By: Lawrence JamesJohnson, President; Delta Gold, LLC; Baltimore, Maryland 21215, USA
Email: deltagoldllc@gmail.com; Phone/WhatsApp: 1-443-447-5352; Skype: larryjjc

How Bitcoin Works

1. The Bitcoin Network

In late 2008, a programmer called Satoshi Nakamoto (a pseudonym) published a paper on cryptography explaining the Bitcoin concept. In January 2009, Nakamoto released software for exchanging Bitcoin. This Bitcoin software is now maintained by an open-source community coordinated by a few core developers. The operation of the Bitcoin Network can be explained in three easy steps:

STEP A – Joining the Network: (R1)
To properly buy or sell Bitcoin in any significant way, the first thing you do is to download and install Nakamoto's Bitcoin Client-Software over the internet. Once the software runs, your computer will become a node on the worldwide Bitcoin network, now numbering in the millions of nodes, and you will be connected to the decentralized network of all Bitcoin users.

The software will generate for you a pair of unique cryptographic keys which you will need to exchange Bitcoin with any other client/node in the worldwide network.
- One key is private and kept hidden in your computer.
- The other key is public and called your Bitcoin Address. This public key will be given to other people so they can send Bitcoins to you if they want to.

(It is practically impossible, even with the most powerful supercomputer, to derive someone's private key from their public key. This prevents impersonation. The use of public and private keys to identify users guarantees a high level of anonymity which is an appealing characteristic of cryptocurrencies.)

STEP B – Transferring a Bitcoin: (R1)
When a seller wants to transfer Bitcoin to a buyer, the seller's Bitcoin software performs a complex mathematical operation that utilizes and combines the buyer's public key with the seller's private key, and the amount of Bitcoin that is being transferred.

- The result of this mathematical operation is then flashed out across the distributed Bitcoin network worldwide. Every client/node in the network will be informed about the pending transfer.
- What happens next is the real genius of Satoshi Nakamoto: All Bitcoin software clients not involved in the original transfer transaction will race to verify the transaction and add it to the public log of all transactions, in order to win a reward of "newly minted" Bitcoin. This is the only way new Bitcoin is created or "mined". The clients who perform this "Bitcoin-transfer-verification/public-log-updating" task are caller miners. And the total computational effort to verify a new block transaction and update the public log of transactions is known as Proof-of-Work ("POW").
- Miners make two checks to verify a Bitcoin transfer:

  - First, miners check the public key of the sender to confirm that the true owner sent the Bitcoin. This involves another complex math that is performed by the software.
  - Second, miners check the public log of every Bitcoin, which is stored on every client's computer, to make sure that the seller owns sufficient Bitcoin to make the transaction.
- When a client verifies a transaction, it forwards the details to other clients in the network so that they too can check the results.
  - Some miners go beyond transaction verification and try to add the transaction to the public transaction log (by solving additional cryptographic puzzle using the software). The winning miner will earn the right to add the transaction to the public transaction log, which will then be sent to all computers on the network.
  - The transfer will be complete when the seller receives an updated log containing his transaction (normally within 10 minutes or less).
- The mathematics make it very easy to verify a transaction, but almost impossible to generate a false transaction (that is, to spend or sell Bitcoin that are not owned by the seller – known as the "double-spend" problem). (R1)

STEP 3 – Obtaining Bitcoin: (R1)
Bitcoin can be obtained by:

- Buying them from an exchange or private seller;
- Accepting Bitcoin in exchange for goods or services;
- Winning the race to solve the cryptographic proof-of-work puzzles (described above) to verify new transfer transactions and update the public transaction log of all transactions. A reward of "newly minted" Bitcoin is sent to the person or miner who is allowed to add/complete the next "block" to the shared transaction log.
  - The amount of Bitcoin given to miners as a reward for verifying transactions and updating the public transaction log is decreasing with time in accordance with a formula established by Nakamoto to limit the maximum total Bitcoin in existence to 21 million Bitcoin by 2040. Currently, there are between 16 and 17 million Bitcoin in existence. (R1)

2. Blockchain Technology

What is the Bitcoin blockchain? To understand what the blockchain is, we must distinguish between Bitcoin and its underlying technology. Bitcoin is a cryptocurrency that exists and trades on a network of computers. Those networks are keeping a "distributed ledger" of transactions which is being communally maintained around the world. That big distributed ledger that tracks these transactions is the blockchain.

In general a ledger is an accounting tool that keeps track of who owns what. From the development of double-entry bookkeeping in 15th century Venice, the ledger didn't change much till it was digitized in the 20th century. But it was only with blockchain that ledgers have been decentralized. Prior to Nakamoto's insight in 2008, ledgers were only understood as centralized objects. (R2)

So blockchain technology is simply a revolutionary or disruptive software tool to create a robust, secure, transparent distributive or decentralized ledger (disruptive in the sense that it can potentially replace any centralized ledger system that stores valuable information). Rather than having a central authority (such as a bank), blockchain incentivizes the peer-to-peer network to approve new "blocks", or transactions, which are then securely and irrevocably added to the "chain" of existing computer code of transactions. The peer-to-peer network essentially acts as a trusted third party, ensuring that no double spending can occur. Cryptography is used to keep the transactions secure, and to bind the blocks together, and the distributed nature of transaction approval makes the system harder to tamper with. The blockchain technology also incorporates a Proof-of-Work ("POW") system to prevent malicious users from forging or modifying transaction blocks that have already been added to the blockchain.

3. The Bitcoin Protocol

The Bitcoin Protocol, built into Nakamoto's software, stipulates that the correct transaction history is represented by the longest blockchain in the network, that is, the chain with the most computer processing unit (CPU) power and proof-of-work effort already invested. Thus all users are always working to extend the branch with the longest blockchain currently, which is rooted in the "genesis block" hardcoded in the software. Any other shorter branches are regarded as invalid blocks and ignored by the network.

This Protocol has two important implications:

- First, no block in an approved chain can be modified without redoing the proof-of-work computation for all descendant blocks. This substantially lowers the probability of a network attack because in order to change a previously approved transaction in the blockchain, an attacker must re-compute the proof-of-work for that specific block and ALL BLOCKS that came after it.
- Second, it gives Bitcoin transactions the attractive property of being irreversible. (R2)

4. To summarize:

The Bitcoin blockchain is the distributed ledger that tracks all Bitcoin transactions. Entries cannot be changed and are transparent to all parties involved. The blockchain technology provides an unforgeable and permanent record of identity, including the history of an individual's transactions, while preserving basic anonymity for users. The safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: members of the general public using their computers to help validate and timestamp transactions, adding them to the Bitcoin ledger in compliance with the Bitcoin Protocol. Miners have a financial incentive to maintain the security of the Bitcoin ledger. (R3)

By: Lawrence JamesJohnson, President; Delta Gold, LLC; Baltimore, Maryland 21215, USA
Email: deltagoldllc@gmail.com; Phone/WhatsApp: 1-443-447-5352; Skype: larryjjc

5. Implications for Private Trading of Bitcoin (BTC)

1/ Small Trial Tranches:
Requests by some Bitcoin buyers that seller send a small TRIAL TRANCHE of Bitcoin to buyer, (sometimes called a "satoshi transaction") to show that seller has control of his wallet, simply reveals buyer's misunderstanding of how Bitcoin works as described in this paper. For as long as a seller originates a BTC transfer of ANY AMOUNT from a node/client in the Bitcoin network (which means that the seller owns legitimate public and private keys generated by Nakamoto's Bitcoin software) and sends the BTC to a buyer with their own legitimate public key/wallet address on the network, the universe of miners reacts instantly and within 10 minutes or less will validate the transfer transaction and update the Bitcoin blockchain!

A seller with control of his wallet simply means a seller with a legitimate private key. A network validation of a BTC transfer and updated Bitcoin ledger/blockchain can never happen after the seller transfers BTC to a buyer unless the seller was the actual owner of the BTC transferred and had control of his BTC wallet.

In short, a small Trial Tranche presents no additional security benefits to a buyer.

2/ Face-to face Private Exchanges:
Face-to-face transactions suffer from the same limitations described above for small Trial tranche deals, in that they also do not present additional security benefits to a buyer (assuming that both buyer and seller belong to the Bitcoin network). In addition, however, face-to-face deals must contend with insecure Wifi networks where the TTM between buyer and seller is being held. Unless great care is taken, which will not always be possible, buyer and seller run the terrible risk of exposing their private keys either to the other party and/or to nearby third parties which could be financially costly for the exposed party.

References:

(R1) Excerpts from: "VATCOIN: THE GCC'S CRYPTOTAX CURRENCY" By: Richard T. Ainsworth, Musaad Alwohaibi, & Mike Cheetham (August 2016)
(R2) Excerpts from: "Bitcoin: The Future of Digital Currencies?" By: Starry Peng, School of Engineering & Applied Science, University of Pennsylvania (December 2013)
(R3) Excerpt from: Comments appended by: Anumakonda Jagadeesh, to "Knowledge@Wharton" article on "The Age of Cryptocurrencies: Is this the End of Money?" By: Geoffrey Garrett