Unknown date | Salvatore Babones

WeChat's red packets are the perfect use case for a Chinese blockchain

February 16 was Chinese New Year, and CNY means one thing to China's mobile payments industry: red packets. These little digital envelopes full of real, spendable cash make the perfect CNY present, replacing the traditional paper envelopes that have been used for centuries. The Chinese social networking platform WeChat is the industry leader in red packets, though followed closely by AliPay and other Chinese payments systems. WeChat's brilliant innovation was to gamify red packets so that people used them as an ordinary part of interacting with their friends. In effect, WeChat surreptitiously used a payments system to build a social network.

So far as anyone outside the company knows, WeChat administers its red packets using conventional financial database management technologies. But the Chinese government is aggressively promoting the use of blockchain technology, and WeChat has all the elements already in place to put its payments system on a blockchain. The Chinese government has lately claimed down on the use of Bitcoin, the world's most popular blockchain cryptocurrency, but Bitcoin is only one use case for the application of blockchain database technology. The blockchain may have been invented for Bitcoin, but its potential applications are much wider.

How blockchain works

A blockchain is an "append only" database structure in which new records can only be added at the end of the existing database. In essence, it's little more than an activity log, but one that is immutable: once a record has been entered, it cannot be erased, though it can be reversed by a later, offsetting entry. Each new record, for example a financial transaction, includes a unique ID code that is mathematically generated as a function of the collective information incorporated in all previous transactions in the

database. As a result, if you know the ID code (called the hash) of the last transaction in the database, you can verify that all previous transactions are as advertised.

The blockchain approach makes it possible for multiple parties to work with identical copies of a single database because it ensures that everyone's copy of the database is the same. Just look at the final hash. If your hash matches my hash, we know we have the exact same data, even if the full database includes trillions of previous records.

The blockchain hash ensures the integrity of past data, but it doesn't determine who can add new data. For that, Bitcoin introduced the controversial practice of mining: every ten minutes or so Bitcoin holds an open competition to see who can solve a complicated mathematical puzzle. Whoever solves it first gets to record the next block of transactions in the Bitcoin ledger — and a small reward for their effort. That small reward is represented as the "mining" of new Bitcoins. The Bitcoin mining approach is controversial because it encourages miners to waste enormous quantities of electricity in the hope of earning a few bits of virtual currency.

But a blockchain doesn't have to rely on "mining" to determine who can enter new records. Bitcoin's mining system was invented by the pseudonymous inventor Satoshi Nakamoto to enable the maintenance of a decentralized, "trustless" blockchain in which anyone in the world could anonymously add records to a widely shared database. But a centralized blockchain to which only one "trusted" party can add records is much simpler to maintain. That may not have been Satoshi Nakamoto's intention, but it is a much more practical approach in real world applications. Large IT and financial companies will certainly administer their own blockchain databases, not rely on the anonymous public to keep them up to date.

Enter WeChat

More closely than anyone else, WeChat already approximates the blockchain model. WeChat has the right product, the right front end, and the right business need. The product, obviously, is the magical red packet. Blockchain database technology could easily be applied to recording who sends red packets to whom, and under what conditional circumstances. WeChat is already using a form of "smart contract" technology to allow people to set complicated decision rules for who can claim a red envelope,

for example, giving a random jackpot to the first of several of a person's friends who claim the envelope, with the remainder of the envelope split among the remaining friends who claim it within a specified time period. These kinds of decision rules are tailor-made for programming into blockchain smart contracts.

WeChat also embeds extensive use of quick response (QR) codes in its interface. Each WeChat user has a personal QR code, which could easily be modified to embed a public key for use in encrypting transactions (if it doesn't do this already). Combined with user's passwords acting as private keys, WeChat already has a system set up for public key cryptography, the basis of identification and hashing on the blockchain. This means that WeChat could move its entire red packet payments system onto a blockchain with virtually no change in customer behavior. With users identified by QR codes, the blockchain front end is already in place.

The only question remaining is whether or not WeChat would benefit from using blockchain technology to administer its payments system — if, indeed, it is not doing so already. The use of blockchain technology would presumably reduce opportunities for external fraud and employee theft, but these are hardly transformative developments. Potentially more profound is the opportunity blockchain technology would create for integrating WeChat's payments system into the emerging internet of things (IoT). The write-only nature of blockchain makes it well-adapted to the IoT, where even smart devices can be quite "dumb," requiring immediate decisions based on prepositioned smart contract decision rules. A blockchain-based payments system would allow WeChat to seamlessly integrate its mini-app ecosystem into the physical world of devices via a unified financial and IoT blockchain.

WeChat is already China's "everything app," used by diners to cashlessly book a table, find a ride, order dinner, share photos, and post a review all through in-app purchases and mini-apps. A blockchain payments system based on WeChat's existing QR code identification technology could tie all this together, with WeChat acting as the blockchain's central "trusted" party. The Chinese government certainly won't allow all this to be done anonymously, but if everything is tied to a biometrically-verified QR code public key, the government is likely to be all for it (since it would allow the state to verify everyone's actions on the blockchain). This is hardly the libertarian crypto-paradise imagined by Satoshi Nakamoto and other

Bitcoiners, but it is a compelling business case for a characteristically Chinese blockchain.

Salvatore Babones

Return Home