BLOCKCHAIN TECHNOLOGY – ANOTHER WONDER TECHNOLOGY FOR AFRICA?

PROF. JOSEPH M. KIZZA,

Editor-in-Chief

Department of Computer Science and Engineering,

The University of Tennessee-Chattanooga, Tennessee, 37403, USA.

IJCIR Reference Format:

Kizza, Joseph. M. "Blockchain Technology – Another Wonder Technology for Africa?", Vol. 11, Issue.2 pp 5 - 13. http://www.ijcir.org/volume 11-issue 2/article 1.pdf.

INTRODUCTION

Blockchain, *Bitcoin*, *Dogabit* and other unpronounceable terms are dominating conversation these days across the globe. What do they mean and why are they the talk of the block? What are these words and concepts that have come to excite not only a few people, age groups, a country but all generations, all country and it cuts across the globe, rich and poor countries alike, mean? As we will shortly see, all these terms refer to the same technology- blockchain. B**lockchain**, was originally **block chain**, a continuously growing list of records, called *blocks*, which are linked data blocks and secured using cryptography [1]. In elementary computer science these linked data blocks are called linked lists. In its traditional way, the chain of blocks consists of connected blocks where each block has a hash pointer as a link to a previous block, a timestamp and of course the transaction data. Because each block data hashes into a *unique number*, blockchains are inherently resistant to modification of the data. Any transaction, between any two or more parties, that uses the data in any of these blocks, according to [2] is in the open, distributed among more than one server, in a peer-to-peer network of servers, uses efficiently verifiable protocols and permanent. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority [1]. This last feature of, decentralized consensus, possessed by the blockchain technology gives it broad appeal in a variety of areas requiring recording of events such as medical records, all types of records management activities, such as identity management, transaction processing, documenting provenance, food traceability or voting [1].

Working of Blockchain Technology

The working of the blockchain technology can be briefly described in the following steps:

1. A transaction (financial or otherwise) involving several parties is initiated by one of the parties at the party's digital device. This transaction may be a payment (i.e. Credit card transaction, or a bank transfer, bill payment or others). The device sends the transaction on to its server in the peer-to-peer network.
2. The initiator's server broadcasts the transaction to all servers in the peer-to-peer network. All servers get the same transaction from the broadcasting server.
3. Upon receipt, each server runs its cryptographic verifying algorithm and generates a proof of the transaction – an invoice.
4. A new block to house the transaction data and invoice is generated and this data is stored in the new block. The block is chained to the existing chain of blocks to create a new, longer (by one block) permanent and unalterable blockchain and stored at each server in a peer-to-peer and any request to any block data on the chain must be approved by all servers.

The blockchain was started in 2008 by an anonymous person, a Japanese called Satoshi Nakamoto (there has been pictures of a person many believe is him) and applied on a *cryptocurrency* called the ***bitcoin***, in 2009. So by this transaction, the bitcoin automatically became the first digital currency to solve the *double spending problem* (counterfeiting or coping), without the need of a trusted authority or central server. Since then, there has been many other kinds of digital currencies including those in table 1 below:

Table 1. Cryptocurrencies since 2099 Source: Wikipedia. https://en.wikipedia.org/wiki/List_of_cryptocurrencies

lease	Status	Currency	Symbol	Founder	Hash algorithm	Cryptocurrency blockchain (PoS, PoW, or other)	Notes
2009	Active	Bitcoin	BTC,[4][5] XBT	Satoshi Nakamoto[nt 1]	SHA-256d[6][7]	PoW[7][8]	The first decentralized ledger currency. Cryptocurrency with the most famous, popular, notable and highest market capitalization.
2011	Active	Litecoin	LTC	Charles Lee	Scrypt	PoW	The first cryptocurrency to use Scrypt as a hashing algorithm.
2011	Active	SwiftCoin	STC	D[11]	SHA-256	PoW	First digital coin with theoretical value based on the work required to produce electricity. First block chain to support currency creation by interest paid on debt. Solidus Bond proto smart-contract. One of the first digital coins patented in the US. First block chain to support encrypted mail with attachments.
2011	Active	Namecoin	NMC	Vincent Durham[9][10]	SHA-256d	PoW	Also acts as an alternative, decentralized DNS.
2012	Active	Peercoin	PPC	Sunny King (pseudonym)[12]	SHA-256d[13]	PoW & PoS	The first cryptocurrency to use POW and POS functions.
2012	Active	Bytecoin	BCN		CryptoNote	PoW	First cryptocurrency based on the CryptoNote algorithm. Focused on user privacy through impassive and anonymous transactions
2013	Active	Primecoin	XPM	Sunny King (pseudonym)[12]	1CC/2CC/TWN[23]	POW[23]	Uses the finding of prime chains composed of Cunningham chains and bi-twin chains for proof-of-work, which can lead to useful byproducts.
2013	Active	Emercoin	EMC	EvgenijM86 & Yitshak Dorfman	SHA-256	PoW & PoS	Trusted storage for any small data: acts as an alternative, decentralized DNS, PKI store, SSL infrastructure and other.
2013[16][17]	Active	Gridcoin	GRC	Rob Hälford [18]	Scrypt	Decentralized PoS	The first cryptocurrency linked to citizen science through the Berkeley Open Infrastructure for Network Computing[19][20]
2013	Active	Omni	MSC	J. R. Willett [21]	SHA-256d[22]	N/A	Omni is both digital currency and communications protocol built on

							top of the existing bitcoin block chain.
2013	Active	Ripple[24][25][26]	XRP[26]	Chris Larsen & Jed McCaleb[27]	ECDSA[28]	"Consensus"	Designed for peer to peer debt transfer. Not based on bitcoin.
2013	Active	Dogecoin	DOGE, XDG	Jackson Palmer & Billy Markus[14]	Scrypt[15]	PoW	Based on an internet meme.
2014	Inactive	Coinye	KOI, COYE		Scrypt	PoW	Used American hip hop artist Kanye West as its mascot, abandoned after trademark lawsuit.
2014	Active	Synereo AMP	AMP	Dor Konforty & Greg Meredith[36]	PoS	PoS	Trying to create a world computer, Synereo's 2.0 tech stack incorporates all faculties needed to support decentralized computation without central servers.[37]
2014	Active	MazaCoin	MZC	BTC Oyate Initiative	SHA-256d	PoW	The underlying software is derived from that of another cryptocurrency, ZetaCoin.
2014	Active	NEM	XEM	UtopianFuture (pseudonym)	SHA3-512	POI	The first hybrid public/private blockchain solution built from scratch, and first to use the Proof of Importance algorithm using EigenTrust++ reputation system.
2014	Active	Titcoin	TIT	Edward Mansfield & Richard Allen[38]	SHA-256d	PoW	The first cryptocurrency to be nominated for a major adult industry award.[39]
2014	Active	Nxt	NXT	BCNext (pseudonym)	SHA-256d[35]	PoS	Specifically designed as a flexible platform to build applications and financial services around its protocol.
2014	Active	BlackCoin	BC	Rat4 (pseudonym)	Scrypt	PoS	Secures its network through a process called minting.
2014	Active	Monero	XMR	Monero Core Team	CryptoNight[31]	PoW	Privacy-centric coin using the CryptoNote protocol with improvements for scalability and decentralization.
2014	Active	Stellar	XLM	Jed McCaleb	Stellar Consensus Protocol (SCP) [40]	Stellar Consensus Protocol (SCP) [41]	Open-source, decentralized global financial network. The usage is for remittances, micropayments, services for the underbanked, mobile money/branches and professional setups.
2014	Active	Vertcoin	VTC	Bushido	Lyra2RE[42]	PoW	Next-gen ASIC resistance and first to implement stealth adresses.

2014	Active	Burstcoin	BURST	Burstcoin Community	SHA-256d	Proof of Capacity	First Proof of Capacity coin, First Smart Contract, First Atomic Cross Chain Transfer.
2014	Active	PotCoin	POT	Potcoin core dev team	Scrypt	PoS	Developed to service the legalized cannabis industry
2014	Active	Auroracoin	AUR	Baldur Odinsson (pseudonym)[29]	Scrypt	PoW	Created as an alternative to fiat currency in Iceland.
2014	Active	NEO	NEO	Da Hongfei & Erik Zhang	SHA-256 & RIPEMD160	dBFT	Chinese based cryptocurrency (formerly ANT Shares which produce ANT Coins) name change August 2017 to NEO and GAs, these enable the development of digital assets and smart contracts.
2014	Active	DigitalNote	XDN	XDN-dev team, dNote	CryptoNight[31]	PoW	A private cryptocurrency with an instant untraceable crypto messages and first blockchain banking implementation, use CryptoNote protocol.
2014	Active	Dash	DASH	Evan Duffield & Kyle Hagan[30]	X11	PoW & Proof of Service[nt 2]	A bitcoin-based currency featuring instant transactions, decentralized governance and budgeting, and private transactions.
2014	Active	Verge	XVG	Sunerok	Scrypt, x17, groestl, blake2s, and lyra2rev2	PoW	
2015	Active	IOTA	IOT, MIOTA[48]	David Sønstebø, Sergey Ivancheglo, Dominik Schiener and Dr. Serguei Popov	SHA-3	Directed acyclic graph	The first cryptocurrency using the Tangle, a next generation blockchain, as distributed ledger technology.
2015	Active	Tether	USDT	Jan Ludovicus van der Velde[32]	Omnicore [33]	PoW	Tether is backed by the USD so that one tether is exactly equal to $1USD. It is commonly used to convert other cryptocurrencies to USD. [34]
2015	Active	Ethereum	ETH	Vitalik Buterin[43]	Ethash[44]	PoW	Supports Turing-complete smart contracts.
2015	Active	Ethereum Classic	ETC		Ethash[44]	PoW	An alternative version of Ethereum[45] whose blockchain does not include the DAO Hard-fork.[46][47] Supports Turing-complete smart contracts.
2015	Active	SixEleven	SIL	fflo (pseudonym)[49]	SHA-256d	PoW	Also acts as an alternative, decentralized DNS.

2016	Active	Zcash	ZEC	Zooko Wilcox	Equihash	PoW	The first open, permissionless financial system employing zero-knowledge security.
2016	Active	Waves Platform	WAVES	Sasha Ivanov	PoS	PoS	Open blockchain platform, featuring token creation, distributed exchange and fast high volume transactions designed for ease of use[50] and mass adoption.
2016	Active	Lisk	LSK	Max Kordek	DPoS	DPoS	Lisk is a dapp creation platform in Javascript. Lisk uses a Delegated-Proof-of-Stake (DPoS) consensus mechanism.
2016	Active	Decred	DCR		Blake-256	PoW/PoS Hybrid	Built in governance and hybrid PoW/PoS.
2017	Active	Ubiq	UBQ	Julian Yap[52]	Ethash[44]	PoW	Supports Turing-complete smart contracts; air-gapped fork of Ethereum
2017	Active	Bitcoin Cash	BCH[51], BCC		SHA-256d	PoW	Hard fork from Bitcoin, Increased Block size from 1mb to 8mb
2017	Active	Electroneum					
2018	Active	Cardano					
2018	Active	Dogobit					

A ***cryptocurrency*** is a digital asset designed to work as a medium of exchange (as we use physical cash) but with the help of cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

This fast developing technology has raised lots of questions, curiosity, anxiety and excitement. There is a growing list of questions that need answers. For example is this technology here to stay or will it evaporate in a year or so like many other technologies before it? What advantages does it have over all other technologies before it? How will it advance the way we work and overall human conditions. The answers to these questions and a lot more lie in understanding what it is and what are its promises.

According to Lucas Mearian [3], blockchain technology is the most disruptive technology in decades. He believes, the technology has the potential to eliminate huge amounts of record-keeping, save money and disrupt IT in ways not seen since the internet arrived. May be he is right.

But no one knows at this time. Everyone is guessing where the technology is heading. Millions are betting their livelihoods on it. Probably the biggest reason why mullions, knowingly or otherwise, are betting on it is that for the first time in human business transactions, here is a technology that eliminates the need to trust the other party when you transact with them. The core and hard backbone reason for this is that the whole peer-to-peer network upon which the distributed technology is transacting is public and safeguarding every record on every server making the issue of hacking a blockchain database is pointless. For this very reason, the technology may be a business transaction and global payment systems game changer for everyone rich or poor, highly educated or illiterate, living in a first world or a third world. Everyone is treated the same. What this means is that the problem of individual and private record keeping where vital and essential records can be vandalized, stolen, or just lost cannot happen anymore. Yes, with all these benefits, the technology offers a dirty cheap and inexpensive way to transact, store and transfer records. Thus, anyone, anywhere, with an Internet connection can use. In a way, it looks like a business and all other transactions equalizer technology.

BENEFITS FOR BLOCKCHAIN TECHNOLOGY

There any many benefits for this most disruptive technology but those that form the core benefits are the following:

1. Between the transacting parties, and even between the transaction initiating device and the peer-to-peer servers there is no intermediaries and no delegation.
2. The transactions in the peer-to-peer network are in public, very transparent and based on incorruptible cryptographic algorithms.
3. Because the technology is based on a peer-to-peer network, it is decentralized and has no one point of failure and final decision is based on a majority vote.
4. Because of the full participation of every server in the peer-to-peer network and the enhanced cryptographic algorithms used to produced a hash in every block of the chain, there is assured security.

BENEFITS FOR AFRICA

For Africa, a continent that has been on the receiving end of old, expensive and many time discriminating technologies, blockchain technology, inexpensive, secure, and can be used by anyone, anywhere, with an Internet connection, on per with any body else anywhere on the globe is a wonder technology that may transform the continent way beyond what the internet and mobile technology have done. Because of these characteristics of blockchain technology, Africa can benefit in a number of ways including:

1. International Transactions and Financial Inclusion

According to Gautam Vir , CEO of the State Bank of Mauritius, close to 80% of Africa's adult population, representing 326 million people, is either unbanked or unabankable [5]. However, financial inclusion and access to capital plays a vital role in reducing poverty. Besides low numbers in bankable African, there is a limited number of financial institutions which leads to lack of access to international transactions. In turn, as Maria Cemerio [4] notes, this prevents poor people from participating in the global market. Blockchain technology has the ability to overcome these hurdles. Using the internet and mobile technology, blockchain can help build financial relationships from all corners of the world without financial intermediaries [4].

2. Fighting the endemic corruption

One of the enduring and mainstay of blockchain technology is its incorruptible cryptographic features that will put an end to corruption in many sectors of society and in this area, Africa is likely to gain the most. For example, conversion of most documents that have chronically been the source of major corruptions like voting cards, national ID, passports, birth certificates, driver licenses, and marriage certificates to digital documents and moving them into the blockchain technology will see these ills greatly diminished.

3. Strengthening of the business and financial sectors

The growth of national economies are mostly based on strong business and financial foundations and principals. These two sectors anchor and are custodians of major contracts and all financial transactions including those in banks and microfinancial institutions need reliable and incorruptible transactions offered by blockchain technology.

REFERENCES

1. WIKIPEDIA. https://en.wikipedia.org/wiki/Blockchain.

2. *HARVARD BUSINESS REVIEW*. https://en.wikipedia.org/wiki/Harvard_Business_Review.

3. LUCUS MEARIAN. What is blockchain? The is the most disruptive technology in decades. https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html.

4. MARIA CENTEIO. How Blockchain Technology Can Benefit Developing Countries. https://cvhustle.com/blockchain-technology/.5. The Internet Society Blockchain 5. Special Internet Group (ISOC-BSIG). *Blockchain Technology: Opportunities for Africa.* https://www.isoc-bsig.org/blockchain-technology-opportunities-africa/