Bitcoin: The currency of future

Sabbir Hossain

CCISO, CEH, ITILFV3, ISO/IEC 27001 LA, COBIT 5, CLPTP

Bitcoin is a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, as the system works without a central repository or single administrator. It was invented by an unknown person or group of people under the name Satoshi Nakamoto and released as open-source software in 2009. Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies. There are no physical bitcoins, only balances kept on a public ledger in the cloud, which along with all Bitcoin transactions is verified by a massive amount of computing power. Bitcoins are not issued or backed by any banks or governments, nor are individual bitcoins valuable as a commodity. Despite it is not being legal tender, Bitcoin charts high on popularity, and has triggered the launch of other virtual currencies collectively referred to as Altcoins. Balances are kept using public and private "keys," which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them. The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may send bitcoins. The private key (comparable to an ATM PIN) is meant to be a guarded secret, and only used to authorize Bitcoin transmissions. Bitcoin will eventually be recognized as a platform for building new financial services.

(b) itcoin VS (B) itcoin

Most people are only familiar with (b) itcoin the electronic currency, but more important is (B) itcoin, with a capital B, the underlying protocol, which encapsulates and distributes the functions of contract law.

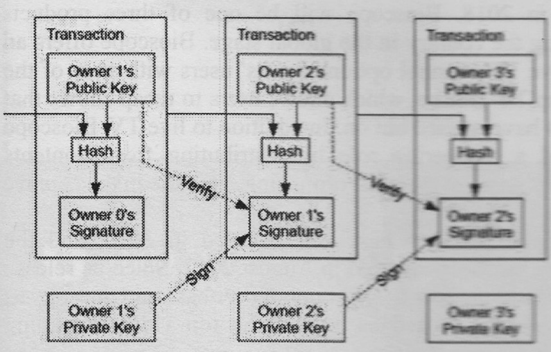

Fig: Bitcoin Transaction process

Bitcoin encapsulates four fundamental technologies :

- * Digital Signatures these cannot be forged and allow one party to securely verify a transaction with another.
- * Peer-to-Peer networks, like BitTorrent or TCP/IP difficult to take down and no central trust required.
- * Proof-of-Work prevents users from spending the same money twice, without needing a central authority to distinguish valid from invalid transactions. Bitcoin creates an incentive for miners, who run powerful computers in the network, to validate transactions and to secure them from future tampering. The miners are paid by "discovering" new coins, and anyone with computational resources can anonymously and democratically become a miner.

Distributed Ledger Bitcoin puts a history of each transaction into every wallet. This "block chain" means that anyone can validate that a given transaction was performed.

So why not just use Pounds or Dollars and use Bitcoin?

Bitcoin is only eight and a half years old, but it is the oldest and most highly valued cryptocurrency out there. In such a short time, it has had a rocky and controversial history, but it has also attracted a fair share of high-profile supporters. One can use bitcoins as high-powered money with distinct advantages. Bitcoins, like cash, are irrevocable. Merchants do not have to worry about shipping a good, only to have a customer void the credit card transaction and charge-back the sale. Bitcoins are easy to send instead of filling forms with your address, credit card number, and verification information; you just send money to a destination address. Each such address is uniquely generated for that single transaction, and therefore easily verifiable. Bitcoins can be stored as a compact number, traded by mere voice, printed on paper, or sent electronically. They can be stored as a passphrase that exists only in your head! There is no threat of money printing by a bankrupt government to dilute your savings. Transactions are pseudonymous the wallets do not, by default have names attached to them, although transaction chains are easy to trace. It has near-zero transaction costs you can use it for micropayments, and it costs the same to send 0.1 bitcoins or 10,000 bitcoins. Finally, it is global so a Nigerian citizen can use it to safely transact with a US company, no credit or trust required.

Some interesting facts about Bitcoin

- * There is a finite number of bitcoins, 21,000,000. The Bitcoin network is more powerful than 500 supercomputers put together.
- * 17 million Bitcoins are expected to be in use in 10 years. The 21 million Bitcoin limit is expected to expire in 2040.
- * The first transaction involving bitcoin was reported on May 22, 2010, when a programmer identified as Laszlo Hanyecz said he "successfully traded 10,000 bitcoins for pizza." As of October 30, 2017, 10,000 bitcoins are worth about $62 million.
- * While it may not seem like it, people continue to use bitcoins to buy stuff. The largest businesses to accept the cryptocurrency include Overstock.com, Expedia, Newegg and Dish.
- * At one point, the U.S. government was one of the largest holders of bitcoin. In 2013, after the FBI shut down Silk Road, a darknet site where people could buy drugs and other illicit goods and services, it took over bitcoin wallets controlled by the site, one of which held 144,000 bitcoins. Investors have been making a large profit by bidding on government-seized bitcoins.
- * Only 807 people worldwide have ever declared Bitcoin income for tax purposes.
- * Chinese mining pools control more than 70% of the Bitcoin network's collective hash rate.
- * Bitcoins generated as a reward for mining halves every 4 years until all Bitcoins are fully mined. A new block of coins is "solved" every ten minutes, which leads to about six new discoveries of Bitcoins per hour.
- * Bitcoin is illegal in Vietnam, Bolivia, Kyrgyzstan, Iceland, Ecuador, Thailand and Bangladesh ■