CST4025 Lecture Notes for Learning Week 1

Dr Ian Mitchell

September 30, 2019

Glossary

BC Blockchain. 1

CQC Care Quality Commision. 1

IoT Internet of Things. 1

JIT Just in Time. 1

P2P Peer-to-peer. 1

PoET Proof of Elapsed-Time. 1

PoW Proof of Work. 1

QAA Quality Assurance Agency. 1

RTW Return to Work. 1

Brief introduction to administration, delivery and assessment of module. Blockchain applications.

Definition: Blockchain is a generic term used to describe the entire technology. It is holistic, whereby the sum of the parts is greater than the whole. Dismantle a wrist watch and you will not be able to tell the time. There is the internation conference on blockchain, that studies consensus algorithms and all things related to blockchain. Whilst incorrect, blockchain is generally used to descibe all the technology put together to produce an append-only distributed ledger.

Uncertainty: The first block is referred to as the "Genisis block". The genesis block in bitcoin has a message. Bitcoin actually promotes uncertainty, in costs and value. So, how can it be used to reduce uncertainty? This is what the module is about.

Categorisation:

Centralised: Central Bank to govern all transactions. If A wants to do commerce with B then they both have to rely on a centralised bank.

Decentralised: Different to distributed. Decentralised includes governance.

Trust: Contracts. Escrow.

Permissionless: Permissionless BC uses P2P networks to support its architecture and disetribution of information related to transactions to be appended to decentralised immutable ledger. It uses PKI to ensure that the information is distributed accross the network. Membership to the ledger is public, in other words anyone can join. There is always an issue of trust between members, member could be malign and benign. The

biggest problem in cryptocurrency networks was the resolving the double spend problem. In cryptocurrency it is possible to spend the same amount in your wallet many times, and cryptocurrency networks needed solutions to this problem. Bitcoin proposed a decentralised network using PKI for privacy and a decentralised ledger for records, however, this did not resolve the double spend problem on it own. The use of consensus algorithms allowed the updated block to be completed if a significant percentage of the nodes agreed with a calculation. For bitcoin the consensus algorithm was PoW, which we will study in the seminar. Membership to the network was two tiered, you could either be a light user and just receive or spend coins, or own a node and be responsible as a bitcoin miner. The bitcoin miners are rewarded for being first to find a valid solution to the problem set out by the consensus algorithm. The reward varies and is currently at 6BTC, however, there is a limitation on how long this reward is available. Many researchers surmise that once BTC offers no reward it could be the demise of BTC. The nodes also receive a reward of a percentage of the transaction, so this encourages or makes more attractive to resolve bigger transactions. The consensus algorithms are resource intensive and require a lot of energy, there is also latency and throughput. For a single transaction it could take a day or more before it is loaded onto the blockchain as a permanent record, current time for a fast transaction is 15minutes.

Permissioned: Uses the same network architecture and technology as permissionless BC. The biggest difference is that the memberships is private, or authorised. You can only become a member of the network by invitation. [think membership, in permissionless there is no membership, in permissioned users are required to have membership... may need to redefine definition above for permissioned network]. This means that members of

the network are trusted. Usually, the nodes are centralised and operated by a single governing body in a decentralised manner? So, an organisation has control over a 1000 nodes that are responsible for updating the ledger. Members do not control nodes, which are responsible for updating the blocks. This changes the dynamics of the trust network, if you have a member they will be trusted, else revoke their membership. So, the consequence of trust means that consensus algorithms can be less CPU intensive and hence have an ecological impact (there are many claims that cryptocurrency are using up more energy than small countries to add a single block). There are many consensus algorithms, but the one with Hyperledger is PoET (Proof of Elapsed-time).

Attributable: Attribution, we can incriminate and proove that an individual is attributable for that crime. With a blockchain we can do the same, someone is responsible for there actions.

intermediary: In business there are many intermediaries that increase the cost. For docking a ship there maybe upto a 1000pages of documentation for each container, that has details on the goods, the insurance, the owner, the delivery, etc... Each area owned by a different intermediary, blockchain has the capacity to remove this.