CRYPTOCURRENCY -THE WORLD OF CRYPTOCURRENCIES

Mrs. Priyanka Tandel[1]

Ms. Sneha Mestry[2]

Abstract

Cryptocurrency is a form of secured digital asset. Cryptocurrency is regulated without interference of any centralized financial authorities like Banks. It is controlled online by a group of currency holders themselves which is possible only using Internet.

Cryptocurrencies use decentralized technology to let its users do secured transactions and keep record of all transactions without the need to use intermediate Financial Institutes like bank. They are maintained on a distributed open catalog called blockchain, which is a record of all transactions updated and held by currency holders.

Keywords— ***Cryptography,Blockchain, Bitcoins, E-wallet, Bitcoin Mining, Transaction, Payment, Bitgold, Currency***

Summary

The current world is full of technologies. About 80% to 90% of the transactions are being done online. So, in this world of technologies, a new cashless coin system came into emergences known as Cryptocurrency.

What is Cryptocurrency?

Crypto- indicates Cryptography used to secure the network communication and Currency- indicates various forms of money used in different countries in return of services or goods.

Currency means "Money System used in a particular country" and word crypto means "secret", is related to cryptography.

Cryptocurrency is a form of virtual asset or electronic cash. This asset is secured by using some cryptographic hashing techniques. Cryptocurrency is not under the regulation of any bank institute, government offices or centralized financial Control Unit. Instead, it utilizes the Internet to assure reliable transactions.

[1] Assistant Professor, Dept. of (MCA)YMTCollege of Management Kharghar,Navi Mumbai, India
priyankamurkute25@gmail.com

[2] Software Developer, Information Technology Department.AsiaPay India Pvt. Ltd.Chakala, Mumbai,India
sneha.mestry16@gmail.com

It is used in form of Distributed Ledger and is open for everyone.

Cryptocurrency come along with use of internet that uses cryptology, the process of converting legitimate information into an almost un-crack-able code, to track purchases and transfer of funds. CryptoCurrency Holders act as a node on its decentralized network. It makes provision for its users so that they can do secure financial transactions without using any intermediate bank institute. They execute on *distributed open catalog* called **blockchain**, keeping account of all transactions performed by currency holders.

Cryptocurrency like **bitcoin** can be used as money. It can be used to make purchase of goods and services and exchanged for conventional currencies

Bitcoin

Bitcoin is the first ever developed cryptocurrency. It is the first decentralized system. The network is Point-to-Point where transactions take place between Nodes. Cryptography is used to secure the communication among nodes of this network. The bitcoin uses the blockchain technology. The transactions are verified by network nodes and if all goes well those transactions are entered in a Distributed-open-Catalog called a *blockchain*. Bitcoin is the outcome in the form of a reward to one of the node who successfully done Mining process.

Few units of bitcoin are referred to as millibitcoin (mBTC).

A *satoshi* is the smallest unit within bitcoin, 1 satoshi = 0.00000001 bitcoin, 1 *millibitcoin* =0.001 bitcoin,

Bitcoin Prior History

In the year 1998, Just 28 years back, Wei Dai published an article for an anonymous, distributed electronic cash system known as "b-money". He is the developer of the Crypto++ library.

There was the mechanism for the decentralized digital currency known as "bit gold" developed by the Nick Szabo. Bit Gold is a currency system in electronic form. For the bit gold, the user need to complete the *proof of work* function. But thereafter the Bit Gold was never being implemented. But still he is the “direct precursor to the *Bitcoin architecture*”.

The b-money and the bit gold were the first ever proposed distributed cryptocurrencies.

Based on the work of David Chaum and Stefan Brandsecash protocols, number of other digital cash technologies were started to form.

Later Adam Back invented *hashcash*, a proof-of-work scheme which controls spam attacks. Hal Finney came with concept of *reusable proof-of-work* where it applies same hashcash for its proof of work algorithm.

Nick Szabo also contributed by adding some additional aspects, a registry to keep record of fund transfers in the form of the linked proof-of-work solutions.

A currency system based on a reusable proof-of-work was later developed by Hal Finney who followed the work of Dai and Szabo.

At last after contribution of so many people, the main hero "BITCOIN" came into existences.

Bitcoin History

Satoshi Nakamoto tried to build a digital cash system without a central controlling authority .

Like a Peer-to-Peer network, this decision became the birth of cryptocurrency.

The first decentralized cryptocurrency was named as "BITCOIN".

Satoshi Nakamoto is the first person to develop the first cryptocurrency and implement it successfully. The domain named as "bitcoin.org" was registered on the 18 Aug 2008. In November 2008,Satoshi Nakamoto published her work with title -"*Bitcoin: A Peer-to-Peer Electronic Cash System"*.

In Jan 2009, Nakamoto released the bitcoin software which was open source. Later in same month, Satoshi Nakamoto mined the first ever block of the chain, known as the *genesis block*, for a reward of 50 bitcoins.

Satoshi Nakamoto is still unknown. Later, on the bitcointalk forums, first bitcoin was used as transaction by an individual. This transaction was carried out of 10,000 BTC. This was used to purchase 2 pizzas from Papa-John's.

Cryptocurrency Technologies

P-O-W

'P-O-W' means "Proof-of-work". It is a basic protocol used to resist cyber attacks like spam attacks on the network.

The main goal is to deter the Network-attacks such as a "distributed denial-of-service" attack where attacker grab the system resources by sending spam or empty packets to make resources unavailable to legitimate users system. Most cryptocurrencies use a "proof-of-work" system. This scheme uses a hard-to-compute but easy-to-validate computational puzzle. Ideally, it's a really hard to resolve *captcha* that requires lots of computing power.

Hashcash P-O-W System

The Hashcash is basically an algorithm based on “proof-of-work” solutions which is used to limit email spam attacks & other attacks and thus assures security. Hashcash is used to create a time-stamp which is appended with message and it serves as a micro-cost to transfer the massage to control spamming. The hashcash time-stamp work as whitelisting that help its users avoid loss of Inbox Messages due to content-based or blacklist-based Anti-Spam Systems.Recently it is used in the bitcoin and the mining algorithm. Bitcoin uses the Hashcash “proof of work” for the block generation technology.

Ledger

Ledger is the bookkeeping application that store the data involved in transaction. It stores the accounting data in the plain text file, in simple format. A distributed ledger is a mutually-agreed register which is geographically distributed among all its users or currency holders , by storing shared & synchronized replicas. This ledger holds all transaction details in digital form and it is spread across multiple nodes. One form of distributed ledger architecture is the blockchain system. This system can be open/public or close/private depending on requirement.

Blockchain

A blockchain is distributed ledger. It is completely open to anyone. Blockchain technology has became backbone for an advanced internet.

This technology is nothing but the distributed database spread within the nodes on the network. As example, consider a excel spreadsheet or a file that contains data or information that is spread on the network and the same is duplicated for every node on the network. Then consider that a program which regularly update this file or excel on each and every node on the cluster. The blockchain’s data is not kept on the single node, but instead it is distributed on the various nodes of network. Hence there is no centralized system for the hacker to hack the data. Moreover this data is available to all participants who have internet connection. No single person can control this distributed database known as blockchain. This is the major benefits of the blockchain technology. The blockchain algorithm reduces human intervention to verify the transactions. It make it possible to do a Secret online transactions. The blockchain was intended to timestamp the digital documents, so it’s impossible for anyone to backdate or tamper with.

Blockchain contains two parts, firstly block and followed by the chains.

Each block contains the hash pointer, the link to the pervious block connected. The block also contains the timestamp to note the date and time for each transaction. Lastly the block contains transaction data. Now, these blocks connected with the hash makes a chain and completes the blockchain technology.

Miners must compute a proof of work for overall data in the block before the block is accepted by network participants. The new block is added to the network at every 10 min. The new block generated should have the hash value less than the current target value. The new block when generated successfully, attached to one of the node in the network and this block continuous the chain of blocks. The blocks are in the chronological order, if not so,then the pervious hash will not be known in the link. Whereas, the blocks are impractical to modify, because every block is linked with the previous block, so if one block on the node gets modified the other node’s block after it will have to be reproduced to form a chain in the network.

This makes the transaction irreversible. The block contains the hash, so changing the data will cause its Hash to change, means data is being tampered. So this technology is secured.

A Blockchain is valid if all of the blocks and transaction data within it are valid, and if it’s first block is the genesis block. There is single path to the genesis block from any other block. There can be forks in the chains as many blocks can be created from time to time. If two blocks are created at the same time at just few millisecond gap,then One-block fork gets created. If such fork is created, the block which enters first is attached to the main chain leaving back the One-block forks. The shorter chains are never being used. The shorter chain blocks are called as orphan blocks because the genesis block (parent block) is missing from the chain. A block always refer to the pervious block, so it is impossible to have two forked chain to merge. Consider a simple example, When we play a maze game, it has only one way to reach its destination. i.e. It will have only one entry point and one exit point. But there will be a lot of diversion on its path. So the road from the entry till the exit is known as the longest chain which includes the blocks.

How Does Blockchain Works?

Blockchains are incredibly popular nowadays. What is Blockchain? How do it serve? How can they be used?

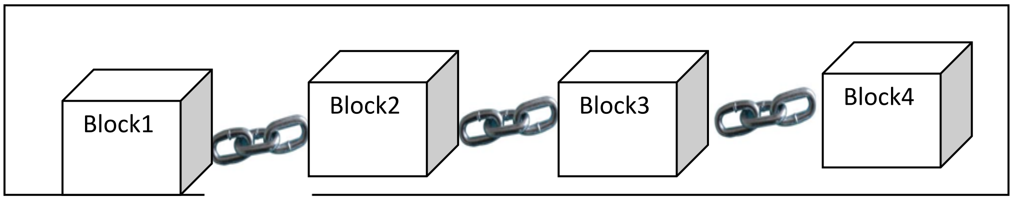


Figure A. Blockchain

Blockchain is a chain of blocks that can store Information. This technique was originally specified in 1991 by a group of researchers and was intended to timestamp the digital documents, so it’s not possible to backdate or tamper. Like Notary! This technique was further adopted by Satoshi Nakamoto in 2009 to create digital cryptocurrency, Bitcoin.

A blockchain is distributed ledger.

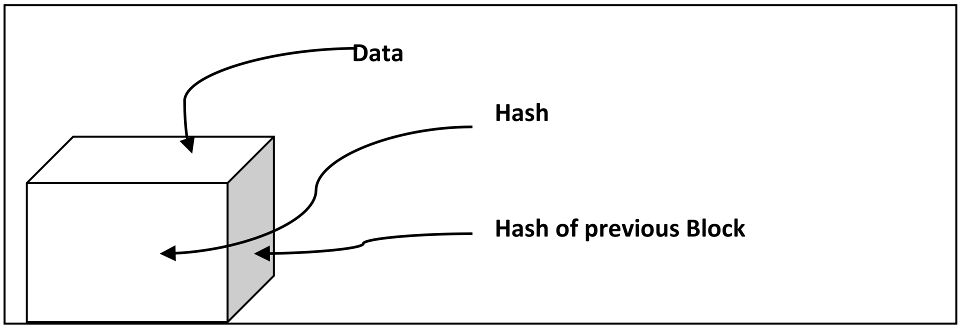
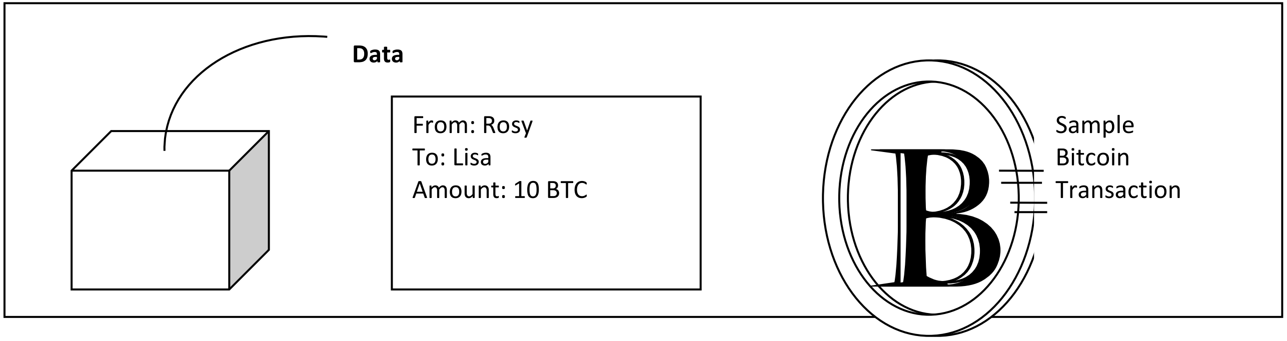


Figure B. Block Structure

Let’s look at a block. Each block contains Data, the Hashvalue of the block and previous block’s hashvalue. The Data that is stored inside the block depends on type of blockchain. The Bitcoin Blockchain, for example, stores the details of transaction, such as sender , receiver and the amount exchanged.



From: Rosy
To: Lisa
Amount: 10 BTC

Figure C. Block Transaction

The Block also has a Hash. You can compare a Hash to a Finger Print. It identifies the block and its contents & is unique just as a finger Print. Once the block is created its Hash is been calculated. If any node try to Change data inside the block will cause its Hash to change. If the fingerPrint of the block change, it is no longer remains the same block that means Block is tampered.

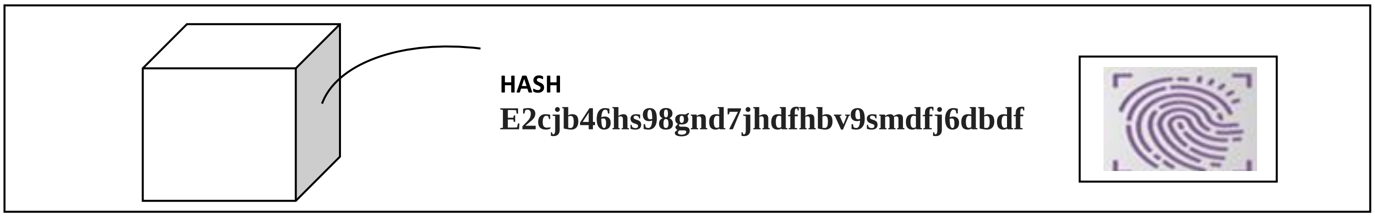


Figure D. Hash as fingerprint

The third element of the Block is the previous block’s hash value. This effectively creates the chain of blocks and this technique makes the blockchain secure.

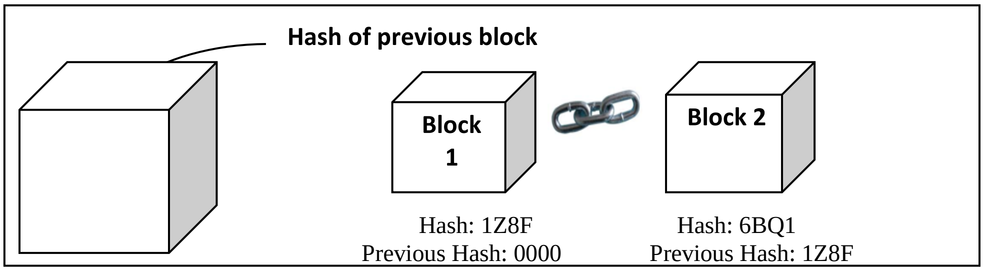


Figure E. Hash of blocks interlinked

Let’s take an example, we have 3 blocks. Each block has a hash and the hash of the previous block. So, Block3 points to Block2 and Block2 points to Block1.First Block is special, it can’t point to previous block. We call this Block as the Genesis Block.

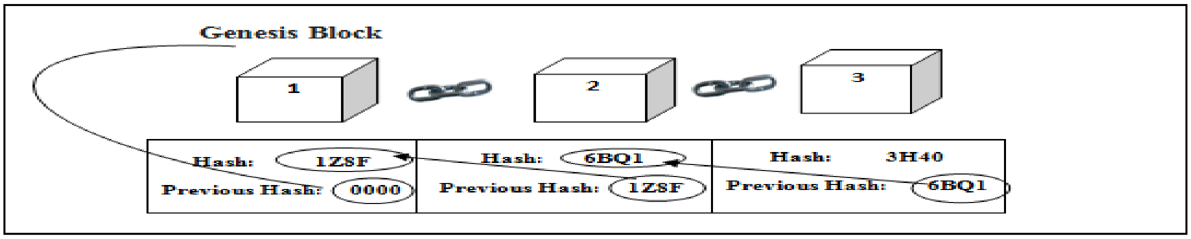


Figure F. Genesis Block & Chain of blocks

What happens when someone changes the content of Block?

Suppose Data of Block 2 in above diagram is tampered, it will cause the hash of the block to change as well. In turn, that will make Block3 and all following blocks invalid because it no longer points to previous block’s hash.

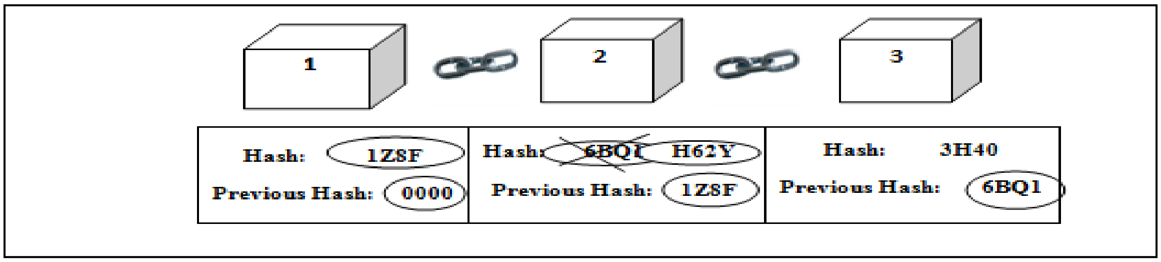


Figure G. Dishonest Node Detection

Bitcoin Minning

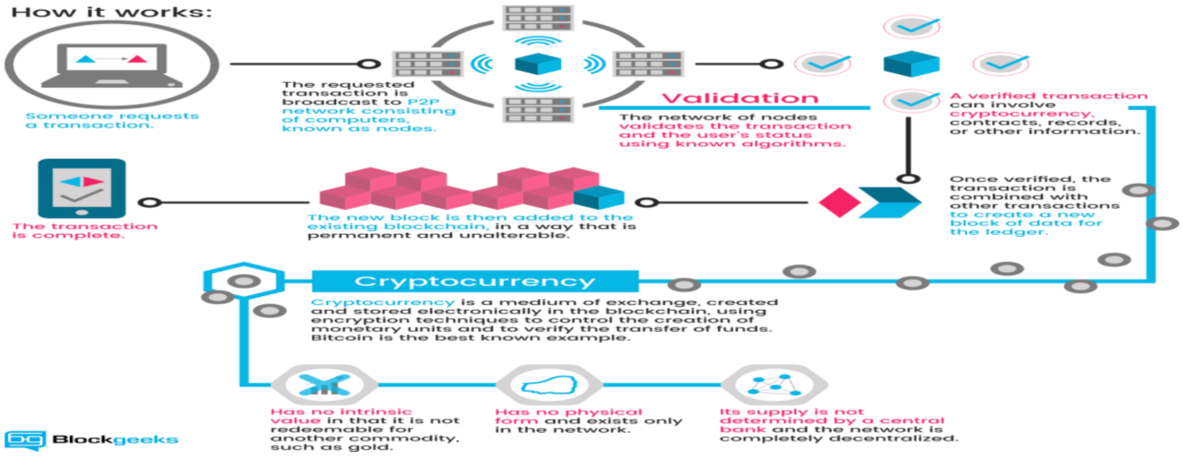

How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Blockgeeks

Figure H. Bitcoing Mining process

Bitcoin network contains network of nodes. Every node has a record of the complete history of all the transaction. For example, say a person ABC gives n number of bitcoins to person XYZ. And they are signed by person ABC’s private key. After that the transaction is broadcasted in the network, which is sent from one node to every other node on the network. Hence, all the nodes know about the transaction, but this transaction gets confirm after some specific amount of time. As the transaction gets confirmed, it is irreversible and cannot be forged. This job of confirming the transaction is done by the Miners. The process of mining is depicted in above *Figure(H).*In the cryptocurrency network , the miner can confirm the transactions. Miner attaches stamp on transaction as true and distribute them in the network. After confirmation, every node has to add it to its database. It has become part of the blockchain.

For this job, miners gets the reward of token. This token is nothing but the bitcoins.

Block is accepted by network participants only after including complete a proof of work for overall data in existing block derived by miners.

A newly created block must contain a proof-of-work with time-stamping, to be accepted by other nodes. The bitcoin miners use a nonce, (a nonce is an arbitrary number that can only be used once) The Block content is now hashed with this nonce, the result is lesser than the network's hard-to-find target. This POW is verified by other nodes in the network, but this is extremely time-consuming to generate, because Bitcoin miners must try variable range of nonce values for a secure and robust cryptographic hash. For 2,016 blocks it takes approximately 14 days that is roughly 10 min per block. The hard-to-find target is adjusted based on the network's recent performance. Thus, this system automatically adapts to the total amount of Bitcoin mining power on the overall network.

Security Of The Bitcoin Network

Mining the Bitcoin is decentralized process. All it needs a person to have an internet connection and suitable hardware to participate. The security of the Bitcoin network lies in this decentralized system architecture, since the Bitcoin network is based on agreement. If there is disagreement about, whether a block should be linked in the existing block chain, then majority consensus is considered, that is, the new block will be added to the chain if more than half of the mining power fits into consensus.

Individual person or organization may corrupt the blockchain, If he/she has control of majority nodes in that network that is greater than half of the mining power of Bitcoin Network. The idea of controlling majority of the mining power to break the block chain is known as a "51% attack".The cost of such attack is proportionate to mining power involved in the Bitcoin network. So the security of the Bitcoin network is directly proportionate to amount of mining power is employed.

Benefits Of Cryptocurrency

- Using Cryptocurrencies people can do fund transfer with each other.
- Public and private keys are used in this system for security reasons.
- Using Cryptocurrency users can avoid these extra cuts of money charged by intermediate Financial Institutes.
- Heart of the cryptocurrencies is the blockchain, an Open-Distributed-Catalog that keeps track of every transactions done using Cryptocurrency.
- A data structure used by this system is secured from attackers using some security mechanism and it can be replicated across all nodes on network having software required for bitcoin installed.
- Block chain is also used in various other applications, such as online voting, crowd funding, etc.
- Many observers look at cryptocurrency as a hope to preserve value for their investment in it.
- It will be facilitating exchanges which will be more feasible than transferring hard metals.

Drawbacks Of Cryptocurrency

- Records stored on online catalog can be damaged by a system crash if there is no appropriate backup & recovery system.

- The exchange rate of cryptocurrency is not stable due to dependency on countrywide regulations.
- Supply and demand affects the rate of Cryptocurrency as well.

Future of Cryptocurriencies

The rate of Bitcoin is increasing day by day, today it has reached till $15,000.

Daily more and more number of cryptocurrencies are being introduced in the market as litecoin, dash, NEO, ripple, bitconnect, regal coin, hecxtra coin , etc.

When Microsoft's IOTA was launched, its price was $0.03 and within a week the price has reached to $3. Many of the sport industries started adopting new cryptocurrencies. The countries like Japan & Korea has also accepted the bitcoin. India has still not accepted the bitcoin but India is on mission to launch its own cryptocurrency named Laxmi coin. It is going to get launch on 01march2018 by RBI. Russia has accepted the bitcoin legally. Chicago share market CBOE will be the first to trade using bitcoin in future.

Worldwide investors have kept their eyes on Bitcoin. Its price has risen more than tenfold this year. It is not regulated by a single country or entity. This have made it tremendously volatile. But many observers are afraid that the currency's bubble could burst, in case if governments move to crack down on its use or otherwise regulate it**.**

References

1. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer electronic Cash System." https://bitcoin.org/bitcoin.pdf
2. Blundell-Wignall, Adrian. "The Bitcoin Question: Currency Versus Trust-Less Transfer Technology." OECD Working Papers on Finance, Insurance and Private Pensions, No. 37. OECD Publishing Paris, 2014. http://dx.doi.org/10.1787/5jz2pwjd9t20-en.
3. *Siluk, Shirley (2 June 2013).* "June 2 "M Day" promotes millibitcoin as unit of choice". *CoinDesk.* Archived *from the original on 7 August 2017*. Retrieved 25 May 2017
4. Empson, Rip (28 March 2013). "Bitcoin: How An Unregulated, Decentralized Virtual Currency Just Became A Billion Dollar Market". TechCrunch. AOL inc. Archived from the original on 9 October 2016. Retrieved 8 October 2016.