Unknown date | Salvatore Babones

Forget cryptocurrencies

Bitcoin's 20-fold rise in value in 2017, from $900 at the beginning of the year to an all-time high of nearly $18,000 before falling back to just under $10,000 today, made blockchain a household word all over the world. Everyone from American millennials to Chinese grandparents got in on the Bitcoin craze. And slew of competing cryptocurrencies, most prominently Ethereum, are aggressively competing to snatch some of the Bitcoin fairy dust for themselves.

But Bitcoin is only one use case for the application of the basic database architecture called blockchain. Blockchain is what it sounds like: a series of blocks of data that are chained together in linear sequence. The sequence is maintained by a link called a hash — a scrambled code that takes the entire contents of a block of data and converts it into a 256-bit reference number.

Every time a new block of data is added to a blockchain database, it starts with a hash of the previous block. Since the previous block started with a hash of the block before that, and the second previous block started with a hash of the third previous block, and so on, the entire history of the database is distilled down into the current hash.

If you know the current hash of a blockchain, you can't rebuild the entire database from those 256 bits. But you can verify whether your version of the database is the same as someone else's. If you both have the same hash, you both have the same database. You don't have to check trillions of lines of data to make sure they're all identical. You just have to check the final hash.

The verifiability built into blockchains through their hashes means that people — and more importantly, their devices — can coordinate their behavior on the basis of just 256 bits of data. If you need millisecond decision-making, blockchain is for you. Of course, you can probably spare more than a millisecond to think over a business proposition. But your

devices can't. That's why blockchain is set to become the preferred database architecture for the internet of things.

From Bitcoin with love

The blockchain architecture was originally developed for use in cryptocurrencies by Satoshi Nakamoto, the pseudonymous inventor of Bitcoin, to power the creation of a payments system that had no central authority. If you can see that you have $20 in your account and your friend can see that you have $20 in your account, you can transfer $20 to your friend as securely as handing over a $20 bill. The hash proves that you're both working from the same shared database, so you both know the money is there.

The bane of Bitcoin is its system for updating that shared database, for writing new blocks to the blockchain. In order to keep Bitcoin free of any central authority, Nakamoto invented the concept of "proof of work," or mining. The basic idea of Bitcoin mining is that transaction service providers compete to solve a complex arithmetic problem, with the prize that whoever solves the problem first gets to process the next batch of agreed Bitcoin transactions — and earn a small fee.

Mining is a very clever idea — if you are a political anarchist who wants to run a cryptocurrency free from corporate or government control. But most of the rest of us aren't so political when it comes to buying a cup of coffee or paying our electric bills. And we can only hope that our devices have no political opinions at all. When I ask my computer to print single-sided, I don't want a lecture on saving the environment. I want my computer to verify that the printer has enough toner and paper for the job, then go ahead and print.

Powering the smart grid

The ability to verify data instantly is what makes blockchain technology so versatile. Autonomous devices don't have to be continuously connected to a central server to receive instructions and check balances. If the devices can verify that they have the same "understanding of the world" through the hashes on their cached databases, they can deal directly with each other.

The emergence of the internet of things is probably the biggest reason why blockchain will endure long after the cryptocurrency fad has run its course.

Smart electrical grids are likely to be among the most important the first adapters of the technology. Smart grids are computer controlled electricity distribution systems, and everything electrical will soon be smart enough to connect to them.

On a blockchain-based smart grid, if your neighbors run their clothes drier on a hot summer day, your fully-charged electric car might sell them power from its batteries to prevent a local power surge. Using the blockchain's distributed database, the appliances can make the deal now and tell the electric company about it later. Or if they're both linked to the same payments blockchain, they may never tell the electric company at all.

Blockchains of things

The internet of things may be the first major non-monetary use for blockchain database structures, but it won't be the last. The world of logistics is primed for a blockchain revolution. Distributed blockchain databases will let smart containers tell gantry cranes which train cars they should be loaded onto. And the instant auditability of blockchain databases will make it much easier to trace components through ever more complicated supply chains.

Self-driving car ecosystems will also rely heavily on blockchain database architectures. Autonomous vehicles have to make instantaneous decisions in communication with their environments (and each other), even when their internet connections go down. Blockchain technologies will allow them to quickly agree on the most recent state of a shared database that can be used as the basis for decision-making.

These and other IoT blockchain applications have one thing in common: they will rely on trusted central administrators to add new blocks to the data chain, not on Bitcoin-style third party "miners."

Electric companies, logistics companies, and even robo-taxi companies will each run their own proprietary blockchain databases. Individual users (and their devices) will plug into these centrally-administered blockchains to interact with the companies that run them — and with each other.

Cryptocurrencies are likely to stick around for a long time, but IoT applications will push them farther and farther toward the dark corners of the blockchain universe. The simple fact is that cryptocurrencies solve a

problem — lack of trust in authority — that most of us don't have. Speculators and anarchists may put their faith (and their money) in Bitcoin as long as its value holds up. But my dishwasher prefers cold hard cash.

Salvatore Babones

Return Home
