Blockchain Technology*

– The Basis for Cryptocurrencies –

Prof. Dr. Victor David Sánchez, Ph.D.
Brilliant Brains. Palo Alto, California

January 2018

Abstract

Through the digital transformation of the economy's transactions, their associated regulation and administration activities have come under heavy pressure for which new methods need to be introduced. The development of blockchain technology is ongoing and promise to deliver some relief and become an integral part of the necessary tool set. In general terms, a blockchain can be understood as an open, distributed ledger used to record transactions in an efficient, verifiable, and permanent fashion [5]. The underlying principles include the use of distributed databases, peer-to-peer information transmission, transparency with pseudonymity, record irreversibility, and computational logic. Using blockchain technology, the transactions' information can be encoded digitally and as such be stored and protected in distributed databases eliminating intermediaries allowing people/organizations and machines/algorithms to efficiently and frictionless interact with one another.

The author has been actively involved for 3 decades in the development of the key underlying technologies and turnkey systems that made blockchain technology possible including secure computer systems and heterogeneous, scalable, real-time, parallel distributed computing architectures for government and private industry programs and applications. For example, after building ASIC-based custom multiprocessors and Real-Time Operating Systems (RTOS) for automation at Siemens AG based among others on ASICs which we designed with an AI-based tool for VLSI the author developed at the Karlsruhe Institute of Technology (KIT), the author, as a decade-long civil servant of the German federal government, designed and built at the German NASA (DLR) an scalable, heterogeneous, parallel distributed supercomputer, the world's fastest of its time, to provide real-time Artificial Intelligence (AI) for space and terrestrial applications [6], an architecture which was almost half a century ahead of its time and which the author initially wanted to build at Siemens Corporate R&D in Munich, Germany. That real-time supercomputer was used in a NASA-ESA-DLR spaceshuttle-spacelab mission flown with the Spaceshuttle Columbia. On the other hand, with the Harris Secure Computer Division in Ft. Lauderdale Florida, he was a senior member of the development team of a Secure (LAN/WAN) Operating System at the highest level of trust in an NSA-related program and he was the head technologist in a telecom-multimedia startup in Pasadena, California, whose technology including encryption in hardware was successfully acquired by Broadcom Corp. within one year for $\$1/3^+$ billion and $2{,}000^+$% ROI. Last but not least, the author has been using own developed ledger-based methodologies for over a decade.

REFERENCES

[1] L. Law et al. How to make a mint: The cryptography of anonymous electronic cash. The American University Law Review 46(4)1131–1162, 1997.

[2] National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS PUB 180-4, August 2015.

[3] M. Orcutt. Why America's Biggest Bank Digs Anonymous Cryptocurrency. MIT Technology Review, November 24, 2017.

[4] M.E. Peck. The cryptoanarchists' answer to cash. IEEE Spectrum 9(6)50–56, 2012.

[5] Harvard Business Review. The Truth About Blockchain. `https://hbr.org/2017/01/the-truth-about-blockchain`.

[6] V.D. Sánchez. Continuous Big Data Applications in Industry – Modern Development Tools, Distributed Operational and Orchestration Systems, Internet of Things –. `http://profdrvdsaphd.lima-city.de/documents/ContinuousBigDataApplications.pdf`, December 2016.

*This abstract has been granted permission for public release.

Blockchains are secure and fault tolerant by design. For example, cryptocurrencies are alternative, virtual, digital currencies based on blockchain technology that use cryptography for transaction security, additional unity creation control, and asset transfer verification. Bitcoin, the first decentralized cryptocurrency was created as open-source software in 2009 by S. Nakamoto, a pseudonymous developer during the height of the Great Recession, who also mined the genesis block, i.e., the first ever block on the chain, and left without further involvement in 2010. Mining uses the cryptographic hash function SHA-256 [2] as its proof-of-work algorithm. It showed that computers connected via the Internet and software could facilitate the peer-to-peer of exchange of "money" instead of a bank. The network computers maintain a secure ledger of every transaction called blockchain to prevent counterfeiting. With an electronic cash system, in analogy to physical cash, two abuses belong to counterfeiting: token forgery or creating a valid looking coin without making a corresponding bank withdrawal and multiple spending or using the same token over again [1]. Counterfeiting can be addressed by detection after the fact or by the preferable prevention. Predecessors to bitcoin include ecash, digicash, b-money, and bit gold. Currently, popular cryptocurrencies apart from bitcoin include among others bitcoin cash, ethereum, litecoin, and ripple. Figure 1 outlines a bitcoin transaction.

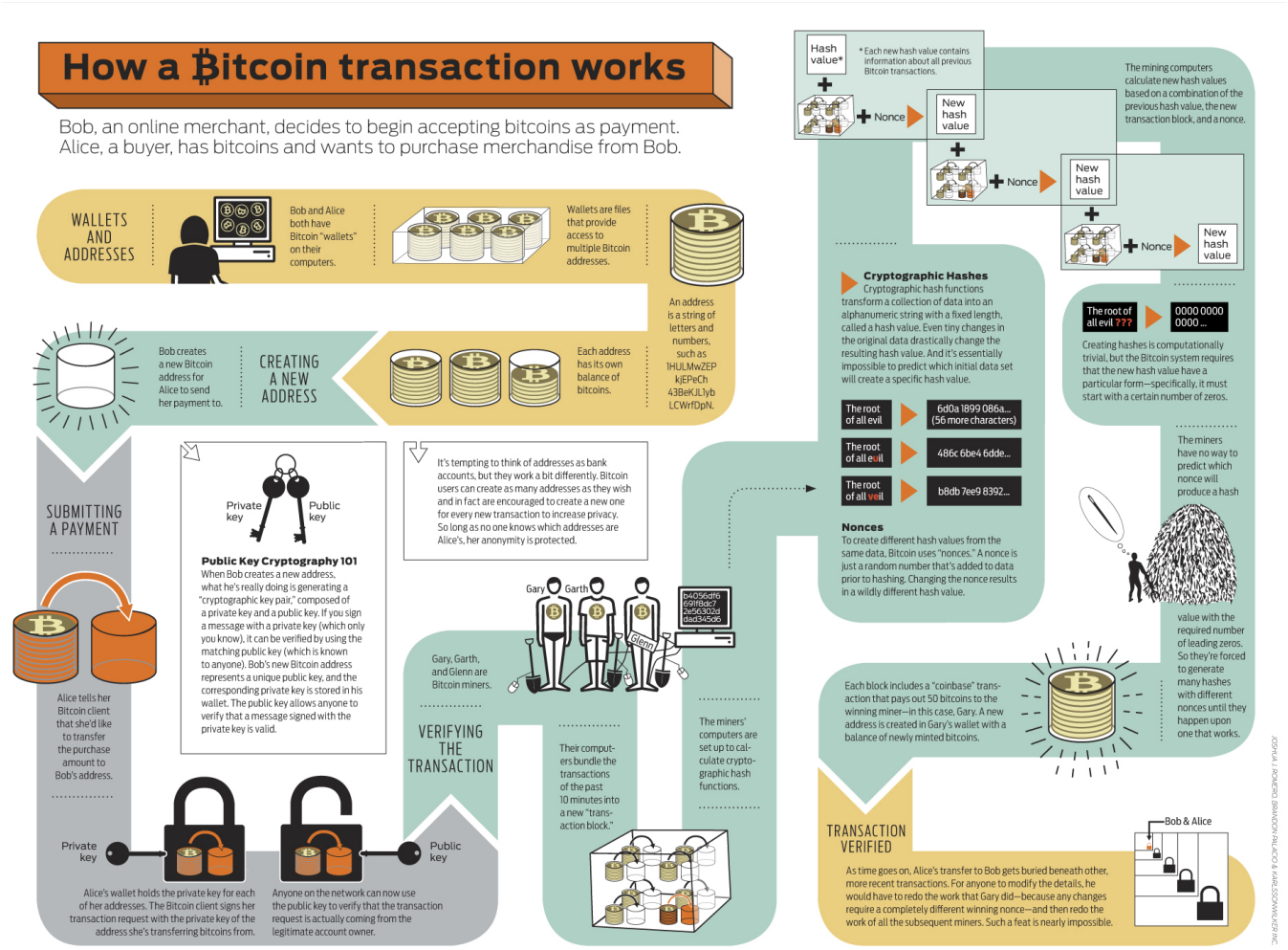

Figure 1: Bitcoin transaction [4]

Young and younger players keep on pushing for new developments and alliances attempting to position themselves best in the market place. Examples are numerous. In one example, Robinhood is about to become Coinbase' main competitor as a digital currency exchange with its new zero-commission Crypto app. In another example of this sort of events, JPMorgan's collaboration with the startup Zcash [3] shows that established financial institutions are highly interested in potentially adopting blockchain technology for use in the entire financial industry. Since the financial industry thrives on privacy, the collaboration is well founded on cutting-edge cryptocurrency privacy technology based on zero-knowledge proofs. JP Morgan Chase & Co. is the largest U.S. bank with $2.5 trillion in assets and the world's 2nd most valuable bank by market capitalization. This in-depth review includes basic concepts and infrastructure, trends, related issues in as wide areas of impact as socioeconomic, policy and legislation, and of course technology advances which as always shake the grounds of progress and civilization.