Article from
CompAct
October 2019
Issue 63

Blockchain—Is the Newest Kid on the Block Going to Be All Right?

By Helen Duzhou and Jeff Guo

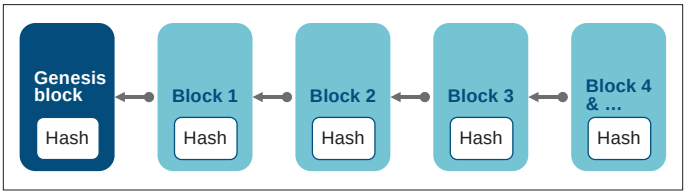
In the world of digital excitement, Blockchain is the newest kid on the technology block. Pull up any search engine, punch in "Blockchain" and find yourself inundated with articles praising improvements over current centralized network systems that many insurers use. But is this praise warranted, and does Blockchain truly cure all ails? In this article, we pose commonly asked questions as well as provide answers from the perspective of an insurance company.

MECHANICS OF BLOCKCHAIN

Definition: Blockchain is a **decentralized** and **distributed** database (also known as a ledger) from which accurate and secure information from any point in the past can be efficiently retrieved. A Blockchain is a connection of a set of blocks in historical order, and each block is a collection of data in a predefined structure.

> "Decentralized" and "distributed" are not the same! In distributed databases the data is spread out over many computers, also known as nodes. For a decentralized database the ability to edit is not centralized and each node can edit the database directly.

Figure 1
Simplified Visualization of Blockchain



Each block contains a cryptographic hash which serves two primary functions: (1) summary of data contained in the block, and (2) marker for the block's location within the chain.

Figure 1 provides a simplified visualization of a Blockchain. The Blockchain begins with a single block called the **genesis block**, which defines the Blockchain's initial parameters. Data (such as transactions or records) are validated by the network through a cryptographic hash algorithm before combined in a block.[1] The subsequent blocks are appended to the previous block, which can be traced all the way back to the genesis block.

Consider the following example Blockchain:

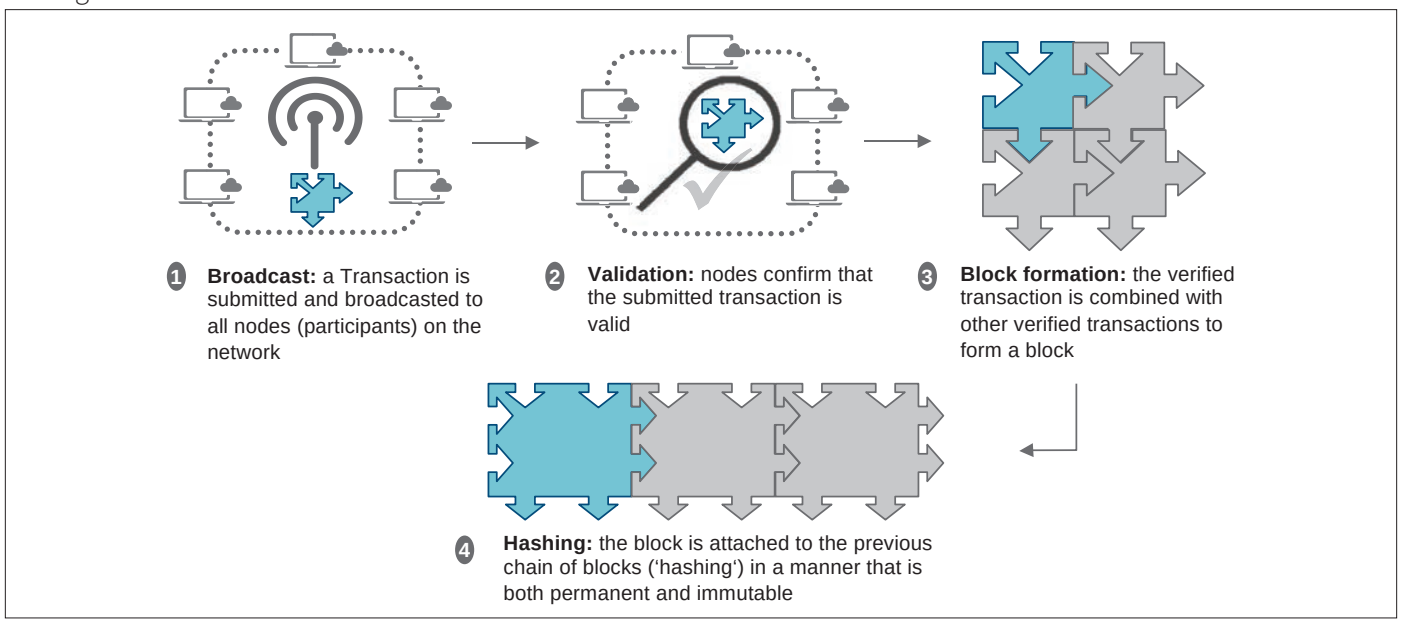
> Beatrice and Anthony live together and split expenses evenly (the "genesis block" that defines the parameters). In January Beatrice and Anthony combine their receipts, check correctness, and create a summary of the transactions. All monthly transactions (for January) would be one block ("block 1").
>
> Thereafter, the February block ("block 2") would be appended to the January block, the March block ("block 3") would be appended to the February block, and so forth.
>
> To figure out how much Beatrice or Anthony have spent, they would be able to review back to January and add up all of their receipts, similar to how information can be retrieved from and added to a Blockchain.

Adding a block is more complicated than two roommates reviewing their monthly receipts together. Figure 2 represents how a new block is verified by the network before being added to the chain.

Cryptographic Hash Algorithm and Mining

Integrity, validity and anonymity associated with a Blockchain are centered around a "magical" **cryptographic hash**

Figure 2
Adding a New Block to the Blockchain



algorithm. The algorithm combines a set of inputs (the hash of the previous block; the hash of the transactions of the current block; and a **nonce** (a **n**umber used **once**) to create a **hash**, which is a unique string of fixed length.

Through the cryptographic hash, the following key properties are realized in a Blockchain:

1. **Immutability.** Transactions cannot be altered since each transaction contains a digital fingerprint (the "hash") that summarizes all prior transactions, preventing manipulation.

2. **Anonymity.** Each participant has a codename, allowing concealment of identity and only the owner can approve transactions.

3. **Integrity.** The hash ensures that the blocks are in proper order and that related information can be reconciled to the block.

A Blockchain is susceptible to a **collision issue** where modern-day computers can create thousands of potential blocks that could be appended to the Blockchain at the same time. To address the collision issue, the participants undergo a **mining** process to ensure only verified blocks are added to the Blockchain at a preset time interval.

During mining, a node intending to update the Blockchain will repeatedly guess a nonce until, by luck, the produced hash meets a network-defined criterion. Benefits of mining include deterring network attacks and distributing the chance of updating the Blockchain across the network based on computation power.

Mining ensures the veracity of the Blockchain. If the majority of the participants are honest and only append to the correct blocks, then an incorrect block will be discarded by the network, and fewer people will append blocks to it because there is greater computational power in the network, and so a greater probability of the network recognizing the right block.

Together, the properties of mining create a **memory of the network** that prevents fraudulent or erroneous transactions.

During mining, a node intending to update the Blockchain will repeatedly guess a nonce until, by luck, the produced hash meets a network-defined criterion.

APPLICATIONS IN INSURANCE

The immutable, synchronous nature and integrity of the Blockchain allow for applications in optimizing loss management, streamlining existing systems, and penetrating new markets.

Several startups and initiatives are taking advantage of these opportunities, noted in Figure 3.

Figure 3
Use Cases

Example	Description	Use Case
Crowd funded industry initiative	Insurance companies merge their efforts in leveraging Blockchain to optimize processes, realize cost savings, and offer network users a variety of integrated applications.	***B3i*** was founded by 16 market participants in 2017 and is now an initiative of 40+ company participants
Fraud detection	Improper transactions are detected by validating the "fingerprint" of encrypted and immutable Blockchain transactions.	***Blockverify*** reduces fraud by tracking product's Blockchain tags along a supply chain ***Everledger*** (e.g., *Diamond time-lapse)* verifies asset authenticity through Blockchain fingerprint
Smart contracts[2]	Smart contracts are written as code in the Blockchain, which self-execute once a triggering event is met, without the need for third-party intervention.	***Etherisc*** provides real-time insurance quotes based on flight delays[3] ***Edgelogic*** uses sensors to detect an event that triggers payment for repairs[4]
Real-time insurance quotes	Blockchain can self-regulate the appropriate insurance premium continuously, which allows for development of tailored products addressing each customer's unique concerns.	***Safeshare Insurance*** facilitates short term commercial insurance contracts

POTENTIAL COMPLICATIONS

Although many insurers are interested in Blockchain technology, few have embraced it as a business proposition. According to one observer, "insurers do not necessarily need a current Blockchain strategy to remain competitive."[5]

Potential complications for a Blockchain implementation for an insurer are as follows:

1. It is unclear how Blockchain will adapt to new regulation, since its structure is immutable. Since Blockchain does not allow tampering with existing blocks, removal of certain data is hindered, which limits compliance with regulation such as General Data Protection Regulation.

2. Future technology such as quantum computing[6] can overpower Blockchain mechanisms, can be used to disrupt hashing as the validation mechanism and can expose private data to the public.

3. Blockchain is entirely dependent on the core source code, which can leave the entire ledger at risk if it is hackable.

4. Since the Blockchain is dependent on the memory of the network, collusion can occur if a party with majority of the computation power commits fraud.

In addition to the points already mentioned, other costs and considerations when implementing Blockchain include:

- First movers who invest in Blockchain will incur considerable up-front costs, due to lack of existing technical standards and expertise.

- Blockchain (currently) is not capable of scaling to handle large amounts of transactions.

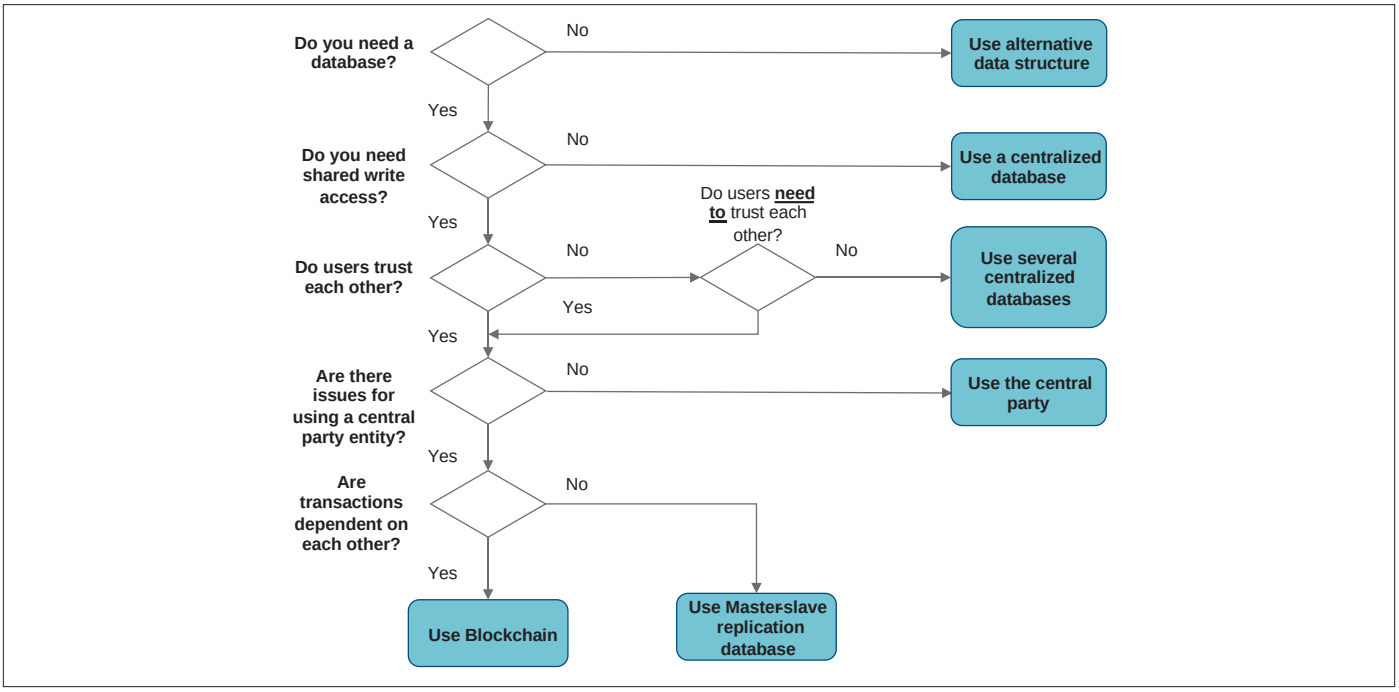
- The process of mining is data-intensive and has high storage requirements relative to central databases that are currently used.

WHEN BLOCKCHAIN MAY BE NECESSARY

The main advantage of Blockchain is that it solves trust issues between firms and individuals. A common situation for which Blockchain would be very useful is if multiple parties are involved and their interests are not aligned. However, most of an insurer's data needs can be addressed with existing technology. For more information, the flowchart in Figure 4 illustrates when it is appropriate to use Blockchain.

While Blockchain is not necessary today, it could become a business requirement in the future. Recent allegations around data breaches and privacy invasion are troubling, as insurers who hold sensitive policyholder information find themselves increasingly at risk of an attack. As Stephen Mildenhall pointed out, the internet has created a **trust vacuum**, which highlights the requirement for verification.[7] The trust vacuum will become increasingly apparent as the world grows more interconnected. With Blockchain's anonymous nature, data can only be approved by the owner.

Figure 4
Do you Even Need a Blockchain?



Source: B. Suichies, revised by Oliver Wyman

CONCLUSION

Although Blockchain offers significant advantages such as improved level of data integrity, anonymity of users, and inability for tampering (immutability), the insurance industry has been slow to adopt the technology. The heavy initial investment and expertise required can be prohibitive to entry by smaller insurers. Even now, most start-ups utilizing Blockchain are in their infancy, with heavy emphasis toward R&D. The general approach is to wait for a more applicable use case to be developed, or to participate in a crowd-funded industry initiative such as B3i.

Even with successful implementation, operational costs and regulatory and technology risks are higher than for traditional databases, with limited potential remediation methods. Insurers may be better off investing in a well-managed relational database.

Like all new kids on the block, Blockchain will develop and resolve many of its initial issues by becoming more scalable and efficient. And with its crucial data privacy benefit, as policyholders seek more control over the use of their data, Blockchain may become necessary in the future as it helps resolve the trust issue between insurer and policyholders.

Growing up is tough, but Blockchain might just be all right. ■

The views expressed are the authors' own and may not represent the views of Oliver Wyman.

Helen Duzhou, FSA, CERA, is a senior consultant at the Financial Services Practice of Oliver Wyman. She can be reached at *helen.duzhou@oliverwyman.com*.

Jeff Guo is a consultant at the Actuarial Practice of Oliver Wyman. He can be reached at *jeff.guo@oliverwyman.com*.

ENDNOTES

1 *https://blockgeeks.com/what-is-hashing-digital-signature-in-the-Blockchain/*
2 *https://blockgeeks.com/guides/smart-contracts/*
3 *https://www.ccn.com/Blockchain-disrupt-air-travel-insurance-flightdelay/*
4 *https://phys.org/news/2015-12-Blockchain-bitcoin.html*
5 *http://novarica.com/Bitcoin-and-insurance-overview-and-key-issues/*
6 *https://medium.com/the-quantum-resistant-ledger/no-ibms-quantum-computer-won-t-break-bitcoin-but-we-should-be-prepared-for-one-that-can-cc3e178ebff0*
7 *http://www.aon.com/reinsurance/gimo/20180711-gimo-Blockchain*