Blockchain: Reason behind Cryptocurrencies

Mukul Nair[1]**, Shobha Tyagi**[2]

[1]Faculty of Engineering and Technology, Manav Rachna International Institute of Research and Studies, Faridabad, India
mukul02nair[at]gmail.com

[2]Faculty of Engineering and Technology, Manav Rachna International Institute of Research and Studies, Faridabad, India
shobhatyagi.fet[at]mriu.edu.in

Abstract: ***Blockchain technology has the potential to significantly alter our corporate environment and will be extremely influential over the coming few decades. It has the potential to alter our economic structure and the way we view corporate processes. Blockchain is a decentralized and distributed ledger system that aims to assure transparency, data security, and integrity because it cannot be changed or manipulated. Only a small portion of current research on blockchain technology is geared toward examining its use in contexts or industries other than cryptocurrencies like Bitcoin. The majority of current research on blockchain technology is concentrated on its use in cryptocurrencies like Bitcoin. Blockchain technology is more than simply bitcoin; it has a number of uses in business process management, government, banking, and finance. As a result, this study makes an effort to look into and examine the opportunities and difficulties associated with current and potential Blockchain Technology implementations. As a result, a sizable number of published papers were thoroughly examined and studied in light of their contributions to the field of Blockchain research.***

Keywords: Blockchain, pier to pier connection, cryptocurrency

1. Introduction

Developed and disseminated among participating parties, a blockchain is a distributed database of records or public records of all activities or digital events. The consensus of the vast majority of users of the system confirms each transaction in the public ledger. Additionally, data cannot be erased once it has been entered. Every transaction made is detailed and confirmed in the blockchain. A well-known model that uses blockchain technology is bitcoin. Also very contentious since it contributes to the emergence of a worldwide market with unregulated, anonymous transactions worth billions of dollars. As a result, it must deal with a variety of regulatory regulation difficulties affecting many national governments and financial organizations. However, blockchain technology has proven to be unquestionably reliable over time and is currently being employed in both financial and non-financial sector applications with success. The most significant invention to come out of the internet itself, according to blockchain, was penned by Silicon Valley tycoon Marc Andreessen last year [3].

The blockchain for bitcoin, a digitally enabled pier to pier connecting software with an operational cost that should be viewed as an invention similar to steam or a combustible engine, according to Johann Palychata of BNP Paribas, who wrote in Quintessence magazine. The foundation of the present digital economy is confidence in a reliable source. All things online What you do depends on your ability to believe someone when they say something is true. For example, an email service provider may confirm that an email was delivered, a certificate authority may confirm the legitimacy of a particular digital certificate, a social networking site such as Facebook may confirm that the information, we post about private life events is shared only with our friends, or a bank may confirm that money belonged to us and was faithfully distributed. The truth is that we rely on a third party to protect our digital security and privacy property, leading a reckless life in the digital world. The truth is that these resources from outside businesses are vulnerable to exploitation, compromise, and exploitation. Blockchain technology is useful in this situation. It has the potential to completely change the way that digital is used in the world by enabling distributed consensus, which makes it possible for all transactions—past and present—to be guaranteed at any point in time. It does this from the outside, endangering the confidentiality of the linked companies' digital assets. Anonymity and shared consent are two crucial components of blockchain technology.

Control issues and technological difficulties are outweighed by the advantages of blockchain technology. "Smart contracts" are a crucial component of the blockchain technology use case. There are smart contracts, which are essentially computer programmers' that can carry out contract conditions automatically. The parties to the contract can make payments automatically in accordance with the terms of the contract when a condition specified in a smart contract between the involved entities is satisfied. Another related idea is smart property, which involves utilizing smart contracts on the blockchain to manage asset ownership. Property can be either tangible—such as a car, house, smartphone, etc. —or intangible—such as stock in a company. The fact that even Bitcoin isn't technically a payment method should be made clear; rather, it's a way to manage who owns what [8].

1.1 Application of Blockchain

Banks and financial organizations no longer perceive blockchain technology as a threat to established business strategies. In fact, by investigating new blockchain programs, the biggest banks in the world are looking for chances in this field. According to Rain Lohmus of the Estonian bank LHV, who spoke about this in a recent interview, blockchain technology has been thoroughly vetted and is secure for use in a variety of banking and finance-related applications. There are countless potential for non-financial applications as well. We can envision evidence of

Licensed Under Creative Commons Attribution CC BY

his presence for all official documents, medical records, and loyalty payments in the music industry, as well as notary, confidentiality securities, and marriage licenses in the blockchain. The goal of privacy or anonymity can be accomplished by retaining digital asset fingerprints rather than the actual digital asset [9].

In this paper, we concentrate on completely disrupting an industry in the current digital economy. As a result of blockchain technology's introduction. As we increasingly use the internet for digital trade and share our personal data with health events, blockchain technology has the potential to be a new motor for the growth of the digital economy. This area offers fantastic potential, and transformation has already started. Ku In the Notary, Insurance, private securities, and a few other non-financial applications, this paper focuses on a few major Blockchain technology applications. We begin by describing a specific history and technology in the beginning.

1.2 Introduction to Cryptocurrency

The viability of our modern economy depends on the use of digital payment systems. For e-commerce, employing digital tokens for trade is essential. A string of bits serves as the fundamental unit of trade in a system of digital money. These bits may be readily duplicated and used for payment, just like any other digital record, which is a problem. The so-called "double-spending conundrum" is essentially the capability of creating a digital token twice. The majority of the time, this issue has been handled by entrusting a reliable third party to keep track of all transactions in a central ledger and transfer balances by crediting and debiting the accounts of buyers and sellers. Digital currency's value is derived from customer trust in a third party to prevent duplicate spending. The real digital money is usually issued by this third party; PayPal is one well-known example. A trustworthy third party is not necessary when using cryptocurrencies like Bitcoin [6].

Instead, they rely on a decentralised network of validators to keep copies of the ledger updated. To ensure that users get and retain control of their balances, validators must come to agreement on the veracity of the transaction record. For such a consensus to emerge, users must have confidence that the validators would update the ledger honestly and refrain from double-spending. It takes the formation of such a consensus, double-spending. How do virtual currencies like Bitcoin address these issues? A blockchain, which guarantees distributed verification, updating, and maintenance of the record of transaction histories, serves as the foundation for confidence in the currency. A blockchain is developed for this. A block is an aggregation of bitcoin user transactions. These blocks are connected to build a chain that records the previous transactions in order to establish a public ledger where the balance or cash that a user holds can be verified. Consequently, a blockchain acts as a log of all past transactions, with each block acting as a new page that records all current events. [7].

1.3 History of Cryptocurrency

American artist David Chaum discovered e-cash, a form of anonymous encrypted electronic money, in 1983. He then used it for Digicash, the first cryptographic electronic payment system, which required user software to extract bank notes and define particular names, keys pushed before being given to the destination. This was in 1995. As a result, tracking digital money is now possible for the issuing bank, the government, or any foreign firm. How to Make a Mint: the Cryptography of Anonymous Electronic Cash, a 1996 National Security Agency study that was later published in the American Law Review in 1997, was the first to provide a description of the cryptocurrency initiative. [1].

The definition of "b-money, " which seems to be an anonymous electronic money distribution system, was released by Wei Dai in 1998. Nick Szabo quickly described a modest quantity of gold. Small gold was characterized as an electronic currency system that required users to complete proof of performance and covertly incorporated solutions, similar to bitcoin and other cryptocurrencies that would follow. and was written.

Bitcoin, the first cryptocurrency, was created in 2009 by an unknown programmer named Satoshi Nakamoto. In its proof of function, it made use of the cryptographic hash function SHA-256. In an effort to establish a different DNS in April 2011, Namecoin was developed to make online research more challenging. Litecoin was launched soon after, in October 2011. Instead than using SHA-256 as its hash function, it has adopted scrypt. Peercoin, another well-known cryptocurrency, combined performance and stack proof evidence.

On August 6, 2014, the UK declared that its Treasurer has ordered a research on cryptocurrencies to determine whether or not they may have any economic impact there. If regulation should be taken into consideration, the study should also document that. In January 2021, it began a consultation on cryptoassets and stablecoins after publishing its final report in 2018. El Salvador became the first nation to recognize Bitcoin as legal tender in June 2021 when the Legislature approved a bill to split cryptocurrencies in half by a 62-22 vote. Cuba implemented Resolution 215 in August 2021 to categorize and control cryptocurrencies like bitcoin. The Chinese government, one of the biggest markets for cryptocurrencies, declared all cryptocurrency transactions to be unlawful in September 2021, putting

1.4 Technical Overview

A system that uses encryption to enable the secure transfer and exchange of digital tokens in a dispersed and segregated region is known as a cryptocurrency. At market rates for fiat currency, these tokens can be sold. In January 2009, Bitcoin, the first cryptocurrency, began trading. Since then, a large number of additional cryptocurrencies have been developed using the same novel techniques introduced by Bitcoin, however some of their unique features that govern algorithms have changed. The double-spending challenge and the Byzantine Generals Problem, two long-term solutions problems in computer science, were made possible by two fantastic new techniques that Bitcoin brought.

Licensed Under Creative Commons Attribution CC BY

1.5 Double Spending Problem

Prior to the creation of Bitcoin, two parties could not conduct an electronic transaction without engaging the services of a reliable third party consultant. The difficulty, which computer scientists refer to as the "double-digit problem, " has been a barrier to attempts to commercialize electricity since the invention of the internet. First, think about how the financial transaction functions to gain an understanding of the issue. The currency manager can give it to someone else, who can then check his hands to make sure you are the only one in possession of that note. For instance, if Alice hands Bob a $100 cash, Bob keeps it but Alice loses it. Bob can easily attest to having a $100 bill in his possession, and Alice, in all honesty, is unlikely to still have it. The actual transfer of funds is similarly final in the sense that the new management simply returns the currency note after a deferred action. In our situation, Bob will need to give Alice $100 back. Money enables various organizations, including strangers, to act independently without trust by providing all these assets.

Consider how electronic currency might operate right now. It goes without saying that paper notes could accomplish this. There will need to be some sort of digital currency. In reality, we might think about a $100 computer file in place of the $100 cash. Before sending Bob a message again, Alice includes a $100 file in the message when she wants to pay him $100. Anyone who has ever sent an email attachment knows that doing so does not remove the file from the recipient's computer. Bob will be able to utilize the same $ 100 each second, third, or fourth since Alice will preserve a flawless copy of the $100 digital copy he supplied to Bob. Bob has no method of verifying Alice's word, even if she makes a pledge to him to destroy the file when he gets a copy.

Up until recently, the only solution to the double-spending issue was to hire a dependable outside expert. In our case, Alice and Bob can both do it since they each have an account with a third party they trust, like PayPal. Reliable websites preserve a record of all account balances and activity, such as PayPal. When Alice informs PayPal she wants to pay Bob $100, PayPal takes the money out of his account and adds it to Bob's. There is almost no work. Bob relies on PayPal to confirm that Alice cannot afford the same $100, and Bob uses PayPal to validate this. All transactions between all accounts eventually converge to zero. However, keep in mind that, unlike money, activities include a third party arbitrator and, as we've already mentioned, transactions can be delayed by a third party.

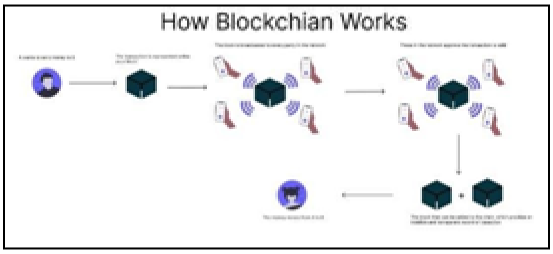
A dual solution to the issue was announced by Satoshi Nakamoto (a pseudonym) in 2008. the issue of spending money without engaging contractors (Nakamoto, 2008). In actuality, his company, Bitcoin, uses digital money. enables the final transfer for the first time of digital assets—not just a copy—in a method that can be guaranteed by outside users who have faith in other teams. Peer-to-peer networking, public key cryptography, and a job-proofing mechanism are used to achieve this. Similar to PayPal, the Bitcoin system uses a block chain, a decentralized ledger that keeps track of transactions. In the Bitcoin economy, every transaction is tracked and added to the block chain. The PayPal ledger is maintained by an intermediate authority, while the block chain is not. Instead, a peer-to-peer public record called the block chain is shared by a large number of nodes in the Bitcoin network. To make sure that bitcoins are the same and have never been used before, new transactions are compared to the blockchain, but no reliable third party performs the work of verifying new transactions. Instead, the task of reconciling and maintaining the block chain book is divided among thousands of users who volunteer their computing abilities. In actuality, a devoted third party serves as the hub for the entire peer-to-peer network.

1.6 Blockchain Architecture

Peer-to-peer (P2P) network design, encryption techniques, distributed ledger technology (DLT), and decentralised data storage are the four key components of blockchain technology (Singh & Singh, 2016). The Internet of Things (IoT), distributed storage, virtual reality (VR), and artificial intelligence (AI) may also be included (IoT). However, file operations, databases, and data storage are the only things that are included in the current definition of blockchain technology. The protocol layer, extension layer, and application layer, respectively, finish up the tasks of data verification, data dissemination, and data representation at the base of the blockchain from the standpoint of architecture design. [11].

The storage and network layers combine to form the protocol layer, which provides network programming, distributed algorithms, encryption signatures, and data storage. A mechanism for accessing and storing data on the blockchain may fully eliminate any dependence on a centralised repository. While the file metadata is kept on the blockchain, the files themselves are saved off-chain using distributed hash tables (DHTs) dispersed over various sites utilising a peer-to-peer network.

Developers have built languages that contain domain-specific script codes in response to the particular challenges of blockchain programming. Blockchain platforms like Ethereum, which permit transactions between untrusted parties on a decentralised computer network, are built on top of these languages.



The consensus and distributed algorithm are essential for sustaining the blockchain's effectiveness and safety. Business logic underlies this concept because it can significantly reduce the size of hardware circuits, make pipeline processing simple to construct, and speed up circuit execution. Blockchain applications in the financial sector may function much better when the proper algorithm is used. Nonrepudiation is another crucial aspect of information

Licensed Under Creative Commons Attribution CC BY

security in blockchains, in addition to decentralised ledgers and high security. An effective nonrepudiation method is a digitally encrypted signature system, which is a crucial component of the bank risk mitigation framework.

The consensus and distributed algorithm are essential for sustaining the blockchain's effectiveness and safety. Business logic underlies this concept because it can significantly reduce the size of hardware circuits, make pipeline processing simple to construct, and speed up circuit execution. Blockchain applications in the financial sector may function much better when the proper algorithm is used. Nonrepudiation is another crucial aspect of information security in blockchains, in addition to decentralised ledgers and high security. An effective nonrepudiation method is a digitally encrypted signature system, which is a crucial component of the bank risk mitigation framework.

The extension layer is in charge of creating the actual applications that use blockchain technology to promote social and economic progress. It is divided into two sections according to various product lines. The first is intelligence technology, which is a crucial conduit for both fiat and crypto currencies and helps with business transactions in a variety of trading markets, including smart contracts and tokens. The second is used to process literal data formats like written text, images, digital books, and videos.

In order to modernise the financial system and raise the standard and efficiency of financial operations, the application layer creates new financial formats or service models. Through e-wallets, transaction URLs, substantial financial APIs, and the blending of online and offline channels, blockchain technology improves the financial environment. By effectively addressing issues with traditional financial risk, such as information asymmetry, the ecosystem and financial service system built on blockchain applications can fully capitalise on the demands of potential customers.

1.7 Types of Blockchain

Mainly there are 2 types of blockchain; Public and Private blockchain. But there are many variations too like consortium and Hybrid blockchain [2].

a) Public Blockchain

A public blockchain is a distributed ledger system that is free from restrictions and permissions. To join a blockchain network and become an approved site, anyone with internet connection can log in to the blockchain. A node or user that uses a public blockchain may access both recent and historical data, verify transactions or show incoming blockchain activity, and mine. the most basic technique for mining and trading bitcoins on public blockchains. As a result, Bitcoin and Litecoin blockchains are the most widely used social blockchains. Users that properly adhere to security guidelines and protocols will make social blockchains far safer. But only if the players disobey the safety agreements will it be dangerous.
Example:-Bitcoin, Ethereum and Litecoin.

b) Private Blockchain

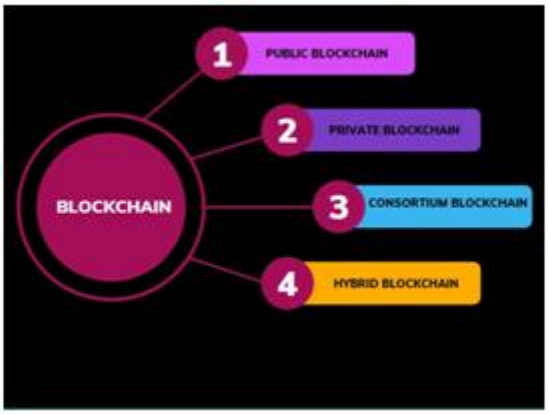
The only restricted or approved blockchain resource on a closed network is private blockchain. In blockchain networks for voting, supply chain management, digital identity, asset ownership, etc., where only chosen individuals are members of the blockchain network, private blockchains are frequently employed. The governing body controls the level of security, authorization, permits, and access. Since they have a more restricted and secure network, private blockchains are used similarly to public blockchains.

c) Consortium Blockchain

A network of blockchains is owned by many organizations in a minimally separated form known as a consortium blockchain. Compare this to what we've seen in the privately owned, single-company-controlled private blockchain. Multiple organizations may act as nodes in this form of blockchain, sharing data or setting up mines. In addition to other organizations, banks and governments regularly employ consortium blockchains.

d) Hybrid Blockchain

A hybrid blockchain combines public and private blockchain. It makes advantage of both sorts of blockchains' capabilities, allowing one to create a private system based on a license that operates without the knowledge of the general public. Users can manage who has access to what data stored on the blockchain thanks to the network's complexity. Only a small fraction of the data or records from the blockchain may be authorized to become public in order to preserve the privacy of the private network. Users can quickly combine a private blockchain with a number of social blockchains thanks to the flexibility of the blockchain hybrid architecture. A private hybrid blockchain network typically verifies what occurs there. Users may, however, download it to the open blockchain for validation. Social blockchains improve hashing and include more authentication nodes. As a result, the blockchain network's security and transparency are enhanced.



1.8 Advantage of Blockchain

- One of the major benefits of blockchain distribution is that it makes it possible to distribute databases decentralized. Unlike a traditional database, the segregation of data on a blockchain makes it nearly difficult to mute data
- Users can control how their transactions and information

are handled.

- Blockchains provide complete, dependable, and up-to-date data without accuracy.
- Because of its dispersed network, the blockchain can withstand any security threats because it lacks a single point of failure.
- Interacting with Blockchain peers peer-to-peer enables the detection of distributed consensus and network fraud. A network can only be affected if the attacker gains 51% control of the nodes, making network attacks very hard.
- Interacting with Blockchain peers peer-to-peer enables the detection of distributed consensus and network fraud. A network can only be affected if the attacker gains 51% control of the nodes, making network attacks very hard [4].

1.9 Disadvantage of Blockchain

- Blockchains are expensive and resource-intensive since each node in a blockchain must repeat a procedure in order to reach agreement.
- Users of blockchains can utilize certification authentication, global titles, hidden funds, etc. to authenticate transactions. Even if both parties agree to postpone the transaction or if the contract fails for some other reason, it cannot be done. A blockchain operation is only completed when all of the network's nodes correctly verify it. As the installation block needs to be authenticated in order to mark the action as true for all nodes, this procedure could take a very long time. This issue might be well-solved by a novel idea termed a lighting network, where performance can be promptly guaranteed [10].

2. Possible Future Directions

a) Blockchain testing

Currently, [52] lists over 700 coins, and new blockchain kinds are only now starting to emerge. To attract investors lured by the prospect of massive rewards, some developers, however, may misrepresent their blockchain performance. Customers that want to use blockchain in their companies also need to know which blockchains are best for them. A framework for blockchain testing must exist in order to test several blockchains.

Blockchain testing and standardization might be divided into two parts. During the standardization process, all criteria must be developed and authorized. When a blockchain is produced, it may be compared to the pre-established criteria to see if it actually performs as well as its designers claim. When doing blockchain testing, specific criteria must be used in terms of the testing procedure. For instance, a user in charge of online shopping cares about the throughput of the blockchain, thus the analysis must include many parameters such as the size of a blockchain block, the average time it takes from the user making a transaction to the transaction being packed into the blockchain.

b) Big data analysis

Blockchain and big data may complement each other well. Data management and data analytics are the broad areas into which the combination has been separated in this case. In terms of data management, as blockchain is secure and decentralized, it might be used to store important data. Blockchain may also ensure the data's uniqueness. If patient health data is maintained on a blockchain, for example, the data cannot be modified, making it difficult to steal such confidential details. Big data analytics may be used to analyse data and be used to blockchain transactions. User trading patterns, for instance, may be accessed. Using the study, users may predict the trading preferences of possible partners.

c) Blockchain application

While blockchains are currently mostly employed in the financial sector, more and more uses are emerging for other industries. Traditional industries should consider using blockchain in their sectors to improve their current methods. User reputations, for instance, might be kept on a blockchain. The emerging sector might use blockchain to boost efficiency at the same time. For instance, the ridesharing firm Arcade City uses blockchain technology to provide an open marketplace where passengers may deal directly with drivers.

An electronic transaction system that executes a contract's provisions is known as a smart contract. This notion has been discussed for some time, and blockchain technology now has the ability to make it a reality. A blockchain smart contract is a piece of computer code that may be executed instantly by miners. Smart contracts have the potential to change a number of industries, including financial services and the Internet of Things.

d) Law Integration into smart contacts

In addition to cryptocurrencies, blockchain technology offers us another practical option called "smart contracts. " Smart contracts' primary concept is their automatic execution when certain criteria are met. Providing things after money has been received is one example. But contracts should also be automatically regulated with regard to other terms. As a result, AIG Insurance is currently testing a blockchain system that enables the creation of intricate insurance policies.

Additionally, bear in mind that smart contracts are decentralized and not subject to any kind of oversight. What should parties do in the event of a dispute, though? Smart contract participants typically consent to being bound by laws, but what if a dispute arises between parties from different nations? The best way to resolve contractual disputes is still up for debate. As a result, in the near future, smart contracts should incorporate the rule of law to settle any disagreements between the parties.

e) Stop the tendency of centralization

Blockchain is designed to operate independently. In the mining pool, there is a tendency for miners to band together. The top 5 mining pools presently control more than 51% of the network's total hash power. Additionally, arrogant mining methods demonstrated that pools with more than 25% of the total computer capacity might profit above their fair share. The selfish pool may someday easily reach 51% of the total power since it would draw logical miners. Since

Licensed Under Creative Commons Attribution CC BY

the blockchain cannot be used to only benefit a select few businesses, this issue must be resolved.

3. Conclusion

In conclusion, the foundation of Bitcoin technology is Blockchain. Given its distributed functionality and the security of Blockchain, the ladder is a very alluring technique for resolving contemporary financial and non-financial issues.

Blockchain-based business applications are very popular, thus many startups are working on them. Adoption is undoubtedly difficult, as was already mentioned. Major financial institutions are investing in evaluating the usage of current business models in blockchain, including Visa, Mastercard, banks, NASDAQ, and others. In fact, a few of them are exploring new business opportunities in the blockchain industry. Some people might choose to use Blockchain's modified controls to keep ahead of the curve.

References

[1] Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works by Muhammad Ashraf FAUZI1, Norazha PAIMAN2, Zarina OTHMAN
[2] Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin by Jaysing Bhosale and Sushil Mavale.
[3] Cryptocurrency: The Economics of Money and Selected Policy Issues by members and committee of congress
[4] Cryptocurrencies: market analysis and perspectives by Giancarlo Giudici, Alistair Milne and Dmitri Vinogradov. .
[5] BlockChain Technology by Berkley university of California.
[6] Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto.
[7] Abadi, J., and M. Brunnermeier.2018. “Blockchain Economics”. Princeton University.
[8] Abraham, I., D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman.2016. “Solidus: An incentive-compatible cryptocurrency based on permissionless Byzantine consensus. ”
[9] Almosova, A.2018. “A Monetary Model of Blockchain. ”
[10] Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems
[11] https://en. wikipedia. org/wiki/Cryptocurrency#History
[12] https://www. researchgate. net/publication/336130918_Understanding_Blockchain_Technology

Licensed Under Creative Commons Attribution CC BY