



## Leveraging Blockchain & Distributed Ledger Technologies for a Sustainable Economy and Society

Presentation to the UN-JRC Workshop on Sustainable Finance (Ispra, Italy)

Dr Ser-Huang Poon  
Professor, University of Manchester, UK  
Turing Fellow, Alan Turing Institute, UK  
Founder & Trustee, Enduring Net (<https://enduringnet.org/>)  
Email: [ser-huang.poon@manchester.ac.uk](mailto:ser-huang.poon@manchester.ac.uk), Tel: +44 7831 362 346

02 July 2019

0

## Ground Rules: Design Concept

1. No Jargon
2. Break Down Barriers to Entry – comprehensible by the layperson
3. How strong is the security?
  - Security in a wider sense, side effect (Bitcoin & money laundering)
4. Maintain transparency with the users
  - The “small print”; speed, maintenance, system upgrade
5. Design Thinking (how do we design a better society?)
  - Problem (not solution) focus
  - How to avoid useless blockchain

02 July 2019

1

## What is a blockchain?

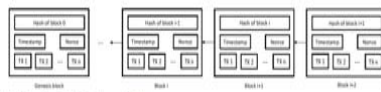


Fig. 1 Example of a blockchain (Zhang et al. 2016)

- It is a chain of “immutable” records by time order (organised by block)
- The records are submitted by users via the “Node” they are connected to.
- A blockchain must consist of at least two nodes; nodes are equal (power).
- The nodes will continuously synchronise the records they contain.
- After the synchronisation, the information (called the ledger) is the same on every node.

***A very effective form of sharing information between two or more parties***

02 July 2019

2

Satoshi Nakamoto’s (2008) Bitcoin Blockchain focused on “no double spending” and “proof of work” is a “disaster” in terms of:

- Energy wastage
- Money laundering
- Drug trafficking and other illegal activities

The biggest game changer is the DLT!

02 July 2019

3

## BAMF - Bundesamt für Migration und Flüchtlinge

- Supporting communication and cooperation in the asylum procedure with Blockchain technology
- A proof of concept by the Federal Office for Migration and Refugees
- Dublin Regulation: The content of any asylum application lodged in the Dublin region (EU, Norway, Iceland, Switzerland and Liechtenstein) is only checked by one state.
- The granting of asylum protection in one Dublin state makes any further review of the asylum application in another state impossible.
- [https://www.fit.fraunhofer.de/content/dam/fit/de/documents/BAMF\\_FhG\\_Whitepaper\\_en\\_final.pdf](https://www.fit.fraunhofer.de/content/dam/fit/de/documents/BAMF_FhG_Whitepaper_en_final.pdf)

VISION



02 July 2019

4

## Blockchain Distributed System

- Open, real-time **distributed ledgers** operated based on agreed principles.
- A trusted design and system without a trusted party: does NOT have a “owner” and **without a central administrator**
- All participants keep a replica of the ledger and updates through **consensus protocol**
- Transactions are **secured with cryptography**, making it difficult to falsify records
- Ledger is replicated on all nodes; **no single point of failure**

## Power of Trusted Decentralised Network

- The trust is established and maintained based on **consensus protocols**, and where appropriate, third-party **validators** (called **oracles** i.e. high priests).
- Validator can be **on-chain** based on a software (online price info), **tamper proof** hardware, **inbound** (e.g. buy if price drops below £1), **outbound** (transfer asset ownership upon payment), **consensus** (3 out of 5 oracles), or **off-chain** e.g. one or more human with designated authority.
- Trust is decentralized through the use of technologies that make it possible for geographically and politically disparate entities to reach consensus on the state of a shared database.
- **Public** (not private!) **permissioned** (towards **permission-less**) blockchain!

02 July 2019

6

Give the power back to the **Little** people!

*The most powerful and the only sustainable blockchain is one that belongs to the people with public support and social resources rather than on the endorsement of government or a centralised party.*

*Otherwise, use a centralised system e.g. Singapore.*

02 July 2019

7



<https://www.hull-coin.org/>

- HullCoin is the world's first Community Loyalty Point.
- Anyone can open a HullCoin Wallet and start using HullCoin.
- If you are an organisation doing great things in the community you can give people HullCoin.
- If you are a business, gain new customers, increase trade and show your commitment to Hull.
- You can gift HullCoin to family and friends or donate HullCoin to a charity in the city.



02 July 2019

8



energy web, Switzerland  
<https://www.energyweb.org/>

Blockchain technology applied in the energy sector has the potential to

- reduce transaction costs,
- enhance data security and transparency,
- open markets to a larger number of active participants (consumers and devices), and
- accelerate the transition towards a digitalized, decarbonized, decentralized, democratized and resilient energy system.

*Similar project is Oxfam's (2018) BlocRice for small-scale rice farmers in Cambodia.*

02 July 2019

9



- After the successful *Building Blocks* an ethereum-based system for cash transfers in Jordanian refugee camps – the UN WFP now plans to test blockchain for the tracking of food delivery in East Africa.
- To monitor the movement of food from Djibouti's port, where the WFP receives shipments, to Ethiopia, where much of its food operations are located.

02 July 2019

10

## Business Supply Chains

- Conflict mineral chains have 7-8 layers between the mine and the consumer.
- The gap can reach 50 layers for electronic components.
- In many cases, the "downstream" companies are often the last to know about illicit activities in their supply chains (such as conflict minerals, child and forced labour)
- Blockchains address these difficulties by making data public verifiable, resistant to alteration, instantly available on the ledgers.
- Digital tags (chip) leverage the interoperability of blockchain with IoT help to ensure the "single truth is not, in fact, a shared falsification.
- SAP Ariba's supply chain transparency and third party compliance certificates; put additional data in transactional map to create correlations that didn't exist before...

02 July 2019

11

## Blockchain Provenance

- Supply chains: Coco-Cola & sugarcane, De Beers/Everledger blood diamonds, Apple & cobalt mining
- Philanthropy and international aid: BitGive & Give Track, WFP Building Blocks, Alibaba/Alipay/Ant Love
- Remittances: Abra, BitPesa, Rebit lower transaction fees from 20% to 1-3, and time from a week to one day (instant/a few hours)
- Identity and land rights: ID2020, Project Amply, Bitland, Govt land registry (Dubai, Estonia, Georgia and Sweden), EU-DECODE's IoT data centric digital economy
- Democracy: Ballotchain, Democracy earth, Bitnation, Follow My Vote, E-vox (Ukraine elections)
- Climate & environment: global coral reef database, land management (usually need satellite) , Malawi tea farmers & land use

02 July 2019

12

## Blockchain Tech

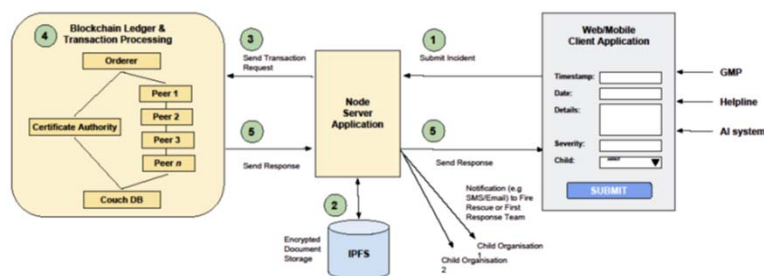


02 July 2019

13

## Permission Blockchain – IBM Hyperledger Fabric

Example Hyperledger Fabric Flow Diagram (Using Composer)



02 July 2019

14

## GDPR & Right to be forgotten

- Personally Identifiable Information (PII) and other private data is stored in a private state database (SideDB), which can only be accessed from authorised peers.
- A hash of that data is endorsed, ordered, and written to the ledgers of every peer node on the channel.
- The encrypted hash resides on the blockchain whilst the SideDB data can be removed to comply with GDPR.
- Data is grouped in organisation permissioned channels, which can be private or designed to interface with other channels.
- Each authorised peer in an individual network will maintain consensus on the SideDB and Blockchain.

02 July 2019

15

## Channels & Collections

- Channels are multiple blockchains in the same network. For each channel, only members of the channel can view the blockchain.
- Not every member of a channel needs to see the business logic or data for every transaction.
- A private data collection can be used to keep data confidential. Only the members authorized in the chaincode (smart contract) receive the data.
- Private data gets sent peer to peer between authorized organizations.
- Channels keep transactions private from the broader network whereas collections keep data private between subsets of organizations on the channel.

02 July 2019

16

## Security

- The key cryptographic element of Hyperledger Fabric is an enhanced version of Practical Byzantine Fault Tolerance (PBFT) known as Sieve.  
(<https://www.altoros.com/blog/how-hyperledger-fabric-delivers-security-to-enterprise-blockchain/>)
- Strong identity management and privacy features can be enhanced within organisations by using strict compliance framework around identity and screening techniques along with authorisation tools such as 2 factor authentication (2FA) and biometric systems (voice, finger print).
- We would expect Law Enforcement, Emergency Services, Charities dealing with vulnerable persons and NGO's to have these security SLA principles in place already so that interfacing with a blockchain system would be a natural step to improve already robust systems.

02 July 2019

17

## Other (Ir)relevant Risks



Might be a problem

- **Wallet Vulnerable To Theft**
- Tracing a coin's history
- Sybil attack
- Packet sniffing
- Denial of Service (DoS) attacks
- Forcing clock drift against a target node
- **Illegal content in the block chain**
- Security Vulnerabilities and bugs
- **Energy Consumption**

Probably not a problem

- Breaking the cryptography
- **Scalability**
- Segmentation
- Attacking all users
- Dropping transactions
- Attacker has a lot of computing power
- Spamming transactions
- The Finney attack
- Rival/malicious client code

See [Weaknesses page on en.bitcoin.it](https://en.bitcoin.it/wiki/Weaknesses)

## Some other important innovations to speed up decentralisation

- Concept of **zero knowledge proof**
- **Privacy** need due to GDPR, and human rights (channel, private data, sideDB, hashing)
- **Encryption** and encryption search algorithms, hash function
- Low volatility central bank and other **digital currencies** (to facilitate payments through blockchains)
- **Distributed PKI** (Public Key Infrastructure)
- **IPFS** (InterPlanetary File System) torrent with "Data Safe Heaven" features
- IoT - **Internet of Things** helps to create **tamperproof Oracles** (validators)
- **Mobile devices** and **social media** (WhatsApp, WeChat, AliPay...)
- **KYC** (know your customer) & **AML** (anti-money laundering) practices developed in the banking industry

02 July 2019

19

## Another important game changer

Central banks and private (facebook Libra?) *low volatility* digital currencies and the *regulations of blockchains*.

- A very important topic for Finance (and Monetary Economics) research and PhD work

02 July 2019

20

## CBDC (Central Bank Digital Currencies)

- David Andolfatto (2018), interest-bearing CBDC increases financial inclusion, diminishing the demand for physical cash. It reduces [banks] monopoly profit, will lead to expansion if banks respond by raising deposit rates.
- Domestic view, omitting the international and blockchain dimensions.
- No about speed; RTGS (Real Time Gross Settlement) is very fast.
- More about the unbanked (50% of adults, worse for developing countries, worst for women) and reducing transaction costs.
- Crypto has more problems than benefit (pegging, LTCM?, deposit insurance?) – interest payments on the chain?

02 July 2019

21

## Regulations of blockchains - challenges

- Boarder and jurisdiction is hard to define
- Initial coin offering: is this a stock issuance thereby regulated by company house? Is this a trade thereby subject to tax? What happen when there is fraud?
- What happen to the millions of missing bitcoins?
- What happen to dispute (e.g. on land right)?
- International money laundering would require international cooperation that does not exist.
- Data harvesting – facebook Libra?


02 July 2019

22



02 July 2019

23



Home About Executive Summary Forum Account

Our mission is to deploy distributed technology and artificial intelligence to facilitate humanitarian work.

02 July 2019 24

## UN SDG Objectives

- Empowering citizen rights (plus share action, consumer action etc.)
- Hold corporate and authority (police, gov agency) accountable
- Supply chain modern slavery audit and certification
- Commercial usage (proof of provenance, extendable to other applications e.g. pollution, carbon emission, plastic etc.)
- SRI goal, reduce search costs for asset managers and investors
- Auditor/assurer, means for monitoring the company and certify the ESG/MSA reports

02 July 2019

25



## Trusted Decentralised Network for Combating Modern Slavery

- There is a big ecosystem of modern-slavery case management systems and services across the world; big organisations develop or customise their own platforms while smaller organisations rely on service providers.
- Each of these systems has a stack of capabilities, storage/database, security, workflow, user interface, messaging, etc.
- Communication between organisation is fragile locally, non-existence globally.
- The proposed blockchain based trusted decentralised network will facilitate the different organisations to work together more effectively.

02 July 2019

26

## Blockchain Value Proposition Modern Slavery Multi-Agency Hub

- Agile, scalable & efficient especially when operated in heterogeneous organisations, geographically dispersed, with (political and policy) uncertainties.
- **Support the victims/beneficiaries** through the entire case journey as they pass through organisations, jurisdictions, countries – can further extend to encompass missing person management and ID2020.
- (4+1)P: Pursue, Prevent, Protect, Prepare, & Partnership



## ***PROBLEM STATEMENT***

02 July 2019

27



MC4

Appalling levels of slavery in India's brick kilns  
A new report and documentary reveals "appalling" levels of slavery in India's brick kiln industry, and points to the payment system keeping workers in the cycle of slavery.



Konstantinos Stathopoulos  
<K.stathopoulos@manchester.ac.uk>



02 July 2019

28

MC3

Feds: Polygamous group's kids used as unpaid workers on pecan farm



In this Jan. 21, 2015, file photo, brothers of polygamous sect leader Warren Jeffs, Lyle, foreground, and Nephi, leave the federal courthouse in Salt Lake City. Federal lawyers say the company violated a 2007 order involving underage labor and should be held in contempt for failing to pay 1,400 workers - including 175 children- who worked at the direction of church leaders who told parents to take days off from homeschooling during the 2012 harvest.

02 July 2019

29

## 5<sup>th</sup> February 2004



02 July

30

## Potential users and stakeholders

### Node access

- GMP & 11 Primary Divisions
- NCA
- Helpline
- NRM
- UK Border Agency
- UK Human Trafficking Centre
- UK Visas and Immigration

### UI/SMS/email/push notification

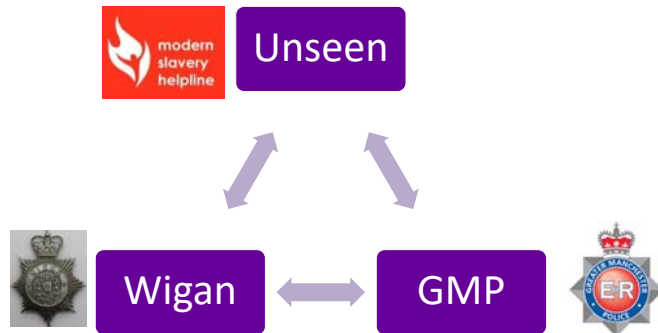
- Fire & Rescue
- GLAA
- HMRC
- Housing Officer / Standards
- Border Force / Immigration
- ICTA
- Local Auth / Victim Support Liaison Officer
- NGO / Charity / Stop-the-Traffik
- NHS / Maternity
- Social Services

02 July 2019

31



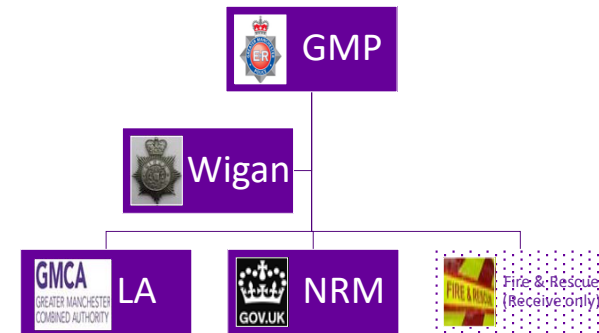
### Three Nodes MVP (Min Viable Product) Concept of “fail Fast”



02 July 2019

32

### Manchester Supported Network



02 July 2019

33

### Example 1: Vietnamese girls in Nail Bar

- A Vietnamese NGO tipped off UK National Helpline about 2 Vietnamese girls being smuggled into the UK by air ended up in nail bars in Wigan, Manchester.
- Outcome: The girls were rescued and followed up by LA, Victim Support Liaison Officer. Their cases were transferred to the National Referral Mechanism.

02 July 2019

34

### Outcome: Unseen, GMP and Wigan Have the same and all Information about the case in real time

Exploitation type	Labour - Health/Beauty			
Location (Encrypted)	WN			
Venue/ Business/ Activity	Nail Bar			
Risk Assessment	M			
Minor (Y/N)	Y			
Timestamp	Submitter	Ref No.	Recipient	Document link
20181101 13:45:23	MSHRC	M5043	GMP	Hash address of encrypted document referenced M5043
20181101 16:23:12	GMP	G067	Wigan	Hash address of encrypted document referenced G067
20181101 18:45:28	Wigan	W007	Local Fire & Rescue, Victim Support Officer	Hash address of encrypted document referenced W007
20181104 10:00:00	Wigan	W007	NRM (girl1)	
20181104 10:10:00	Wigan	W007	NRM (girl2)	

**Note:**

- Access to encrypted documents at hash address will depend on security clearance.
- Fire-Rescue and Local Authority will see only (all) the blue record.
- NRM will see only (all) the green records.
- Fire & Rescue will only receive (SMS/email) messages.

02 July 2019

35

## Example 2: Missing Child & CountyLine Crime

- A boy reported missing to GMP after not returning from school. The case was recorded at PNC (with name, DOB, address etc), and a PNC# was returned.
- The boy was found in public park in Cornwall. Devon and Cornwall (DCP) Police contact PNC and located PNC# for this child.
- AI (internal programme) notices the same PNC# and connect GMP & DCP. DCP might contact GMP given the address is in Manchester.
- Outcome: The boy was delivered to GMP by British Transport Police (BTP). GMP record the outcome and notify PNC.

02 July 2019

36

Exploitation type	Missing Child, Criminal - Drug distribution				
Location (Encrypted)	WN				
Venue/Bus/Activity	Public Park				
Risk Assessment	H				
Minor (Y/N)	Y				
Timestamp	Submitter	Ref No.	Recipient	Comments	Document link
20181101 13:45:23	GMP	G067	National Missing Contact Point (PNC)	Child not return from sch, report missing	Hash add of encryp doc G067
20181101 16:23:12	PNC	P749	GMP	Return of national PNC# (name, DOB, address)	Hash add of encryp doc P749
20181101 18:45:28	DCP	DC007	National Missing Contact Point (PNC)	Contact with Child in CountyLine drug gang	Hash add of encryp doc DC007
20181104 10:00:00	PNC	P821	Cornwall_PF	Return of national PNC# (name, DOB, address)	Hash add of encryp doc P821
20181104 10:10:00	AI Validator	AI991	GMP, Cornwall_PF	Connect GMP & Cornwall_PF (common PNC#)	Hash add of encryp doc AI991
20181102 08:15:22	DCP	DC007	GMP, BTP (British Transport Police)	Notify GMP & BTP returning child to Manchester	Hash add of encryp doc DC007
20181103 16:15:22	BTP	B0801	GMP	Record delivery of child to GMP	Hash add of encryp doc B0801
20181103 21:25:10	GMP	G067	National Missing Contact Point (PNC)	Record child return to family home	Hash add of encryp doc G067

### Note:

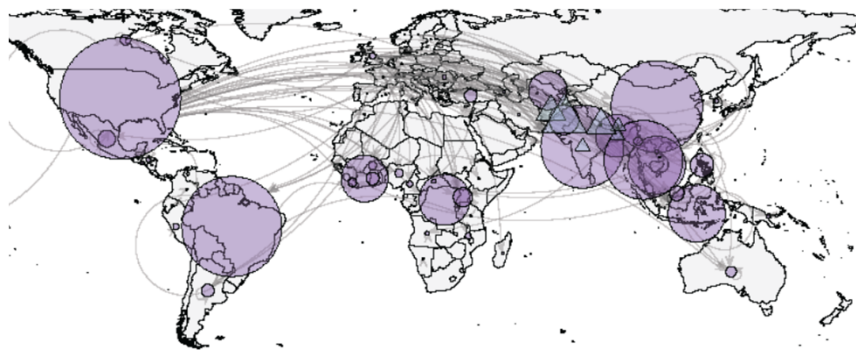
Here we assume DCP (Devon & Cornwall Police) is also a node.

The PNC (Police National Computer) and the BTP (British Transport Police) can enter record with restricted one-time login to GMP & DCP Node server.

02 July 2019

37

Child Labour RepRisk News Count (Circles) and National Survey Data (Triangles)



Sectors vulnerable to forced labour in India are "Food & Beverages", "Personal & Household Goods", and "Retail".

02 July 2019

38

## Artificial Intelligence and Machine Learning

- Pittsburgh Marinus Analytics's *Traffic Jam* analyses sex trade postings through text and image analysis, using one victim to find other victims, locations, traffickers' names and telephone numbers
- Demi Moore and Ashton Kutcher's *Thorn* ML highlight escort ads that may be fronts for trafficking; recognising underage kids is particularly challenging
- Albuquerque *DeliverFund* emphasise human review of Traffic-Jam's potential false negative
- U of Nottingham *SlaveryFromSpace* identified 20-50,000 kilns in Brick Belt joining Pakistan, Nepal, and India that are notorious in bonded forced labour

02 July 2019

39



## Demo

<http://35.177.18.77:8080/user>

For Unseen, Modern Slavery helpline (level-1)

User: Avinash

P/W: Avinash@1234

For Greater Manchester Police (level-2)

User: rushikesh

P/W: Avinash@1234

For level 3 user - No login required at the moment

<http://35.177.18.77:8080/api/getStatusByCrimeType>

In this implementation, Unseen was given more access right than GMP. So Unseen can see all the records while GMP can only see all the records it submitted and received. We have not yet implemented the user "Wigan" in this version.

If you submit new incidents, please wait for a while for the nodes to be synchronised bearing in mind that Unseen is level 1 and GMP is level 2.

02 July 2019

44



The blockchain revolution has started...  
We need EU partners!!!

02 July 2019

45