Article from

Actuary of the Future

November 2018
Issue 43

A Short Introduction to Blockchain Technology

By Xiaochuan (Mark) Li

Bitcoin got everyone's attention in 2017 when its price rose to $20,000 from $800. (The price dropped to around $6,500 recently.) During the height of Bitcoin fever, other cryptocurrencies were invented, most of which are associated with different initial coin offerings (ICOs) to fund projects claiming to apply the backend technology to various business areas.

Supporters claimed that Bitcoin could change the financial system fundamentally, while many other people suspect its legitimacy is due to the speculation in cryptocurrencies and huge price fluctuations. Whether cryptocurrencies will replace traditional currencies is still to be decided; the backend technology, blockchain, will definitely have wider applications. We actuaries need to be aware of this new technology; the goal here is to describe the basic characteristics of blockchain.

PROBLEM WITH CURRENT PEER-TO-PEER SYSTEMS

The core problem in a peer-to-peer system is that there is an unknown number of peers with unknown reliability and trustworthiness. When one person sends property to another on the internet, it is hard to confirm that the property right is correctly transferred without third-party verification.

Blockchain is a purely peer-to-peer system. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. Its main characteristics include decentralization, pseudonymity and immutability. It is claimed to solve the problems of the current peer-to-peer system.

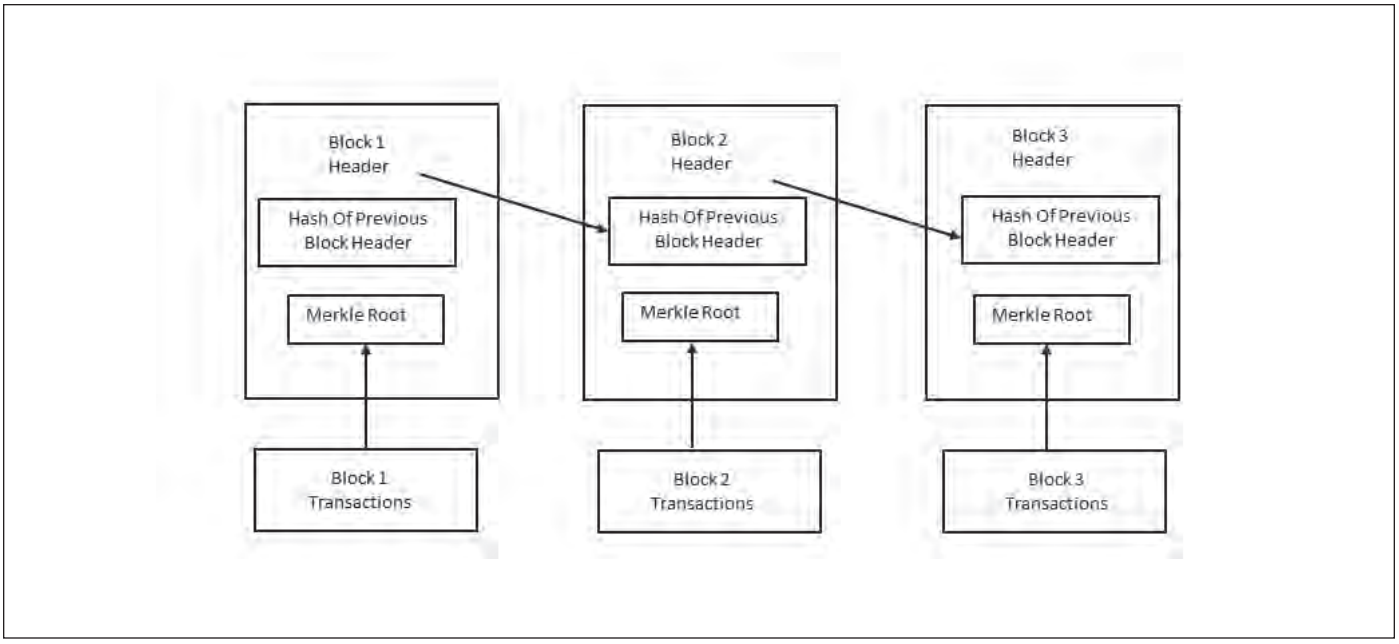
BLOCKCHAIN DATA STRUCTURE

The blockchain data structure is made up of ordered units called "blocks." Each block of the blockchain data structure consists of a block header and a tree structure that contains transaction data. Each block header references the header of the preceding block, preserving the order of the block headers and blocks, respectively, that make up the blockchain data structure (see Figure 1).

IMMUTABILITY OF STRUCTURE

Blockchain uses hash functions to create digital fingerprints for the references and contents. Hash functions are small computer programs that transform any kind of data into a number of fixed lengths, regardless of the size of the input data. If two hash values

Figure 1
Simplified Blockchain Data Structure



are identical, their corresponding input data are also identical. Hash values are useful for making basic file operations such as comparing, referring and storing data securely and efficiently.

The data structure of blockchain is change-sensitive. Rewriting a block needs to start from the head of the whole chain. Each block from the head presents a puzzle to solve, each of which requires massive computation. One example is a Hash puzzle that takes on average about 100 billion billion (1e-20) attempts to find. And there is no short cut. Therefore, it becomes impractical to change the existing blocks.

On the other hand, adding a new block to the blockchain data structure is less computationally expensive because it only requires adding the hash reference that points the current head of the chain to the new block header, declaring it the new head of the chain.

WHO CAN ADD NEW TRANSACTIONS?

Blockchain is an open system, allowing everyone to add new data to the history of transaction data while preserving its integrity. Hash functions are also used to allow computers to challenge other computers in deciding who can add new blocks to the chain. The computer that solves the puzzle first gets the right to add new blocks.

Blockchain uses a carrot-and-stick strategy. All nodes of the system are allowed to add blocks and also act as supervisors of their peers. Blockchain will reward nodes for adding valid and authorized transactions and for finding errors in the work of others; it will punish nodes for adding invalid or useless blocks. All nodes of the system have an incentive to process transactions correctly and to supervise and point out any mistake made by peers. The incentives can be in the form of cryptocurrencies, like bitcoin. Nodes-added new valid blocks get rewarded and penalized by adding invalid ones, while nodes in these situations will be rewarded.

The blockchain algorithm holds a continuous competition for rewards based on two criteria: speed and quality. Only the node that wins both competitions receives the reward for submitting a new block. The trick of the competition is that the losers of the speed competition are the referees in the quality competition, and they validate the block that the winner of the speed competition submits. This ensures a strict examination of the submitted block.

Each node will add new transaction data as a new block once informed of the data. Due to delays or errors in passing messages, at a certain point in time, all nodes may not hold an identical understanding of the transaction history. When nodes try to add new blocks, they may have different opinions regarding which is the previous block. The blockchain algorithm uses collective decision-making to solve this problem. They follow two criteria: either the longest-chain criterion or the heaviest-chain criterion to reach an agreement. These two criteria represent the chain that comprises either the largest number of blocks or blocks with the most difficulty levels; in essence, chains with the most aggregated computational effort.

APPLICATION IN INSURANCE

Blockchain uses the mechanisms specified previously to become a purely peer-to-peer system that is secure, resilient and consistent. It is mainly used as a public ledger to clarify and transfer ownership. The most notable application so far is in cryptocurrency. But there are many possible applications in different areas, including the insurance industry.

The potential of blockchain technology in insurance may include sharing data, processing claims and preventing fraud. The level of underinsurance due to lack of trust, high costs and inefficiency may be reduced to some extent by this technology.

One area to reduce inefficiency is in data management. Personal data can be controlled by individuals themselves and verified on the blockchain. One company, Tradle, is trying to develop blockchain solutions for know-your-customer (KYC) data. Clients' personal information can be more securely and easily retrieved and verified by institutions and regulators.

Privately held insurance adviser American Association of Insurance Services (AAIS) has also introduced its blockchain-based insurance database and reporting tool to enable the efficient and permission-based collection of statistical data on behalf of insurance carriers, regulators and other participating contributors.

One way to improve claim processing is through a smart contract issued on blockchain between the insured and the insurer. The contracts can be recorded and verified; only valid claims are paid and multiple claims on the same accident will not be paid. Payment can be a trigger on blockchain without human intervention. The whole process will be more transparent and customer-centric.

To prove policies and verify claims requires extensive cooperation to share information between insurers, manufacturers, customers and other parties. The Blockchain Insurance Industry Initiative (B3i) was launched in October 2016 to explore the potential use of distributed ledger technology. It currently includes dozens of direct insurer, reinsurer and brokers around the globe. ■

Xiaochuan (Mark) Li, ASA, is a data scientist at RGA Reinsurance Company, in Chesterfield, Missouri. He can be reached at *xli@rgare.com.*