International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Effects of new Buzzword "Blockchain" on Developers

Author(s): Manisha Pal and Edvin Guromin

Vivekanand Education Society's Institute of Technology, Mumbai, India

Vivekanand Education Society's Institute of Technology, Mumbai, India

Abstract

The blockchain, which is at the heart of Bitcoin, has recently gotten a lot of attention. Blockchain acts as an immutable record that allows decentralized transactions to take place. Blockchain-based applications are gaining traction in a variety of industries, including financial services, reputation management, and the Internet of Things (IoT), among others. However, there are still a number of issues with blockchain technology to address, such as scalability and security concerns. This paper provides an in-depth look at blockchain technology. First, we give an introduction of blockchain architecture before comparing several common consensus methods utilized in various blockchains. Technical problems and recent advancements are also briefly mentioned. We also discuss likely blockchain developments in the future. [1]

Introduction

These days digital currency has turned into a trendy expression in both industry and the scholarly community. As one of the best cryptographic money, Bitcoin has partaken in an enormous accomplishment with its capital market arriving at 10 billion dollars in 2016. With an exceptionally planned information capacity structure, exchanges in Bitcoin organization could occur with next to no outsider and the centre innovation to fabricate Bitcoin is blockchain, which was first proposed in 2008 and executed in 2009[2].

Blockchain could be viewed as a public record and all serious exchanges are put away in a rundown of blocks. This chain develops as new blocks are added to it ceaselessly. Unbalanced cryptography and circulated agreement calculations have been carried out for client security and record consistency. The blockchain innovation by and large has key attributes of decentralization, persistence, namelessness and auditability. With these qualities, blockchain can significantly save the expense and work on the efficiency. Since it permits installment to be finished with practically no bank or any delegate, blockchain can be utilized in different financial administrations like advanced resources, settlement and online payments. [3]

Furthermore, it can likewise be applied into other fields including brilliant agreements, public administrations, Internet of Things (IoT), notoriety frameworks and security services.[4] Those fields favour blockchain in more ways than one. Most importantly, blockchain is permanent. Exchange can't be altered whenever it is pressed into the blockchain. Organizations that require high dependability and trustworthiness can utilize blockchain to draw in clients. Furthermore, blockchain is dispersed and can stay away from the weak link circumstance. Concerning savvy gets, the agreement could be executed by excavators naturally once the agreement has been sent on the blockchain. A blockchain is an exceptional kind of electronic record, one that depends on cryptographic strategies and new techniques for agreement to catch and get the information. It is intended to be perused by a PC, instead of by the natural eye.

A blockchain is signified by the accompanying qualities:

• The record is divided between and chipped away at by numerous, perhaps doubting, members, none of which has a solitary place of control over it.

• A consistently developing chain of record passages connects the whole history in such a way as to forestall messing with or reworking past records.

• Carefully marked exchanges or guidelines show purpose to record or change information, or to move advanced resources.

Emergence of Blockchain

Despite the fact that the blockchain has only been around for a relatively short time, its impact has already been seen throughout the technological world.

1979 – 2007: Early years of the blockchain

Many of the technologies that underpin blockchain were in development long before the now famous Bitcoin cryptocurrency. The Merkle tree, named after computer scientist Ralph Merkle, is one of these technologies. Merkle presented "tree authentication" as a method for public key distribution and digital signatures in his Ph.D. thesis at Stanford University in 1979. But Merkle wasn't the only one who had a role in laying the groundwork for blockchain. In his 1982 Ph.D. dissertation for the University of California, Berkeley, David Chaum presented a vault system for constructing, maintaining, and trusting computer systems by mutually suspicious organizations. This was a system that incorporated many of the characteristics of a blockchain. Chaum is also credited with creating digital currency, and he launched the DigiCash Company in 1989.

Stuart Haber and W. Scott Stornetta released an essay regarding digital document time stamping in 1991. The objective was to keep the document's privacy intact while avoiding the need for a time stamping service to keep track of it.

The P2P network, popularized in 1999 by the now-defunct Napster, rose to prominence during this period. Some contend that because Napster relied on a centralized server, it was not a real peer-to-peer network. Nonetheless, the service aided in reviving the P2P network by allowing the creation of a distributed system that could take advantage of the compute power and storage capacity of thousands of machines.

In this age, the notion of proof-of-work (PoW) was established to validate computing effort and prevent cyber-attacks. This led to hashcash, a PoW technique that protects against denial-of-service attacks. Hashcash was created by Adam Back in 1997 to combat email spam. Then, in 2004, Hal Finney invented reusable PoW, a technique for exchanging an RSA-signed hashcash token for a non-exchangeable or non-fungible- hashcash token.

2008-09: Bitcoin & blockchain get their start

Satoshi Nakamoto released a white paper in 2008 that explained the principles of Bitcoin and blockchain. Nakamoto is assumed to be an alias for the person — or group of people — who suggested the technique. According to the white paper, blockchain infrastructure would enable safe, peer-to-peer transactions without the need for trusted third parties like banks or governments. Although Nakamoto's exact identity is unknown, there has been no shortage of ideas.

Nakamoto built the system in such a way, so there would never be more than 21 million Bitcoin. Currently around 18 million have already been mined. Based on the current rate of mining, Bitcoin should reach the 21-million limit sometime around 2140. In the meantime, their value continues to grow, despite continuous fluctuations in price. In October 2009, a Bitcoin was worth less than 1 cent. Today, each Bitcoin is worth more than $35,000 (USD).

2010-12: Bitcoin & cryptocurrency take hold

Mt. Gox, a Tokyo-based Bitcoin exchange, was founded not long after by a programmer called Jed McCaleb. Mt. Gox was an abbreviation for Magic: The Gathering Online eXchange, a fantasy card game. Mt. Gox processed more than 70% of all Bitcoin transactions at its height. However, in August 2010, a hacker took advantage of a flaw in the blockchain coding to produce over 184 billion Bitcoin in block 74,638, damaging Bitcoin's image. Nakamoto released a fresh version of the Bitcoin software, but he vanished by the end of the year.

Despite the absence of Satoshi Nakamoto, the Bitcoin trend remained constant. One-quarter of the 21 million Bitcoins have been mined at the end of January 2011. By early February 2011, the price of Bitcoin had reached parity with the US dollar. Jed McCaleb sold Mt. Gox to Mark Karpelès shortly after. Bitcoin shortly after achieved parity with the Euro and the

British Pound Sterling. WikiLeaks began taking Bitcoin donations later that year. Mt. Gox, on the other hand, was hacked and Bitcoin was taken, resulting in an artificial reduction in value and the stoppage of trade. Then, in October 2011, Litecoin, one of the first Bitcoin spinoffs, was created.

2013-15: Ethereum & Blockchain rise to fame

When the year 2013 dawned, Bitcoin had already made a name for itself and was continuing on its upward trajectory. Coinbase reported selling $1 million worth of Bitcoin in a single month at a price of more than $22 per in February.

The creation of the Ethereum Foundation was launched in 2014. Ethereum made it possible to utilize blockchain technology for applications other than cryptocurrency. It offered smart contracts and gave a platform for developers to create decentralized apps. Financial institutions and other businesses began to understand and investigate the possibilities of blockchain in 2014, changing their attention from digital money to the development of blockchain technology.

2016-19: Blockchain getting a world wide acceptance.

Instead of being recognized as two concepts in Nakamoto's original work, the term blockchain has come to be accepted as a single word. A defect in the Ethereum code for decentralized autonomous organizations was exploited, causing the Ethereum network to split hard. The Bitfinex Bitcoin exchange was hacked, and over 120,000 Bitcoins were stolen, amounting to a $66 million reward.

Bitcoin has been recognized as legal tender in Japan. In some form, blockchain technology was employed by about 15% of worldwide banks.
Stripe, a popular online payment service, has ceased taking Bitcoin payments. The Blockchain Observatory and Forum was founded by the European Commission. Baidu has announced the launch of its blockchain-as-a-service platform.

Amazon has made its Amazon Managed Blockchain service available to everyone on AWS. The number of transactions on the Ethereum network has surpassed one million per day. According to Deloitte's 2020 Global Blockchain Survey, about 40% of respondents had used blockchain in production, and 55% saw blockchain as a major strategic goal.

2020-2021: The Year of the NFT

The year 2021 was declared the Year of the NFT, with a massive increase in NFT supply and demand. The rise in NFT demand, particularly within the metaverse, was spectacular around the end of the year, after Facebook rebranded as Meta and went into the metaverse.[5]

Blockchain Related Technologies

BaaS : Blockchain- as-a-Service

The development and operation of pall- grounded networks by a third party for companies developing blockchain operations is known as blockchain- as-a-service (BaaS). BaaS is grounded on the software as a service (SaaS) conception and allows guests to construct, host, and manage their own blockchain apps and associated operations on the blockchain using pall- grounded technologies. Guests profit from BaaS because it allows for faster operation development, lower conservation costs, and hastily relinquishment of Blockchain technology.[6]

DeFi : Decentralized Finance

Decentralized finance (DeFi) is a new fiscal system erected on distributed checks similar to cryptocurrencies. Decentralized finance, or DeFi, is a system of removing third parties from fiscal deals by utilizing developing technologies. The system decentralizes authority over plutocrats, fiscal goods, and fiscal services from banks and institutions. Peer-to- peer fiscal networks that employ security protocols, connectivity, software, and tackle developments are used to achieve this. Stablecoins, software, and tackle that enable the development of apps are all part of DeFi. The structure for DeFi, as well as its regulation, are still in the workshop.[7]

NFT

A non-fungible commemorative (NFT) is a fiscal security made out of digital data stored on a blockchain, which is a distributed tally. The blockchain records the power of an NFT, which can be transferred by the proprietor, allowing NFTs to be vented and changed. NFTs may be manufactured by anybody, and they need little or no rendering knowledge. Digital data similar to images, flicks, and music are constantly substantiated in NFTs. NFTs vary from commutable cryptocurrencies in that they're uniquely recognizable. The digital train that an NFT refers to determines its request worth.

NFT proponents say that they give a public instrument of authenticity or substantiation of power, still the legal rights that an NFT conveys might be nebulous. The power of an NFT, as defined by the blockchain, has no natural legal meaning and doesn't indicate brand, intellectual property rights, or other legal rights over the digital material it's connected with. An NFT doesn't block the product of NFTs that source analogous lines, nor does it circumscribe the sharing or copying of its associated digital train.

From 2020 to 2021, the NFT request developed dramatically. Trade of NFTs climbed by percent to further than$ 17 billion in 2021, compared to$ 82 million in 2020. NFTs have been criticized for the high energy costs and carbon footmark associated with authenticating blockchain deals, as well as their frequent operation in art frauds. The NFT request has been compared to a Ponzi scheme or a profitable bubble.[8]

Smart Contracts:

Smart contracts[9] are computer programs that are hosted on a network of blockchain and then are executed there. Each smart contract consists of law specifying destined conditions that, when met, detector issues. By running on a decentralized blockchain rather than a centralized garcon, smart contracts allow multiple parties to come to a participating result in an accurate, timely, and tamper-evidence manner.

Smart contracts are an important structure for robotization because they aren't controlled by a central director and aren't vulnerable to single points of attack by vicious realities. When applied to multi-party digital agreements, smart contract operations can reduce counterparty threat, increase effectiveness, lower costs, and give new situations of translucency into processes.

Smart contracts are tamper- evidence programs on blockchains with the following sense “if or when x event happens, also execute y action.” One smart contract can or may have various different conditions and one operation can have multiple different smart contracts to support a connected set of processes. There are also multiple smart contract languages for programming, with Ethereum’s reliability being the most popular.

Challenges and Opportunities

While a lot can be seen about blockchain applications and its potential in the FinTech sector, little study has been conducted to explore blockchain technology's user-centric paradigm in allowing diverse applications other than banking.

One of the fundamental motivations behind why blockchain pulled in such a lot of consideration of late, is likely because of the likelihood that it can permit further layers of trust between individuals in a given organization. Blockchain innovation has been portrayed as an innovation that is trustless, mysterious, accessible and decentralized. What empowers this, is its basic calculation, ready to be based upon and mixed into various arrangements.

If appropriately created and incorporated inside the organization, blockchain can drastically have an impact on the manner in which two clients settle on the terms and execution of an agreement of any sort.

Regardless, and in spite of every single possible advantage, smart contracts actually face many difficulties, which is keeping them from accomplishing far reaching acknowledgment. Other than regulation consistency, smart contracts are more inclined to processing issues like bugs and mistakes. No computerized stage, programming or code is resistant to issue. Ethereum's Network is as likely to have hacks and issues as some other PC program.[10] Research completed in 2018 by the National

University of Singapore and University College London found more than 34,000 weak smart contracts on the Ethereum network. They have likewise distinguished how attacks came about because of the abuse of ineffectively coded agreements, provisos and different weaknesses.

The DAO (a smart contract-driven investment vehicle formed for the Ethereum blockchain) is one example of how a flaw in a poorly-written smart contract allowed most of its capital to be stolen. [11] There was a heated discussion over how to resolve the problem. This finally resulted in a split, with the majority of participants deciding to roll back the loss of money, while others maintained the status quo and formed a rival blockchain, now known as Ethereum Classic. This reversion was only possible because more than half of those who took part consented to it. It will take some time to construct smart contracts that "talk" to outside systems on a daily basis, improve, organize, and appropriately control them. For this to happen, we must also have a solid cybersecurity plan in place to cope with the new concerns brought on by smart contracts, since their growth will open up new pathways for possible harmful conduct.

Perception of Software Developers

Due to this sudden widespread use of the term blockchain and cryptocurrencies, many people, especially the developers, have gotten a new insight on this technology. This sudden boom of the term in the technological industry gave many developers a new variety of fields and options to choose from. Also due to this, many people started investing in such technologies, predicting a huge spike in the usage of blockchain. We have conducted a survey on 52 developers, who are currently either pursuing MCA or are working in the tech field. This survey mainly focuses on the thoughts of the developers on blockchain technology.

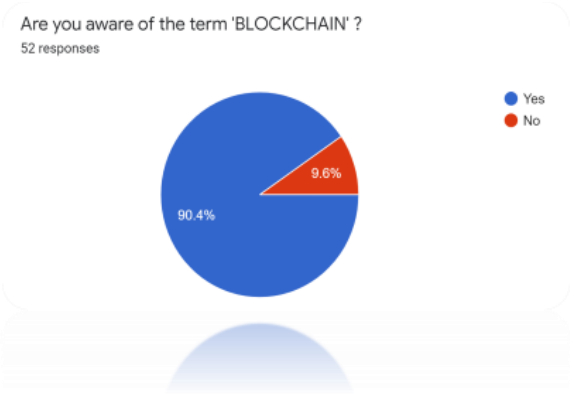

Fig 1: Awareness of the Blockchain Technology

The figure above indicates almost 90% of the respondents (developers) are aware of the technology. Looking more into the data, the main reason behind this result was due to the fact that most of the respondents are students pursuing MCA (Masters in Computer Applications). Due to the new craze of blockchain technology, the subject was added as an elective in the syllabus of MCA from the academic year 2020-21. This new subject intrigued the students and became more aware in this field.To get more insights of what all terms they are exactly aware of, we asked some more questions about the various technologies.

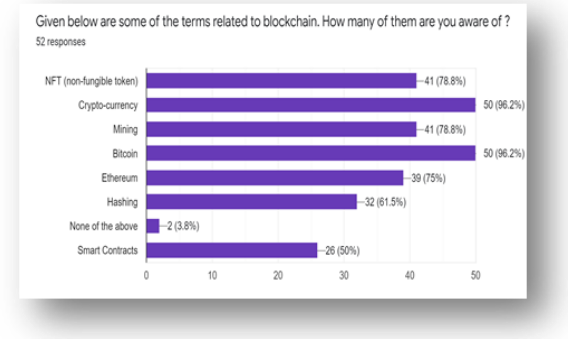

Fig 2: Survey on awareness of blockchain related terms

The above figure indicates that most people are accustomed to the terms Crypto-currency and Bitcoin. This is mainly due to the fact that many mainstream media's introduced these terms to the viewers. Many news reported about Bitcoins during the time when Bitcoin price started increasing very rapidly.

The term NFT was being used very frequently during the year 2022. This sudden fame of this term resulted

in many people investing in NFT and trying to mint those NFT. Many celebrities like Snoop Dog, Logan Paul, and Eminem started investing and buying many NFT. Due to their huge fan following, NFT got widespread popularity.

The term Ethereum, Hashing and Smart contracts was only known by the new MCA students who opted for the Blockchain elective. Students have taken interest in these technologies and this resulted in them being aware of the unheard terms.

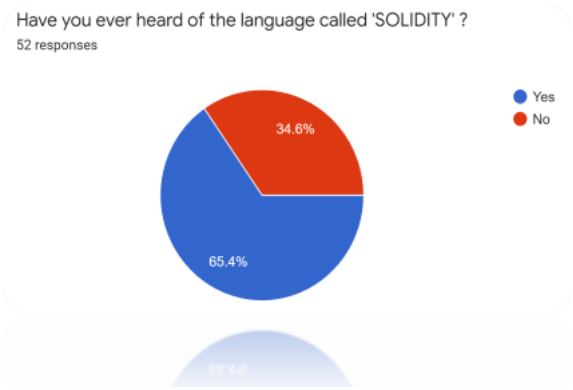

Fig 3: Survey on awareness of Solidity

The main trend seen here is only due to the MCA students opting Blockchain subject. Solidity is an object oriented programming language which is mainly used to create smart contracts. These 65.4% of the respondents have hands-on experience in this language. This made some students interested in Solidity and Smart contracts. We also asked the respondents whether they are interested in working in these technologies. Given below are the statistics we got to see.

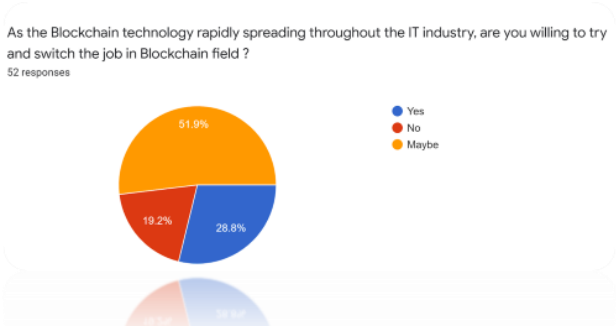

Fig 4 : Survey results of willingness to switch job to blockchain field

Even though many respondents are aware of the technology and have hands-on experience in this field, not many respondents are readily willing to work in this field. This is due to the uncertainty of the job risks of this field. Even though many companies are adapting to blockchain technology, not many vacancies and jobs are currently available in India. Due to this, many employees don't want to risk their current job by switching to blockchain technology.

Almost 52% of the respondents are not sure about whether to switch jobs or not. This is due to the same reason for the job vacancies and the uncertainty of the risk factor of the job in India.

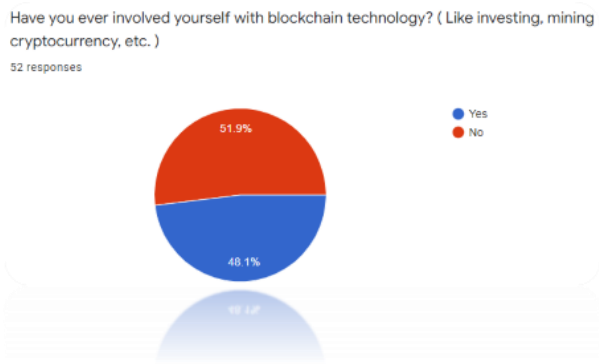

Fig 5 :

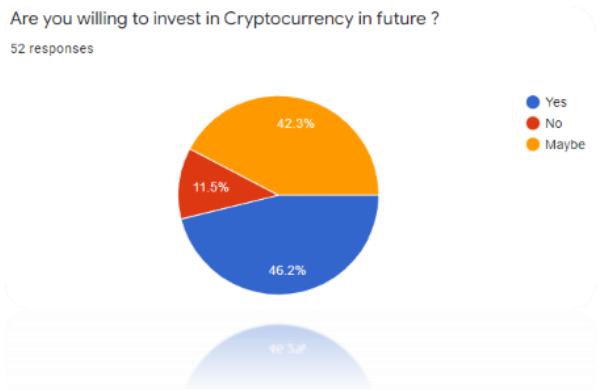

Fig 6 :

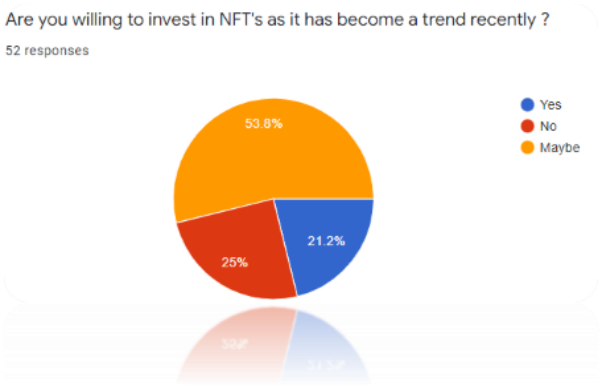

Fig 7 :

These three figures collectively indicate that, even though the awareness rose among the respondents, most of them are unwilling to participate in any of the blockchain transactions related stuff. This is due to India's Finance Minister Nirmala Sitharaman announcing the two major Crypto related announcements for the upcoming financial year. First, the government wants to tax any profits from cryptocurrency transactions at a rate of 30% and charge a source tax of 1% on all transactions (TDS). The second mention of a deadline is that India plans to launch the digital rupee (also known as a CBDC, or central bank digital currency) during the current fiscal year.The announcements' largest source of user misunderstanding is how cryptocurrency may be taxed while being illegal. The government has not made any claims that cryptocurrencies are legitimate. First, the government wants to tax any profits from cryptocurrency transactions at a rate of 30% and charge a source tax of 1% on all transactions (TDS). Tax analysts, attorneys, and executives from cryptocurrency exchanges worry that the TDS will drain market liquidity by requiring high-frequency traders to drastically reduce their activity.

Conclusion

From the survey conducted, it is clearly visible that many respondents are aware about the blockchain and its related technologies. But even though they are aware, the chances of them switching jobs to this field is very less. Many various factors contribute to the result we got. This situation might change in the future as there will be a huge rise in the number of companies adapting to blockchain technology.

References

[1] IBM What is blockchain technology? https://www.ibm.com/in-en/topics/what-is-blockhain#:~:text=Blockchain%20defined%3A%20Blockchain%20is%20a,patents%2C%20copyrights%2C%20branding

[2] 'State of blockchain q1 2016: Blockchain funding overtakesBitcoin' (2016)[Online] http://www.coindesk.com/state-of-blockchain-q1-2016

[3] A. Chapelle,G. W. Peters and E. Panayi Trends in crypto-currenciesand blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2646618

[4] Mrs. Bharati M. Ramageri, Dr. Maithili V. Arjunwadkar (2020) Applications of Blockchain Technology in Various Sectors https://www.researchgate.net/publication/354652587_Applications_of_Blockchain_Technology_in_Various_SectorsA_Review

[5] A timeline and history of Blockchain. https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

[6] Blockchain as a Service solutions https://www.trustradius.com/blockchain-as-a-service-baas

[7] What Is DeFi? Understanding Decentralized Finance https://www.forbes.com/advisor/investing/cryptocurrency/defi-decentralized-finance/#:~:text=Decentralized%20finance%2C%20also%20known%20as,technology%20to%20manage%20financial%20transactions.

[8] What is NFT? How do NFT's work ? https://www.forbes.com/advisor/in/investing/what-is-an-nft-how-do-nfts-work/

[9] Shafaq Naheed Khan, Faiza Loukil (2021) Blockchain smart contracts: Applications, challenges, and future trends https://link.springer.com/article/10.1007/s12083-021-01127-0#:~:text=Smart%20contracts%20are%20executable%20codes,paper%20contracts%20into%20digital%20contracts

[10] Mike Orcutt, (2022) 'Ethereum's smart contracts are full of holes'

https://www.technologyreview.com/2018/03/01/144962/ethereums-smart-contracts-are-full-of-holes/

[11] Nathan Relief, Erika Rasure (2021) 'What Was the Decentralized Autonomous Organization (DAO)' https://www.investopedia.com/tech/what-dao/

Other References

Amiangshu Bosu, Anindya Iqbal, Rifat Shahriyar & Partha Chakraborty (2019)Understanding the motivations, challenges and needs of Blockchain software developers https://link.springer.com/article/10.1007/s10664-019-09708-7 Bandara, I.B., Ioras, F., Arraiza, M.P.: The emerging trend of blockchain for validating degree apprenticeship certification in cybersecurity education (2018)

Gadnis, A., and K. Cronen. 2017. "Unchaining Modern-Day Slavery: Blockchain Offers a Real Solution." January 24. http://blog.chemonics.com/unchaining-modern-day-slavery%3A-blockchain-offers-a-real-solution. [Google Scholar]

Barber S., X. Boyen, E. Shi, and E. Uzun. 2012. "Bitter to Better – How to Make Bitcoin a Better Currency." In Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science, edited by A. D. Keromytis, 7397. Berlin: Springer. https://link.springer.com/chapter/10.1007/978-3-642-32946-3_29#cities. [Crossref], [Google Scholar]

Blockchain Daily News. 2017. "Top 250 Blockchain Companies & Startups." July 6. http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html. [Google Scholar]

Cummings, D. 2016. "Use Cases of Ethereum in Different Sectors 2016." December 15. https://www.ethnews.com/use-cases-of-ethereum-in-different-sectors-2016. [Google Scholar]

Huckle, S., R. Bhattacharya, M. White, and N. Beloff. 2016. "Internet of Things, Blockchain and Shared Economy Applications." http://www.sciencedirect.com/science/article/pii/S1877050916322190. [Google Scholar]

Abran A, Moore JW, Bourque P, Dupuis R, Tripp L (2004) Software engineering body of knowledge. IEEE Computer Society, Angela Burgess