Research Paper
Impact Factor: 4. 695
Peer Reviewed & Indexed Journal

IJMSRR
E- ISSN - 2349-6746
ISSN -2349-6738

EVALUATION OF BITCOIN AND INDIA'S STAND ON CRYPTO CURRENCY

Mohammed Nahib Sulthan.M* **Huzefa A Patel***
**Department of BBA(CA),Kongu Arts and Science College,(Autonomous) Erode*.

Abstract
Bit coin was invented by an unknown person or group of people under the name Satoshi Nakamoto and released as open-source software in 2009. Bit coins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services. As of February 2015, over 100,000 merchants and vendors accepted bit coin as payment.

Introduction

Bit coin is a crypto currency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a block chain . Research produced by the University of Cambridge estimates that in 2017, there are 2.9 to 5.8 million unique users using a crypto currency wallet, most of them using bit coin .

History

On 18 August 2008, the domain name "bitcoin.org" was registered. In November that year, a link to a paper authored by Satoshi mailing list. Nakamoto implemented the bit coin software as open source code and Nakamoto titled Bit coin: A Peer-to-Peer Electronic Cash System was posted to a cryptography released it in January 2009 on Source Forge. The identity of Nakamoto remains unknown.

Block chain

The block chain is a public ledger that records bit coin transactions. A novel solution accomplishes this without any trusted central authority: the maintenance of the block chain is performed by a network of communicating nodes running bit coin software. Transactions of the form payer X sends Y bit coins to payee Z are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The block chain is a distributed database – to achieve independent verification of the chain of ownership of any and every bit coin amount, each network node stores its own copy of the block chain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the block chain, and quickly published to all nodes.

Transactions are defined using a Forth-like scripting language. Transactions consist of one or more inputs and one or more outputs. When a user sends bit coins, the user designates each address and the amount of bit coin being sent to that address in an output. To prevent double spending, each input must refer to a previous unspent output in the block chain. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. Since transactions can have multiple outputs, users can send bit coins to multiple recipients in one transaction. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments.

Mining

Mining is a record-keeping service done through the use of computer processing power. Miners keep the blockchain consistent, complete, and unalterable by repeatedly grouping newly broadcast transactions into a block, which is then broadcast to the network and verified by recipient nodes. Each block contains a SHA-256 cryptographic hash of the previous block, thus linking it to the previous block and giving the blockchain its name.
To be accepted by the rest of the network, a new block must contain a so-called proof-of-work. The system used is based on Adam Back's 1997 anti-spam scheme, Hashcash..

Supply

The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees. As of 9 July 2016, the reward amounted to 12.5 newly created bitcoins per block added to the blockchain. To claim the reward, a special transaction called a coinbase is included with the processed payments. All bitcoins in existence have been created in such coin base transactions. The bit coin protocol specifies that the reward for adding a block will be halved every 210,000 blocks (approximately every four years). Eventually, the reward will decrease to zero, and the limit of 21 million bitcoins will be reached c. 2140; the record keeping will then be rewarded by transaction fees solely.

Bitcoin paper wallet generated at bitaddress.org

Trezor hardware wallet

A wallet stores the information necessary to transact bitcoins. While wallets are often described as a place to hold or store bitcoins, due to the nature of the system, bitcoins are inseparable from the blockchain transaction ledger. A better way to describe a wallet is something that "stores the digital credentials for your bitcoin holdings" and allows one to access (and spend) them. Bitcoin uses public-key cryptography, in which two cryptographic keys, one public and one private, are generated. At its most basic, a wallet is a collection of these keys.

Privacy

Bit coin is pseudonymous, meaning that funds are not tied to real-world entities but rather bit coin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the block chain are public. In addition, transactions can be linked to individuals and companies through "idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses. Additionally, bitcoin exchanges, where bit coins are traded for traditional currencies, may be required by law to collect personal information.

T **Classification**

Bit coin is a digital asset designed by its inventor, Satoshi Nakamoto, to work as a currency. It is commonly referred to with terms like digital currency, digital cash, virtual currency, electronic currency, or crypto currency.

The question whether bit coin is a currency or not is still disputed. Bit coins have three useful qualities in a currency, according to *The Economist* in January 2015: they are "hard to earn, limited in supply and easy to verify". Economists define money as a store of value, a medium of exchange, and a unit of account and agree that bit coin has some way to go to meet all these criteria. It does best as a medium of exchange; as of February 2015 the number of merchants accepting bit coin had passed 100,000. As of March 2014, the bit coin market suffered from volatility, limiting the ability of bitcoin to act as a stable store of value, and retailers accepting bitcoin use other currencies as their principal unit of account.
o heighten financial privacy, a new bit coin address can be generated for each transaction. For example, hierarchical deterministic wallets generate pseudorandom "rolling addresses" for every transaction from a single seed, while only requiring a single passphrase to be remembered to recover all corresponding private keys.

General user

According to research produced by Cambridge University, there were between 2.9 million and 5.8 million unique users using a cryptocurrency wallet, as of 2017, most of them using bitcoin. The number of users has grown significantly since 2013, when there were 300,000 to 1.3 million users.

Payment service providers

Merchants accepting bitcoin ordinarily use the services of bitcoin payment service providers such as BitPay or Coinbase. When a customer pays in bitcoin, the payment service provider accepts the bitcoin on behalf of the merchant, converts it to the local currency, and sends the obtained amount to merchant's bank account, charging a fee for the service.

Criminal activity

See also: Bitcoin network § Criminal activity

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media. In the United States, the FBI prepared an intelligence assessment, the SEC issued a pointed warning about investment schemes using virtual currencies, and the U.S. Senate held a hearing on virtual currencies in November 2013.

Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods. In 2014, researchers at the University of Kentucky found "robust evidence that computer programming enthusiasts and illegal activity drive interest in bitcoin, and find limited or no support for political and investment motives".

India's stand on Bitcoin

It has been a tumultuous week for cryptocurrencies across the globe. While China has blocked crypto exchanges, U.S. banks are steadily declining cryptocurrency purchases. Meanwhile, Indian finance minister Arun Jaitley, during the national finance budget, stated that the country does not recognize Bit coin as legal tender and steps would be taken to penalize crypto payments, sending crypto currency enthusiasts and investors in a tizzy. Shortly after the minister's statement, the price of Bit coin fell to a two-month low of less than $7,000.

Jaitley's comments managed to invoke doubts in India's crypto community again about legitimacy of trading, except this time, authorities have decided to steer the debate clear of controversy for good.
Shortly after the budget announcement, secretary of economic affairs SC Garg said that the government will set up a panel to examine trading of crypto assets in unregulated exchanges. The panel is expected to submit its findings in a report by the end of March 2018.

Ajeet Khurana, head of the Blockchain and Cryptocurrency Committee (BACC) of Internet and Mobile Association of India (IAMAI) is one among the many people in India working towards spreading awareness on cryptocurrency in India. Following the finance minister's comments, Khurana revealed that he was happy that cryptocurrency at least found a mention in the country's national budget. "I recognized that it was a step in the right direction. Having the finance minister say that cryptocurrency isn't legal tender is perfectly logical — every nation barring Japan has taken this stance. It doesn't mean crypto trading is illegal, but comes with its own risks like any other investment asset in the market."
What happened after was unprecedented. Widespread coverage on media outlets seemed to indicate that the Finance Minister had stated that cryptocurrency was illegal, causing a tumult in investor circles. Since February 1 (when the national finance budget was announced), Khurana has been fielding calls to assuage harrowed investors and curious buyers of the government's stance and the value of crypto assets.

Conclusion

Bitcoin was soon after the financial crisis in 2008 . The aim was to eliminate man made mistakes which was the sole reason for the crisis . And to bring a complete de-centralised system . It can be a brilliant idea to avoid finical crisis. One more successful concept of Bitcoin is the Block chain . This has already been adapted by many banks and government organisation globaly .

Reference

1. Wikipedia.
2. www.coindesk.com.
3. www.iqoption.com.