The Chinese University of Hong Kong, Shenzhen

MDS 6117

Blockchain Technology and Development

Assignment 1

Author:
Li Jingyu

Student Number:
118010141

February 27, 2022

1 Question 1

Blockchain is a novel approach to the distributed database. Please articulate the differences between blockchain and traditional database. (30 points)

i Traditional database is centralized, and there is central authority controlling the system. Blockchain is distributed, the data spread across a network, there is no central authority to mediate disputes for public chain. The transaction relationship is peer-to-peer.

ii Traditional database usually has only one copy (some database may have 2 or 3 to ensure reliability). Blockchain has multiple duplication of the data, and its redundancy level is high.

iii In traditional database, data can be modified, deleted easily. In blockchain, write operation is irreversible and no modification on written information. Data can only be appended to the blockchain but cannot be edited or deleted.

iv Traditional database can organize the data in any logical order. Blockchain is organized as chain in chronological order. Each block contains a "hash" of the previous block. Transactions (data) on the blockchain are time stamped, making it useful for tracking and verifying information.

v In traditional database, the data is usually private and not disclosed to others. In blockchain, every transaction is completely public, and everyone can check data and their history.

vi Traditional database records the data manually without verification. Blockchain uses consensus mechanism to record data, and transactions must be verified and agreed upon as valid by majority of the network.

vii Traditional database uses account-password to secure. It is vulnerable to frauds and cyber crime.Blockchain uses dual-key encryption, cryptography and digital signatures to prove identity,authenticity and enforce read/write access rights, which can avoid malicious activities in the network.

2 Question 2

Some people argue that blockchain is slower than traditional transaction system. State your opinion about this argument in terms of correctness and reasons. (30 points)

Correctness: My opinion is **NO**.

Reasons:

i Traditional transaction system requires third-party's involvement or verification, costing lengthy settlement time. Blockchain transaction is point-to-point, without third-party and time-consuming verification procedure.

ii Traditional uses manual or electronic contract to ensure trust, which may take days to agree and sign. Blockchain uses smart contract, which is automatically executed and can process in minutes.

iii Traditional transaction requires manual remittance or escrow. Blockchain uses consensus process to enable payment exchanges and remittance without need of centralized clearing house automatically.

iv Traditional database costs great time to handle trick or accidents. Blockchain can check the authenticity easily and avoid errors caused by manual and accidents, no lawyer is required.

v Take an example: SWIFT takes 3 to 5 days to send money internationally. Ripple sends money in seconds / minutes. Ripple reduces settlement risks, eliminates intermediaries, midpoint failure, delays. It provides instant, bilateral and straight through processing.

3 Question 3

What industries and applications (aside from cryptocurrency) do you think that blockchain has the potent to make a major impact. (a) Please give an example of how blockchain can potentially change or transform the industry and the specific application. For example, the financial industry (industry) and cryptocurrency (application) (b) Please state the advantages and limitations of blockchain technology in the proposed industry and application. (40 points)

(a) **Industry**: Supply chain and manufacturing industry (like food/machine production), trade finance.

Application: Ant chain in Alibaba. Product provenance and lifetime history and real-time tracing. Facilitates chain of custody process for products in the supply chain where the party in custody is able to log evidence about the product.

(b) **Advantages**: Real-time checking; Easy to trace the origin and find responsibility holder; Consistent; Efficient; Transparency, information can flow through each party easily; Trust-worthy, no modification on data; Security; Resilient.

Limitations: Cannot avoid data origin forge or make sure the offline items/transactions are real; Relatively slow processing, not suited for high-performance transactions (in milliseconds); Not a solution for one participant, only make sense in business network; Not suited for low-value, high volume transactions; Not a messaging solution.