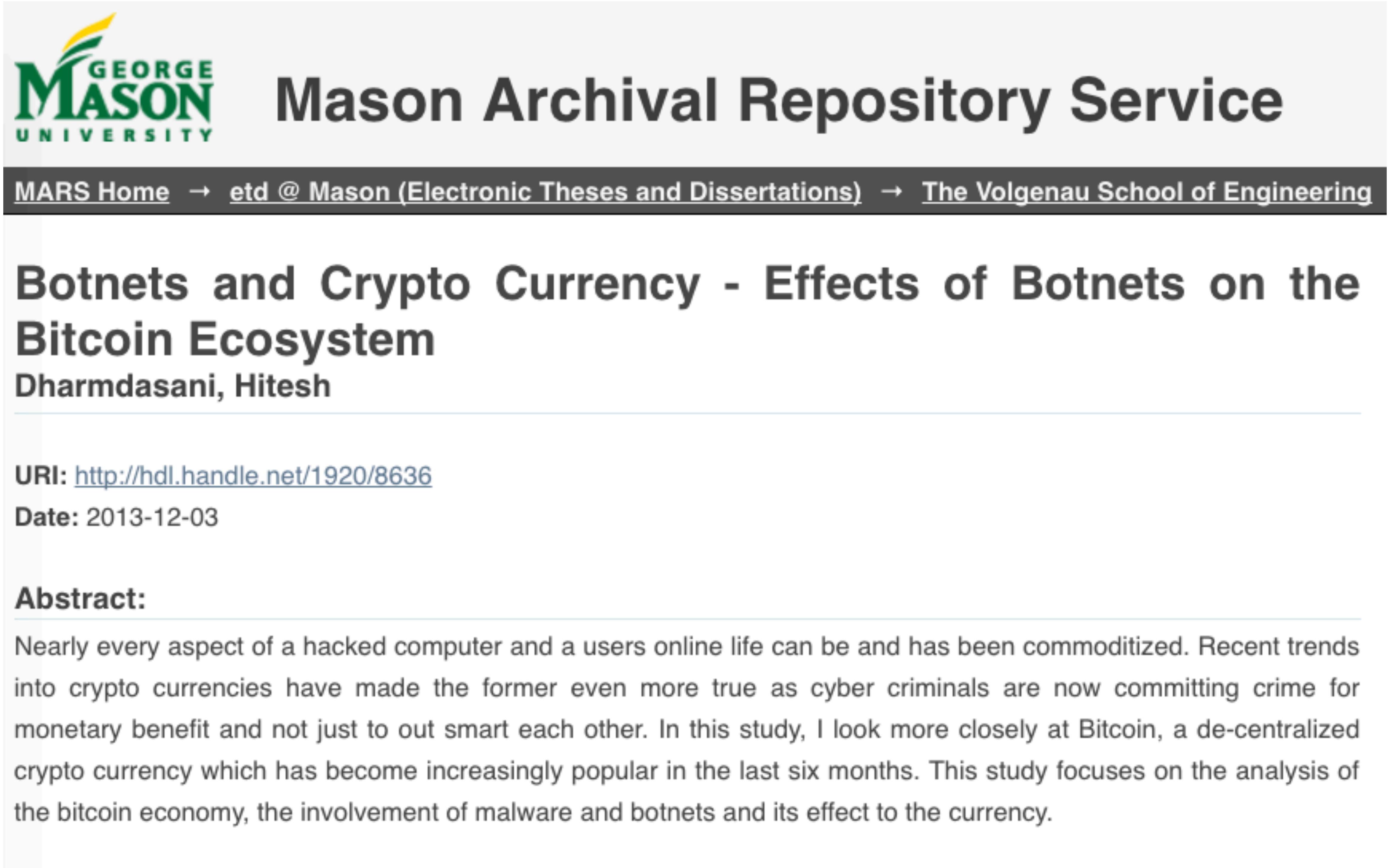


Blockchain

Building trust where there is none

Hitesh Dharmdasani
Informant Networks



Mason Archival Repository Service

MARS Home → etd @ Mason (Electronic Theses and Dissertations) → The Volgenau School of Engineering

Botnets and Crypto Currency - Effects of Botnets on the Bitcoin Ecosystem

Dharmdasani, Hitesh

URI: http://hdl.handle.net/1920/8636

Date: 2013-12-03

Abstract:

Nearly every aspect of a hacked computer and a users online life can be and has been commoditized. Recent trends into crypto currencies have made the former even more true as cyber criminals are now committing crime for monetary benefit and not just to out smart each other. In this study, I look more closely at Bitcoin, a de-centralized crypto currency which has become increasingly popular in the last six months. This study focuses on the analysis of the bitcoin economy, the involvement of malware and botnets and its effect to the currency.

Bitcoin since 2012

Also, Regret giving 100 Bitcoin to people for free in 2012

Not going to mention Bitcoin

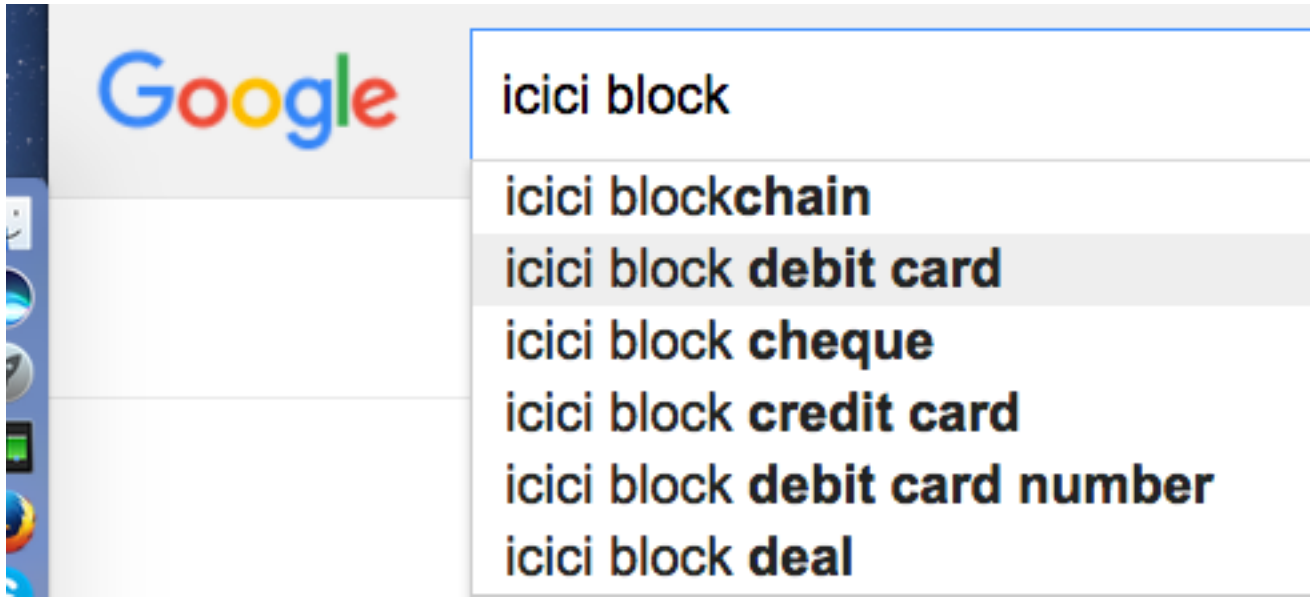
Blockchain

Decentralisation and Openness

What Blockchain is doing to Record Keeping
is what
Internet did to Communications

Where things are

- BoA and Merrill Lynch working with MS
- ICICI did a proof of stability with their transaction this week



icici block

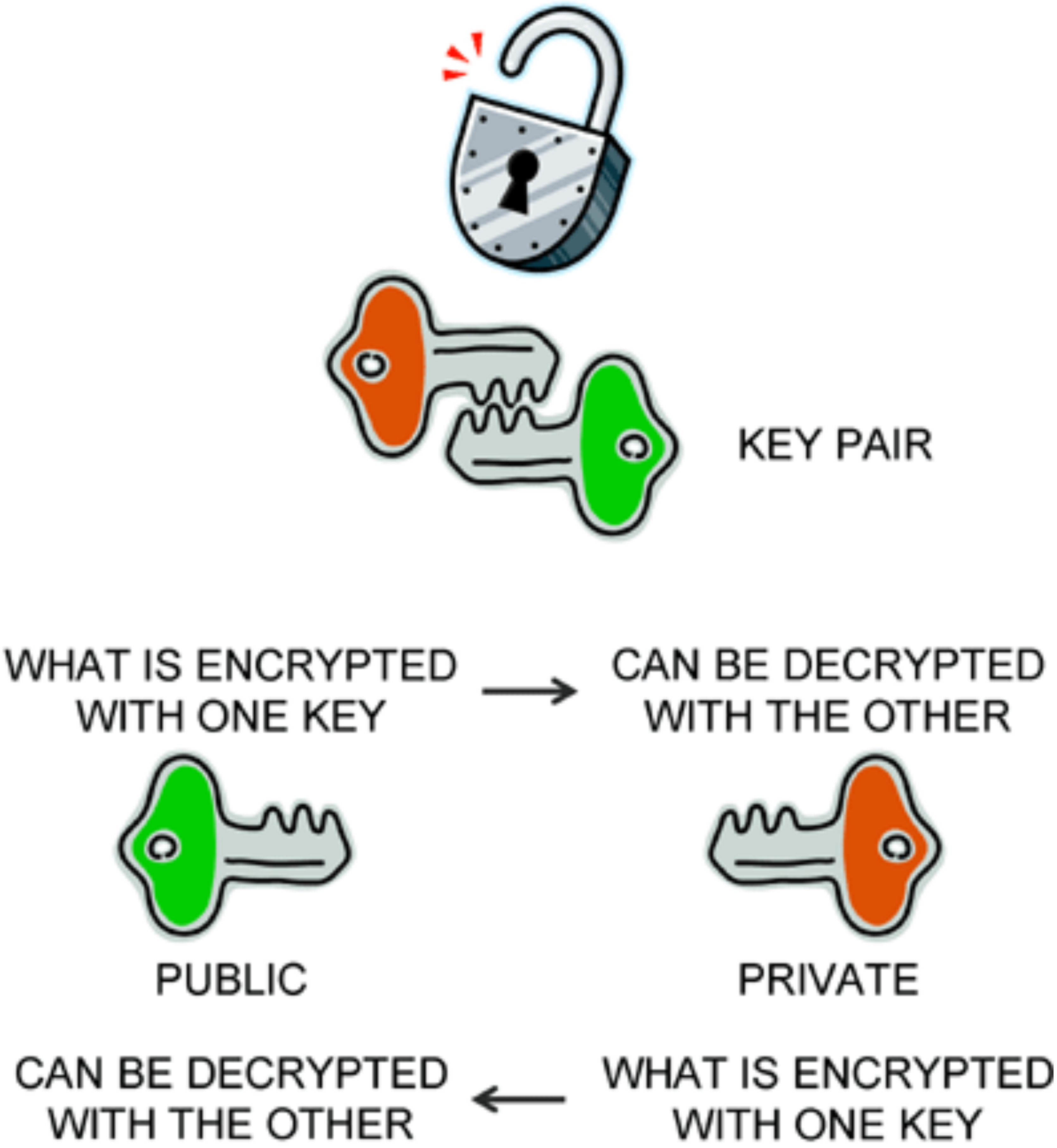
icici block**chain**
icici block **debit card**
icici block **cheque**
icici block **credit card**
icici block **debit card number**
icici block **deal**

Blockchain

- Paradigm shift. Radically challenging the status quo in record keeping
- Distributed Ledger i.e. everyone has a copy
- Trust is based on maths rather than “because i say so”
- X gives Y, A receives from B. Ownership graph!

Extremely Powerful System

HTTPS runs on the principle



KEY PAIR

WHAT IS ENCRYPTED WITH ONE KEY → CAN BE DECRYPTED WITH THE OTHER

PUBLIC

PRIVATE

CAN BE DECRYPTED WITH THE OTHER ← WHAT IS ENCRYPTED WITH ONE KEY

Public Key is given to the world (your identity on the blockchain. i.e. account number)

Private key is a secret passcode

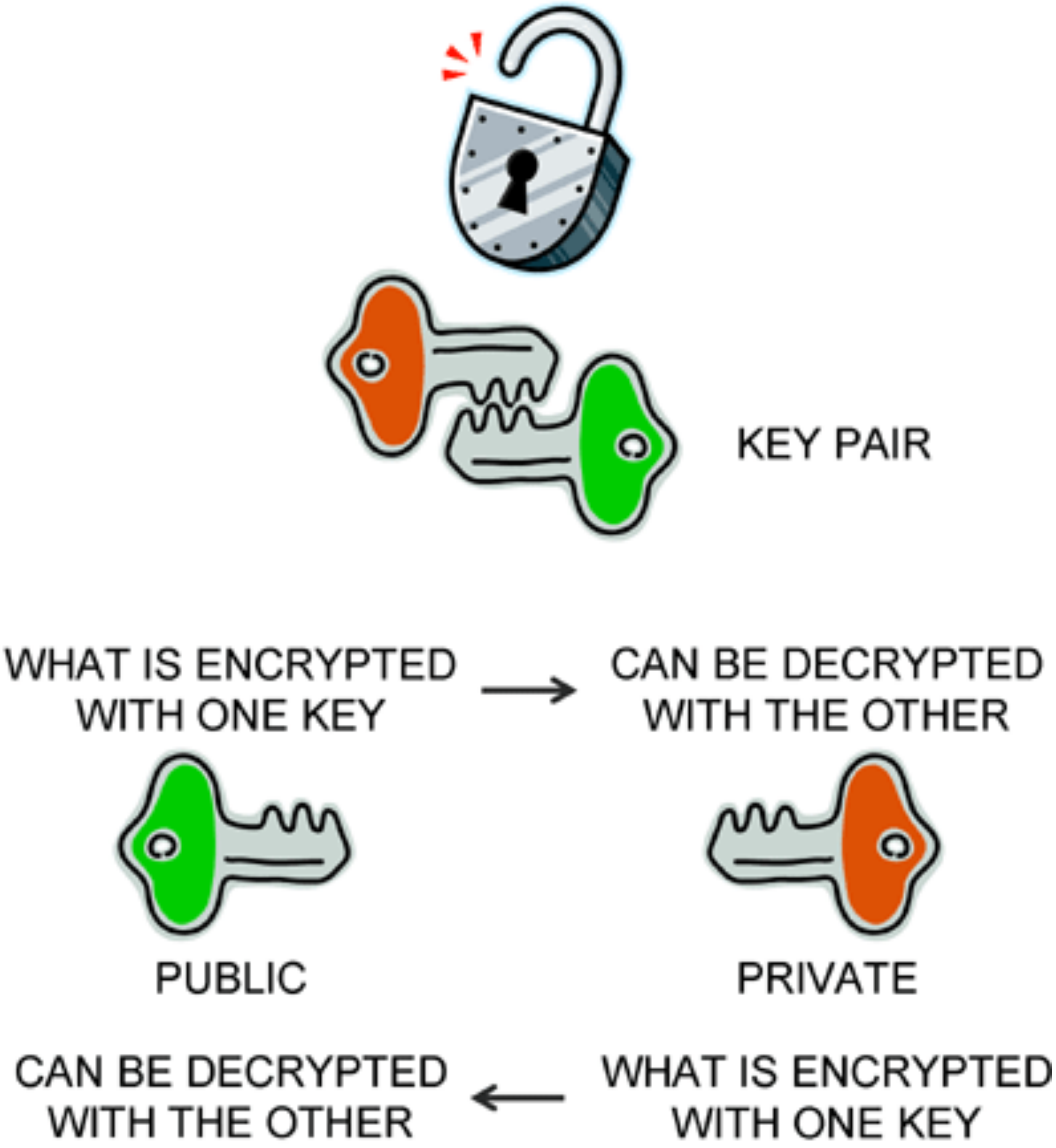
Which means?

- If someone can unlock using public passcode. they know I (user) locked it

- If someone(user) can unlock using private passcode. they know nobody else saw it

- If someone can unlock using public passcode. they know I (user) locked it

- Only the owner of the private code can see/receive the message



WHAT IS ENCRYPTED WITH ONE KEY → CAN BE DECRYPTED WITH THE OTHER

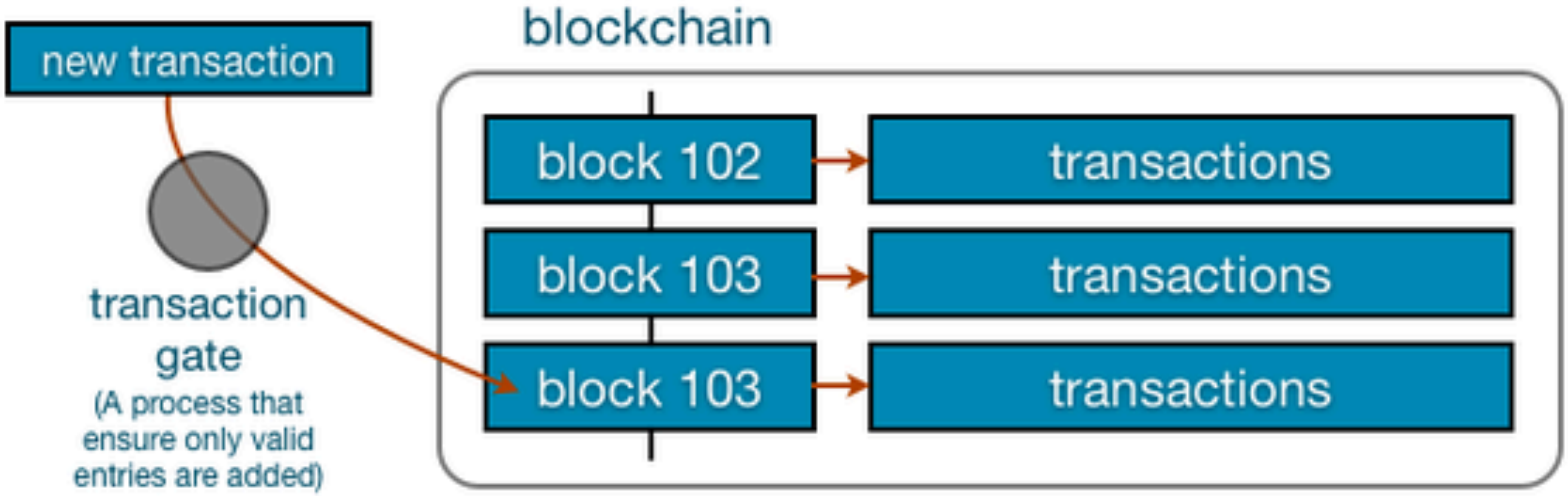
CAN BE DECRYPTED WITH THE OTHER ← WHAT IS ENCRYPTED WITH ONE KEY

Which also means?

- I can write a transfer note (IOU)
  give 1000 INR to TIE
- Lock this note
  - 1st with my private passcode (So they can verify that Hitesh sent it)
  - 2nd with their own private passcode (So they can keep the note for future transactions)

How blockchain works

A blockchain is a database shared by every participant in a given system. The blockchain stores the complete transaction history of a cryptocurrency or other record keeping system.



Transactions aren't recognized until they are added to the blockchain. Tampering is immediately evident, and the blockchain is safe as record because everyone has a copy. The source of discrepancies is also immediately obvious.

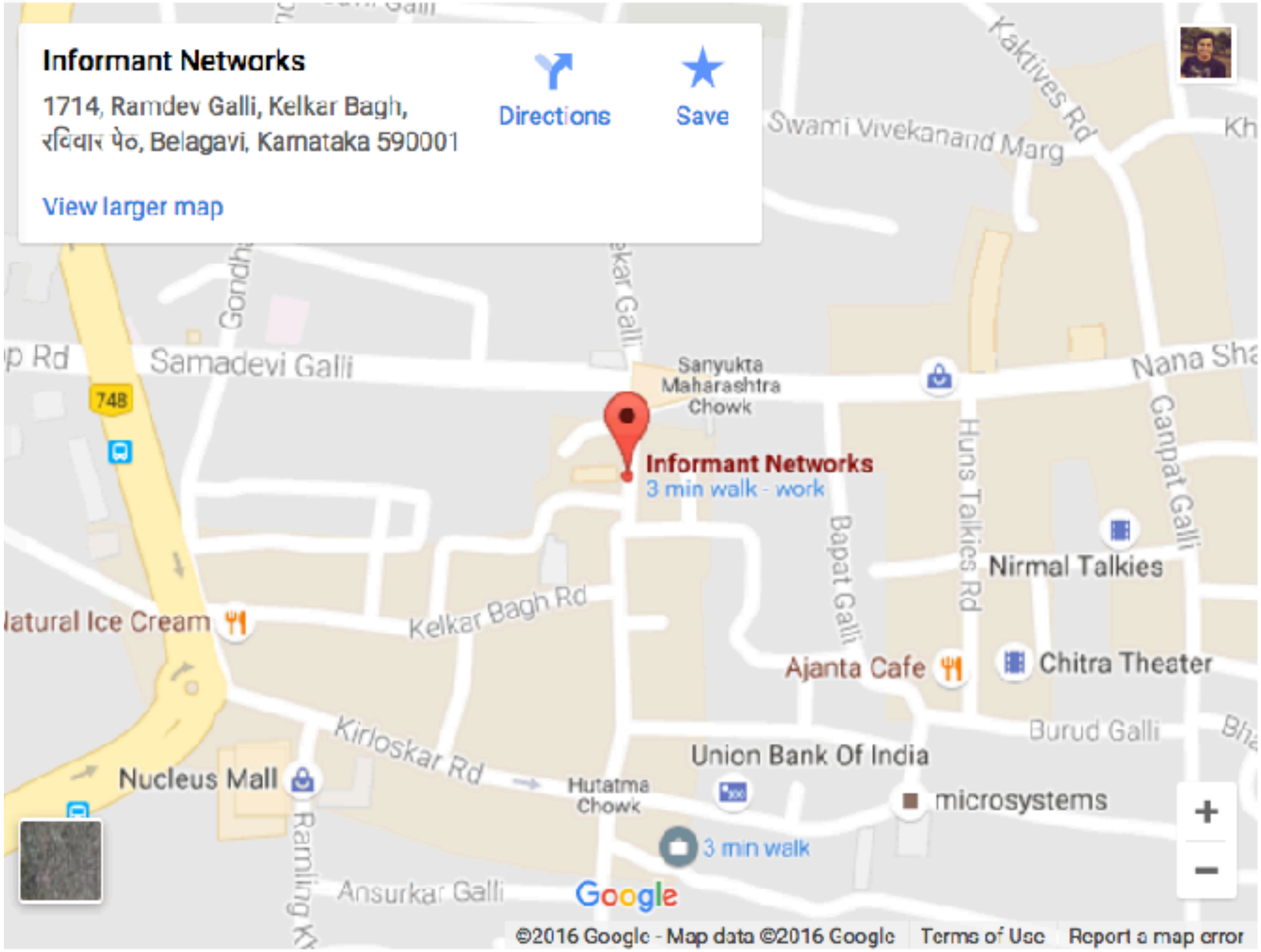
Heavily Tuneable

- Settlement every x minutes
- Type of record does not matter. i.e. money, chocolates
- Corruption/Fraud is immediately evident

One sort of `con`

- Cant rollback. Unlike Credit/Debit transactions

- Escrow to the rescue



Informant Networks
1714, Ramdev Galli, Kelkar Bagh,
रविवार पेठ, Belagavi, Karnataka 590001

Contact

Informant Networks
3rd Floor,
1714 Ramdev Galli,
Belgaum, Karnataka, India - 590001

☎ P: +91-9880936126, +91-9972713357

✉ E: hello@informantnetworks.com

Questions?

Anything related to a computer will do