Assignment

- Contract data

→ Introduced in the year 1995

→ Cryptographer Szabo first proposed the concept of Smart contract.

→ He pointed out that Smart contracts stimulates contract execution by using protocols and user interfaces.

Smart Contract

→ Commercial contract, self-executing contracts containing the terms and conditions of an agreement among peers.

→ Terms and Conditions of the agreement are written into code.

→ Written in a programming language that automatically enforces the terms of contract when predetermined conditions are met, thus achieving goal of "code is the law"

→ life cycle includes three stages

* Contract generation
* Contract publication

* contract execution

Structure

Each block contains the following information

→ Roots hash of the current block

→ Root hash of the previous block

→ time stamp

→ contract data

→ other descriptive information.

Problems to be solved in blockchain data analysis

Based on relevant literature analysis, the focus of the block chain data analysis can be summarized into 7 aspts:-

1) Entity Identification

→ In Bit coin transactions, users are anonymous.

→ Transactions involves multiple users, and one user may participate in multiple transactions at the same time.

→ As it is not possible to confirm that a user is identified, it is generally considered in the literature that an entity is identified, entity may be user or an organization.

2) privacy protection

→ Blockchain privacy protection can be divided into

* Identity privacy protection
* transaction privacy protection

→ Identity privacy protection requires that user's identity information physical address, IP address are not related to user's public key, address and other public information on the blockchain.

→ Transaction privacy protection requires that data information of transaction itself be anonymous to authorized node.

3) Network portrait

→ In the face of massive transaction data researches hope to analyze how many users involved in transaction, characteristics of there users etc.

→ From point of view of complex network, the characteristics of Bitcoin network are analysed.

4) Network Visualization.

→ with prevalence of blockchain technology, the transaction data stored in the blockchain

increases rapidly

→ Therefore, in the face of a large and rapidly growing trading network, it is an important research direction to study its visualization tools.

5) Market effect Analysis

→ prices of encrypted currencies such as Bitcoin are highly volatile.

→ perspective of finance, its extremely high volatility has attracted economists to discuss whether bitcoin is currency or not.

6) Illegal behaviour detection

Unlike traditional bank payment system, Bitcoin is an anonymous, non-centralized payment system.

7) Transaction pattern recognition

Valuable Question that whether specific patterns can be identified from blockchain transaction records to detect related illicit activity.