The Blockchain cures all ails. It is an immutable (unchangeable) and unhackable database. It lowers transaction costs and enables trust between strangers. It unshackles us from authority. It will revolutionize insurance: Executives everywhere must pay attention. Blockchain is the new plastic. Or so the myth goes.

Numerous articles have explained how using a blockchain will lower costs, increase profitability and produce a clear competitive advantage for insurers. Fewer articles cover blockchain mechanics and magic—yes, it contains some magic. Executives need to have a basic understanding of the mechanics and an appreciation of the magic in order to assess the applicability of blockchains to their insurance business problems. This article will step back from the hype and explain how a blockchain works. It will highlight some surprising capabilities and debunk some confusing myths and inaccuracies.

Executives need to have a basic understanding of the mechanics and an appreciation of the magic in order to assess the applicability of blockchains to their insurance business problems.
Blockchain is a Database

A blockchain is a database. Blockchain databases are generally distributed, that is, stored on multiple machines rather than held by a single authority.

Blockchain databases store records that can be thought of as transactions because they have a temporal order: later transactions can depend on earlier ones. The importance of transactional databases to insurance is obvious.

Individual records are stored in blocks that are chained together through an index, hence the name. The data in each block is called the payload. The payload can be structured data, such as details of a financial transaction or an insurance policy, or unstructured data, such as an image, video, or a PDF file of an insurance contract. Each block is given an index that is used to locate it. (SQL databases work this way. Even though data is presented as a table it is stored in indexed blocks.) The chain arises by including the index of the preceding block as part of data payload on each block. Chaining enforces the temporal order of the database.

Given the index of the latest block a user can pull out an ordered list of blocks from the database by following the index chain.

Database users have three concerns: does the data have integrity, is the data valid, and is the data secure? Blockchains offer innovative solutions to these three concerns.

Integrity and Hashes

Does an extract from a database faithfully match the original? That is, does it have integrity? Blockchains use hash functions, a magical mathematical construct, to ensure database integrity.

A hash function is a deterministic algorithm that will reduce an input of arbitrary length (e.g. the data on a block) to a fixed length output. A familiar example of a hash function is to concatenate the first five letters of your last name (padded if necessary) and the first letter of your first name, a hash beloved of IT departments creating user names. However, as every J. Smith knows, this hash has a problem: many different names can map to the same hash, giving a hash collision. Here’s our first magical ingredient: there exist hash functions where the probability of a hash collision is extremely low. Given two different inputs the probability the hash produces the same output is negligible. Negligible not as-in not in one hundred, but as-in the chances of a collision within one billion messages is less than the probability of picking a particular atom in the universe. The SHA256 algorithm is an example of such a hash function. It produces a 64 digit hexadecimal output, equivalent to a 77 digit decimal number.

How does a blockchain use the SHA256 hash function to ensure integrity? It is surprisingly simple. It uses the hash of the block payload as the index. Remember the payload includes the index of the previous block, as well as whatever data is stored in the block. The integrity of data download from the database is easy to check: hash the payload and compare the answer to the index of the block. If the two match you can be very confident (not quite mathematically certain, but certain enough) your extract matches the original, that is, your copy has integrity. If you know the hash-index of the most recent card in the database you can determine the integrity of a copy of the entire database by recursively computing hashes. One 77 digit decimal number is sufficient to determine if a copy of the entire 184 gigabyte Bitcoin blockchain has integrity!
Validity and Nonces

Database integrity is important, but an accurate copy of invalid data is useless. Users are also concerned their data is valid: that it is legally or officially binding and acceptable. Data validity is usually enforced by a trusted authority such as a bank, employer, insurer, or government agency. The second magical capability of a blockchain is to enable validity without an authority: to enable distributed validation of new database records.

Given a blockchain it is easy to make an invalid copy with integrity: change a block, for example to credit your bank account, and then recompute all the block index hashes. The SHA256 function is very fast to evaluate so this is a quick and easy change. There are now two different copies of the database which both have integrity. Which is valid?

Validity is an incremental problem: given a copy of the database which all users agree is valid, how should the next block of transactions be confirmed and appended? The new block needs to be consistent with the existing transactions and then “locked-in” somehow, so it becomes immutable, or at least very hard to change.

The Bitcoin network enforces validity through a proof-of-work consensus mechanism. The process has several steps. First, a so-called miner checks new transactions to ensure each is valid by looking at the existing database, which provides a record of who owns what. This stage forestalls double-spending because a miner will only allow a Bitcoin to be spent once. The miner knows that others will independently check their work, so cheating will be detected and their mining in vain. Next the miner combines a number of valid transactions into a block payload. Third, the miner computes the hash-index for the block. This is done hashing the payload concatenated with an additional number, called a nonce (number used once). The nonce is selected so that the resulting hash is smaller than a certain threshold (the block difficulty). Bitcoin miners try to find these nonces through brute-force, by trying different nonces until they chance upon one which produces a small enough hash. The brute-force mining process consumes a massive amount of electricity—another popular fact in Bitcoin press coverage! Fourth, the proposed block is transmitted to other users. If they agree it is valid it can be added to the chain and the process starts over. Checking if a block is valid is very quick—once you have been given the nonce. Miners are rewarded with newly created Bitcoins for their mining efforts.

Why does this process create an (almost) immutable record? Suppose I want to change an old block. I can do that but it takes time, the time to find the nonce for each block I want to change. As this time is elapsing, new blocks are being created. Unless I control the majority of the mining computing power (hence: 51 percent attack) I can never catch up with the current block. Thus it is practically impossible for me to go back and alter the blockchain.

Security and Encryption

A distributed database, where everyone has access to all the underlying records, appears inconsistent with good security. Blockchains use encryption to ensure security. The data payloads on each block are public but encrypted. Without a key issued by the owner of the data it is impossible (again, not mathematically impossible, but practically impossible) to extract the underlying information. Given the purported security of a blockchain why are there so many news reports of Bitcoin hacks and thefts? Encryption is an unbreakable lock—but all locks have a key.

Given the purported security of a blockchain why are there so many news reports of Bitcoin hacks and thefts? Encryption is an unbreakable lock—but all locks have a key.
For Bitcoin the key is simply a number. And that number must be stored. Steal the number and you control the Bitcoin. All reported blockchain hacks involve the theft of keys, not a breaking of the underlying encryption. If individuals hold their own keys and there are no extensive databases of keys exposed to hackers then mass data breaches cannot occur. Security has been distributed. Encrypted security technology offers some magical possibilities. It is feasible to issue security keys that allow one-time access to data. And keys that expire. To grant a third party access to check my credit record using a blockchain credit bureau I would issue a one-time, read-only key. The party would access my record at a point in time but would not be able to use the same key twice. Today, of course, I have to reveal my social security number and other sensitive information and to trust the recipient only looks at my record once. There is enormous potential for using blockchain technology to return ownership and control of private information to individuals.

Applications
Commentators often tout blockchains as a solution to the insurance industry’s processing and back-office inefficiencies. But this is a rather narrow view, and one which completely misses its true potential for insurers.

The internet, which has delivered free access to vast troves of information, has paradoxically created a Trust Vacuum. Alleged instances of election hacking highlight the need for identity verification. The Equifax cyber hack reveals the weaknesses of centrally controlled repositories of private information. Blockchain technology allows us to re-democratize data and reassert the individual’s control over their private data. To enable this will require infrastructure and an alternative revenue model. Insurers are well positioned to provide these services and to profit from the Trust Vacuum, stepping in to replace outmoded and insecure centralized networks with distributed blockchain solutions. This revolutionary model represents the true potential of the blockchain for our industry.

Insurers are well positioned to provide these services and to profit from the Trust Vacuum, stepping in to replace outmoded and insecure centralized networks with distributed blockchain solutions.
About the Author:

Stephen Mildenhall is an Assistant Professor in the School of Risk Management, Insurance and Actuarial Science at St. John’s University in New York. He was previously Global CEO of Analytics for Aon plc, based in Singapore, and head of Aon Benfield Analytics. During his career, Stephen has gained extensive experience in the global insurance industry.