

February 13th, 2017

Bitcoin is stored and managed through a network of computers that serves as a bank. This bank is far simpler than an actual institutional bank, because it specializes in tracking only the movement of bitcoins between accounts. It does so in a secure way that prevents invalid transactions (e.g. double-spending, fraud) while maintaining complete user anonymity. This bank is called the Blockchain.

Recently, we've found a way to store arbitrary data on the bitcoin blockchain, by representing the data as a sequence of transactions. This allows us to store anything on the blockchain, for example the Seinfeld theme song, a picture of Michael Jordan or the Bible.

We believe that this technology is well-suited for digital contract storage and validation. We can store legal contracts on the bitcoin block-chain in an extremely secure way. The encrypted contract will be stored on millions of unaffiliated computers across the globe, and can never be tampered with - this key feature is especially valuable in developing countries where governments are prone to corruption.

In developed countries, it would help to eliminate costly notary services, inefficient paperwork and legal disputes. Eventually we see our product also entering the general consumer sphere - for example, the contract you might sign with a landlord or supplier. We can also support sophisticated signature schemes (such as anonymous signing, or contracts that can be approved by a majority of member signatures).

Michael Li

Saul Fuhrmann