



On-going research in Blockchain

Ashish Rajendra Sai



About me

Researcher - Horizon Globex

Ph.D. Candidate - University of Limerick
Security evaluation of PoW Blockchain

M.Eng. - University of Limerick
Information and Network Security

B.Tech. - RTU
Computer Science and Engineering

For more information visit [ashishrsai.github.io](https://github.com/ashishrsai)



Blockchain Interest Group (BIG)- UL

Research in Blockchain Interest Group is focused on evaluating the privacy and security of distributed ledger technology.



Dr. Farshad Toosi

Farshad is a post doctoral researcher at Lero.



Ashish Rajendra Sai

Ashish is a Ph.D. candidate at Lero.



Dr. Jim Buckley

Jim Buckley is a senior lecturer at the University of Limerick, Ireland.



Dr. Andrew Le Gear

Andrew is the CTO of Horizon Globex.

More about the research projects in a bit.
For more info on BIG visit - bigireland.github.io

Outline

What is Blockchain?

Blockchain = Cryptocurrency?

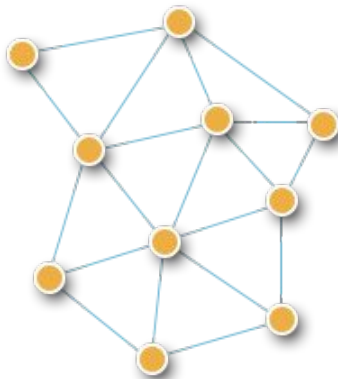
On-going Research

- Security-Centralization-Inequality
- Fraud-Transaction-Analysis

Things we need to know before we look at blockchain

1) Distributed Computing (Specifically Peer to Peer Network)

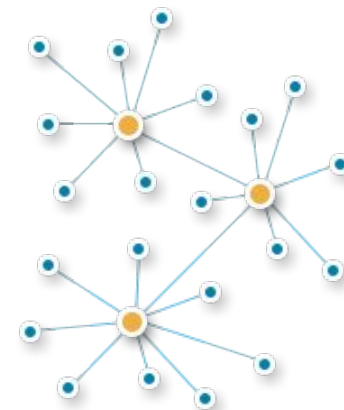
Distributed



Centralized

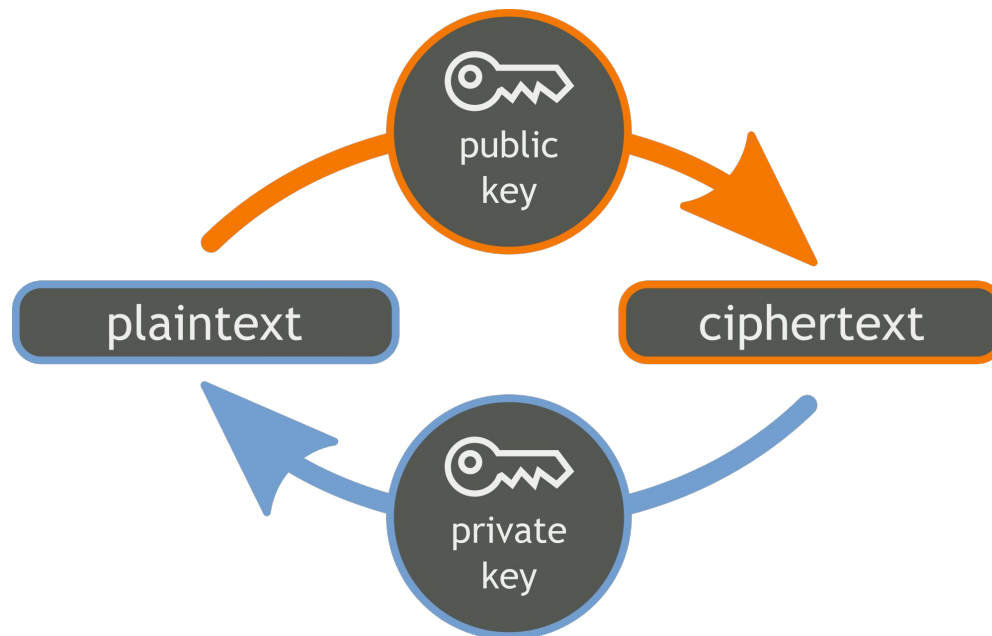



Decentralized



Things we need to know before we look at blockchain

2) Cryptography = The art of writing or solving codes.



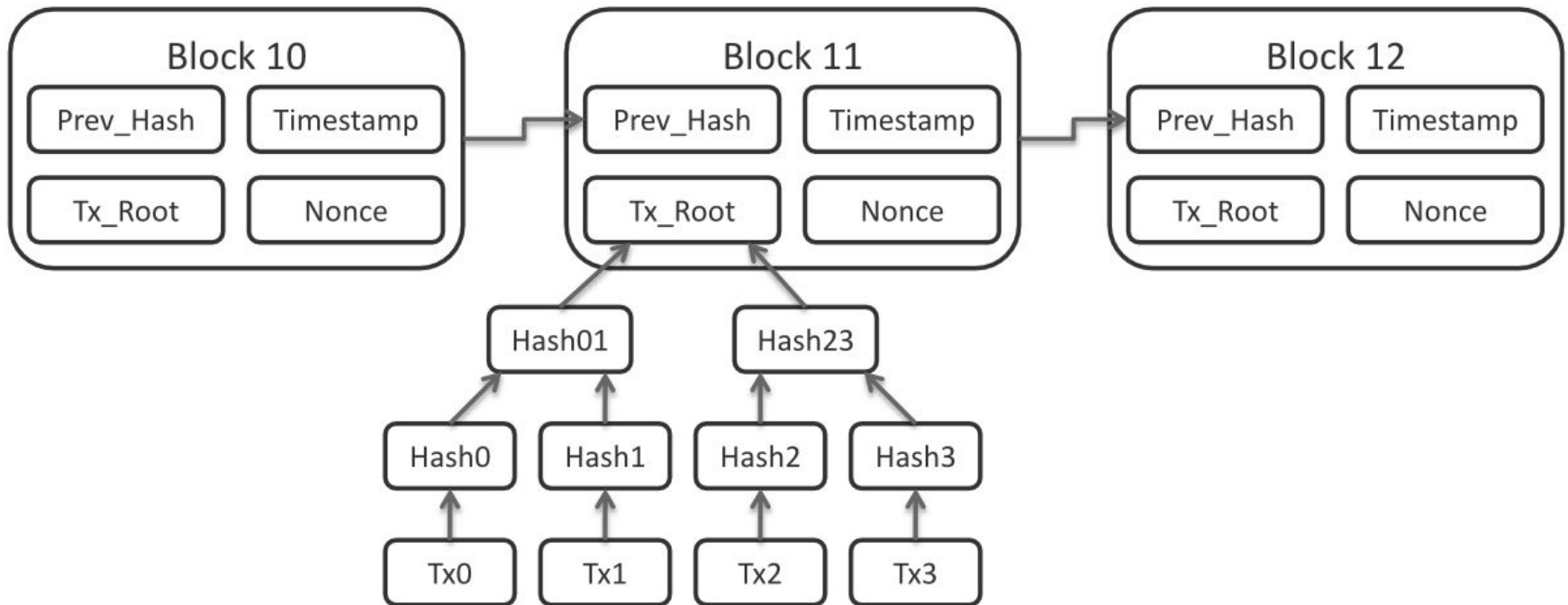


What is Blockchain?

The term blockchain was first used by Satoshi Nakamoto (Bitcoin) in a GitHub commit to refer to a *cryptographically linked data structure*.

Main Property => Append Only

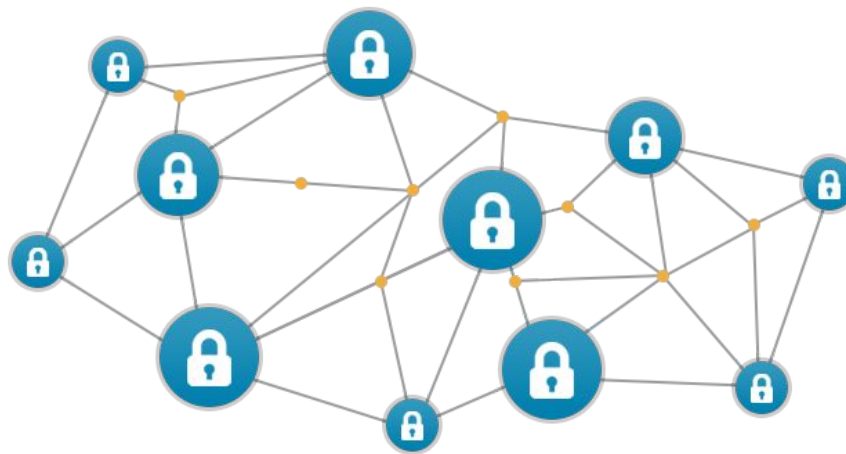
Blockchain



So blockchain is a data-structure?

The term blockchain is used as an umbrella term to refer to the broader field of Distributed Ledger Technologies (DLT).

DLT = Distributed Systems (Consensus) + Blockchain (Data Structure + Cryptography)





Popular consensus mechanism in DLT

Proof of Work

Requires participants to perform an expensive computational task to become the coordinator. Execution of this computational task is known as Mining.

Proof of Stake

Requires participants to put a Monterey stake on the network. On malicious behavior, the participant risks lose of the stake.



Cryptocurrencies - Bitcoin, Ethereum (Ether)

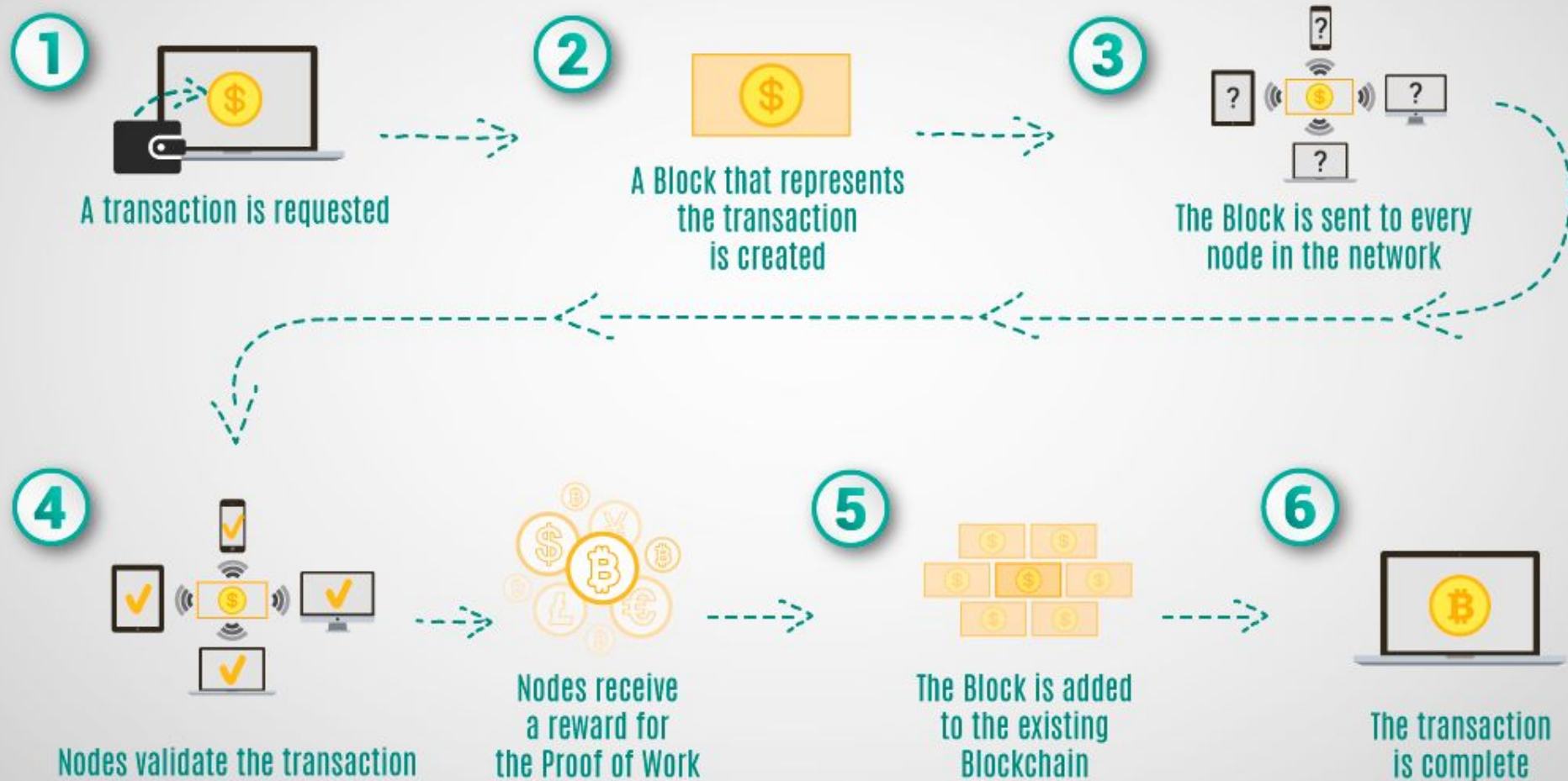
Bitcoin

A decentralized distributed system with clever proof of work based consensus mechanism + chain of blocks of transactions (aka blockchain).

Ethereum

A decentralized distributed system with clever proof of work based consensus mechanism + chain of blocks of transactions (aka blockchain) + Turing complete virtual machine for executing smart contracts.

How exactly does Bitcoin work?





**Blockchain =
Cryptocurrency ?**

**Not really, Cryptocurrency is
one of many applications of
Blockchain (or more precisely
Distributed Ledger
Technology)**



**DLT is still in an early stage of development;
thus it presents many research opportunities.**

The blockchain interest group (BIG) at the University of Limerick focuses on two main research areas of Blockchain = Privacy and Security.



Security

Open network + Monetary value = Goldmine for hackers

A total of **US\$ 3.55B** has been lost due to attacks on cryptocurrencies since 2010 [Chia18].

Chia, V., Hartel, P., Hum, Q., Ma, S., Piliouras, G., Reijnders, D., van Staaldhinen, M. and Szalachowski, P., 2018. Rethinking Blockchain Security: Position Paper. *arXiv preprint arXiv:1806.04358*.

Types of attacks on Blockchain

OPSEC

Traditional Information system security threats.

Smart Contracts

Security vulnerability in the contract deployed over blockchain (e.g. Ethereum contracts)

Consensus Protocol

Threats to the consensus mechanism used in the distributed computing component.

Consensus Protocol

51% attack, Double Spending, Selfish Mining, Eclipse Attack

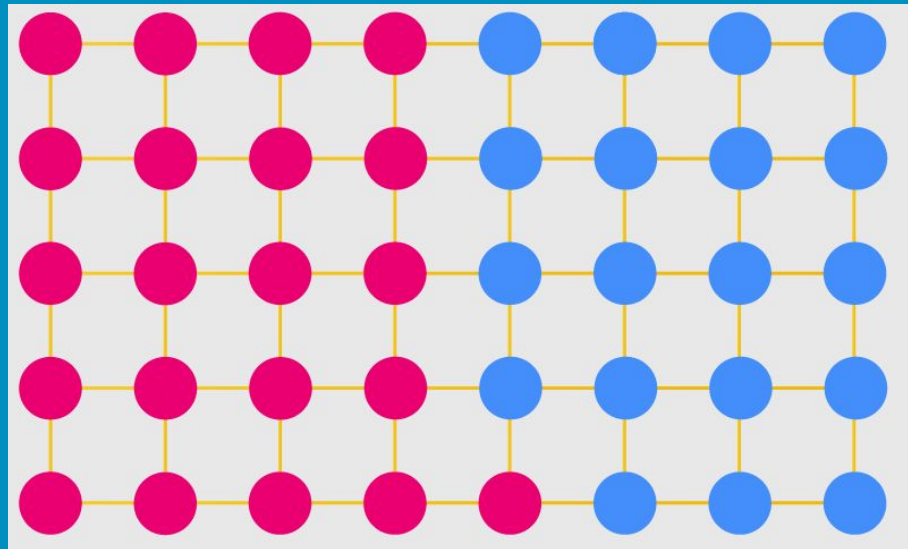
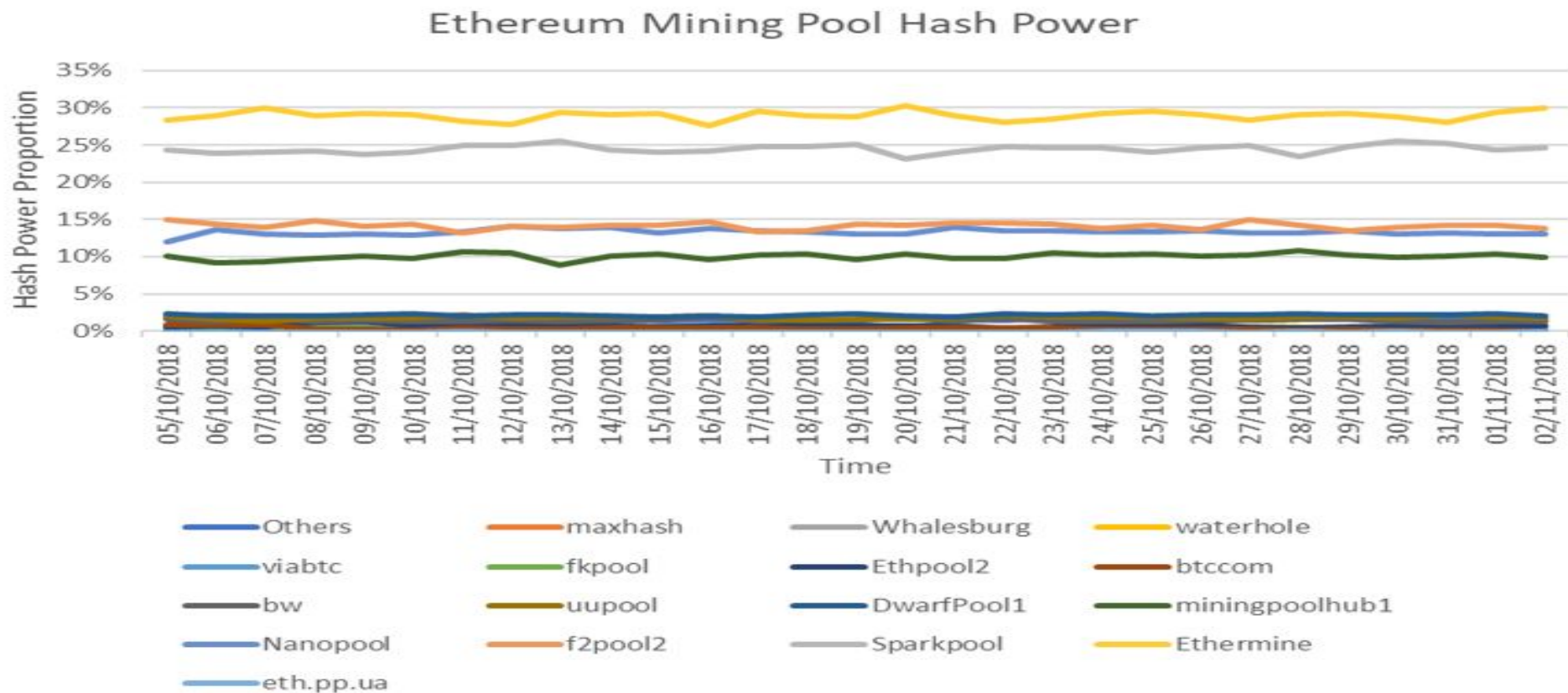


Image Source = <https://www.binance.vision/security/what-is-a-replay-attack>

Does anyone have 51% control over any significant blockchain?



Are major cryptocurrencies decentralised?

Debatable. The inequality in the power distribution in major cryptocurrencies may be a significant threat to the security.

Blockchain Interest Group is focused on establishing metrics that can be used to measure the centralization of decentralized blockchain and also the security impact of increasing centralization.

Privacy

Most cryptocurrencies are pseudo-anonymous.

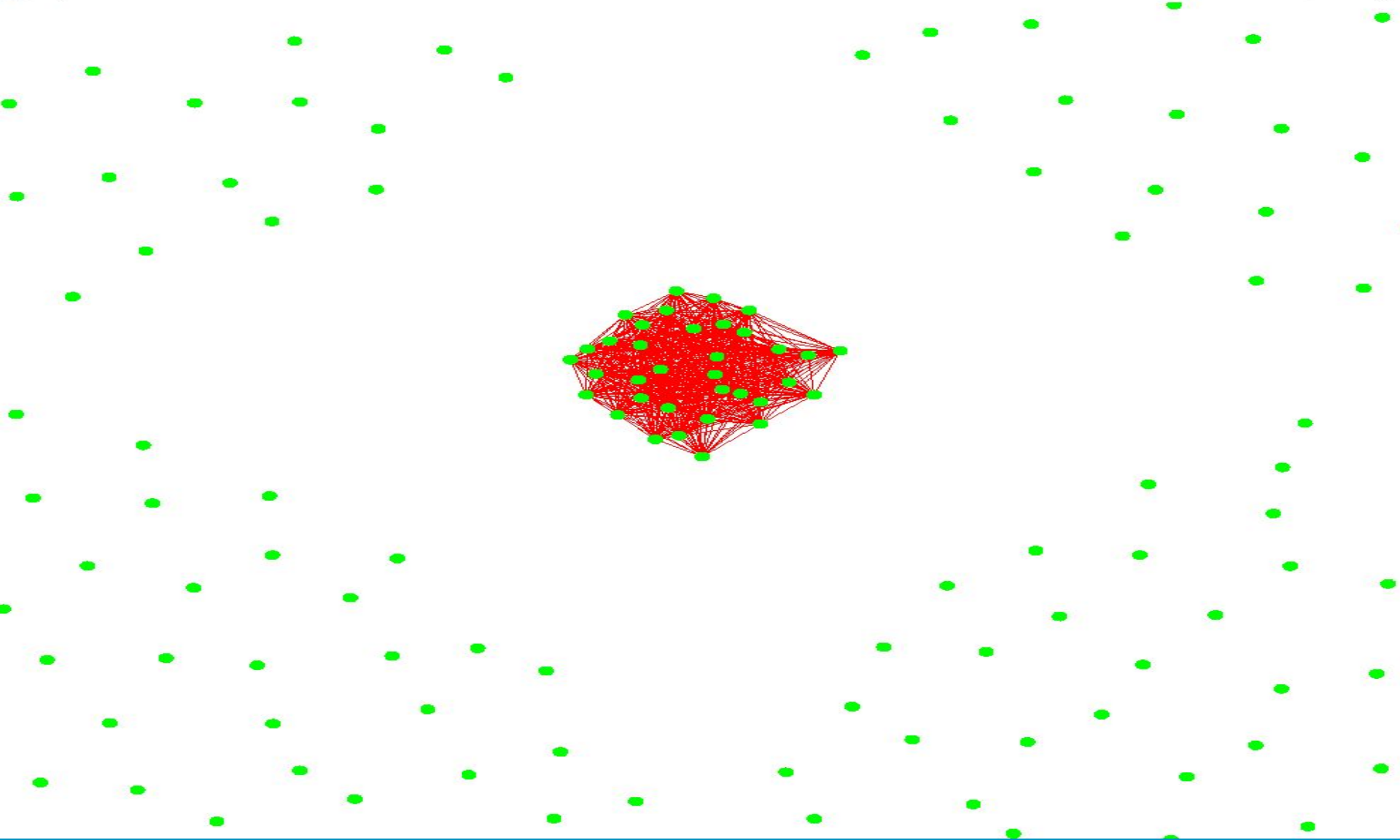
Anonymity is attractive for fraudulent activities. The first major use of Bitcoin was in the dark web as a payment method.

To read more about dark web and bitcoin visit = <https://www.thebalance.com/what-is-a-dark-market-391289>

Reverse Engineering the blockchain

Software reverse engineering is the generation of abstracted views of large software systems from detailed implementation artifacts.

Blockchain Interest Group has developed novel graphing techniques to detect coordinated behavior on Ethereum blockchain.



Toosi, Farshad; Buckley, J. S. A. R. L. G. A. (2018). Reverse engineering the blockchain as illustrated using eigen decomposition. European Conference on Information Systems (Workshop Paper), Portsmouth.

Blockchain Interest Group

If you want to work on Blockchain in your FYP or Master's thesis, please contact Dr. Jim Buckley or me.

