MARCH 2017

FINANCIAL SERVICES

The promise of blockchain

Blockchain has huge potential to enhance insurers' business model, but is also being used by digital start-ups to attack it. Hence the imperative for incumbents to start exploring this nascent technology.

Many have likened the revolutionary possibilities of blockchain technology to those of the internet, such is its perceived capacity to transform the ways in which people and businesses cooperate.

Investors put more than $800 million into blockchain-related start-ups between 2014 and 2015.

Sensing this, investors put more than $800 million into blockchain-related start-ups between 2014 and 2015. Perhaps even more indicative of its disruptive potential, in late 2016 four European insurance giants, Aegon, Allianz, Munich Re, and Swiss Re, set up a combined pilot project known as B3i to explore the nascent technology.[1]

The insurance industry in general, however, lags behind other industries, such as banking, in terms of the interest it has so far expressed. It will have to catch up, because as well as demonstrating potential to enhance insurers' current business model,

blockchain is being used by digital start-ups to attack it.

Blockchain is a shared, public ledger of records or transactions that is open to inspection by every participant but not subject to any form of central control. The *Economist* newspaper has described it as a machine for building trust.[2] In the case of the virtual currency bitcoin, arguably its most famous application, it tracks transactions and facilitates money transfer, while preventing double-spending, without the need for a bank. But blockchain lends itself to many other systems for keeping static records (of land titles, for example), for registering dynamically the exchange of assets, and for making payments such as ticket purchases. It is also a platform for "smart contracts"—computer programs that automatically initiate certain actions when predefined conditions are met.

How it works

While blockchain technology can be used in different ways, a blockchain solution generally builds on four features.

Decentralized validation. When a transaction such as a ticket sale occurs, new data blocks describing it are added to a chain only after consensus is reached among the relevant participants on the validity of the action—for example, when

1 See also *Beyond the hype: Blockchains in capital markets,* December 2015, McKinsey.com.

2 "The promise of the blockchain: The trust machine," *Economist*, October 31, 2015, economist.com.

the seller is validated as the owner of a ticket that is sold.

Redundancy. The blockchain is continuously replicated on all or at least a group of nodes in a network. As a result, no single point of failure exists.

Immutable storage. Blockchain confounds hackers because to

In a digital world, winning companies meet exacting consumer needs—for tailored products, simplicity, and transparency, for example.

tamper with data they would have to alter not just one block in a chain but also all successive blocks and the majority of their replications. In addition, data is registered in the blockchain with a digital fingerprint that includes a date and time stamp; any attempt to change data would be apparent because the new digital fingerprint would not match the old one.

Encryption. Digital signatures based on pairs of cryptographic private and public keys enable network participants to authenticate which participant owns an

asset, initiated a transaction, signed a smart contract, or registered data in the blockchain.

Opportunities for insurers

With these characteristics, blockchain can help address some of the key challenges that many incumbent insurers face in a digital age, including the need to understand and meet customer needs more fully and to cut costs by making operations more efficient. There follow some examples of the way blockchain might be applied.

Meeting customer needs

In a digital world, winning companies meet exacting consumer needs—for tailored products, simplicity, and transparency, for example. Insurers traditionally have had little opportunity to understand such needs, interaction with customers being limited to buying a policy or making a claim, processes that might anyway be delegated to brokers and agents. This explains both the threat and often the success of digital attackers that make customer satisfaction their priority.

Blockchain can help insurers in this both by sparing clients the frustration of repeatedly having to provide data for verification purposes—a copy of a passport, for example—and by reducing privacy concerns. No longer will it be possible to pass that data on to a third party without the client's permission.

For instance, UK start-up Tradle is working on a blockchain solution that

will enable financial institutions to conduct the know-your-customer (KYC) checks required by regulators to prevent money laundering—a process that is otherwise expensive and time-consuming for institutions and annoying for clients if they have to offer up the same information about their identity and source of wealth to different institutions. Once KYC data is verified, the customer can use a private key to grant companies in the network access to the encrypted data whenever it is needed.

In addition, blockchain provides greater transparency and hence perceived fairness in respect of tariffs and claims

An estimated 5 to 10 percent of all insurance claims are fraudulent.

handling. Another UK start-up, InsurETH, is working on a peer-to-peer flight insurance policy built on blockchain with smart contracts. The contracts initiate payouts to the holders of insured tickets when cancellations or delays are reported from verified flight data sources, making the claims and payments process quick and easy. (Although many travelers could claim compensation for flight delays under their usual insurance, few do so as the

process of verifying the delay can be a lot of effort for relatively little reward.)

Similarly, smart contracts could trigger the claims and payments processes for damage caused in the home or to a car and detected and verified by sensors linked to the Internet of Things, doing away with quibbling about the causes of damage and phone calls to chase the progress of a claim.

Fraud prevention

An estimated 5 to 10 percent of all insurance claims are fraudulent, costing US non-health insurers more than $40 billion a year according to the FBI. By serving as a cross-industry, distributed registry of external and customer data, blockchain can be used to identify fraud.

It can, for example, expose falsified damage or theft reports by validating the authenticity, ownership, and provenance of goods, authenticating documents such as medical reports, checking police theft reports and claims histories, and verifying identities.

It is clear that extensive cooperation between insurers, manufacturers, customers, and other parties will be needed to unlock blockchain's full potential. Blockverify, a UK start-up, is building a system that will enable users to check for fraudulent transactions, counterfeiting, or theft relating to goods such as personal electronics, pharmaceuticals, and luxury items. It works by labeling products and then storing their history and supply chain

activity in a blockchain. Everledger, also based in the United Kingdom, has devised a similar application, used to verify diamonds and transactions relating to them, and targeted at helping insurers, law enforcers, and those in the diamond trade to detect fraud.

Efficiency

Underlying many of these use cases is another clear opportunity for insurers—to reduce operational and administrative costs. Automated verification of policyholders' identity and contract validity, the auditable registration of claims and data from third parties such as doctors, the underwriting of smart contracts, and the automation of claims procedures all reduce costs while speeding up processes.

The lower handling costs of a smart contract could feasibly help open up new growth markets. In emerging markets, blockchain and smart contracts could be used to offer microinsurance to farmers, for example, triggering payments to them when drought conditions are verified by a reliable meteorological source. And insurers could potentially save the many millions currently spent chasing down fraud.

The way ahead

Blockchain clearly facilitates innovative business models and promises cost advantages to insurance companies and their customers. Various barriers impede its widespread adoption, however.

Scalability is the first challenge. The technology's consensus-based validation mechanism, its continuous replication, and the ever-growing amount of stored data means that the larger the blockchain grows, the greater become the requirements for storage, bandwidth, and computational power. That leads to a risk of centralization if the blockchain becomes so large that only a few nodes are able to process a block.

The lower handling costs of a smart contract could feasibly help open up new growth markets.

Second, recent incidents have shown that for all blockchain's security attributes, it is not impregnable. For example, hackers stole $65 million from Bitfinex, a cryptocurrency exchange. Such threats are not as well understood as those related to conventional database architectures.

Standardization is a third challenge. To realize sustainable benefits from an open or partially shared and distributed system, some standardization will be necessary. The current absence of industry standards—which the B3i project is seeking to address—reflects the newness of the technology. A distributed system that sometimes depends on collaboration between competitors, suppliers, and others will take time to evolve. So will the resolution of legal and regulatory issues. Thus there is a high risk of initiating

inefficient solutions, and investment decisions will need to be taken carefully.

But the obstacles should not deter insurers given that new companies are rapidly embracing the technology and its cost advantages. At their core, insurance companies collect premiums, pool the money, and reassign it to those with a valid claim. Blockchain means all this can now be automated and today's insurers potentially disintermediated—by the likes of InsurETH, for example, or Dynamis, a start-up that is using smart contracts to offer peer-to-peer supplementary unemployment insurance. In the latter case, it is other policyholders on the network who validate both the application for insurance and the claim, using social media.

These examples pose no immediate great threat to incumbents' business. But they should alert incumbents to blockchain's disruptive potential, and to the need for them to help shape the blockchain insurance ecosystem. The starting point is to develop a thorough understanding of how the technology can address customers' needs as well as their own, and to identify potential applications. That will mean working with consortia, technology experts and start-ups, regulators, and other market participants to address the challenges. Incumbents can learn from the start-ups and might consider partnering with or acquiring companies that are entering the insurance market with blockchain-based products and processes.

For the time being, it is important to bear in mind what blockchain can and cannot facilitate. If a limited number of parties are involved in a transaction then insurers' current transaction models are likely to suffice. Moreover, it is unlikely to be beneficial if no intermediary is needed, or a trusted one already exists. But in transactions involving multiple parties, perhaps with competing incentives, where an iron-clad record of data is needed, and no central trusted authority is available or needed—then blockchain technology holds out huge promise, which insurers would be wise to explore. □

Matt Higginson is a partner in McKinsey's New York office, **Johannes-Tobias Lorenz** is a senior partner in the Düsseldorf office, **Björn Münstermann** is a partner in the Munich office, and **Peter Braad Olesen** is an associate partner in the Copenhagen office.