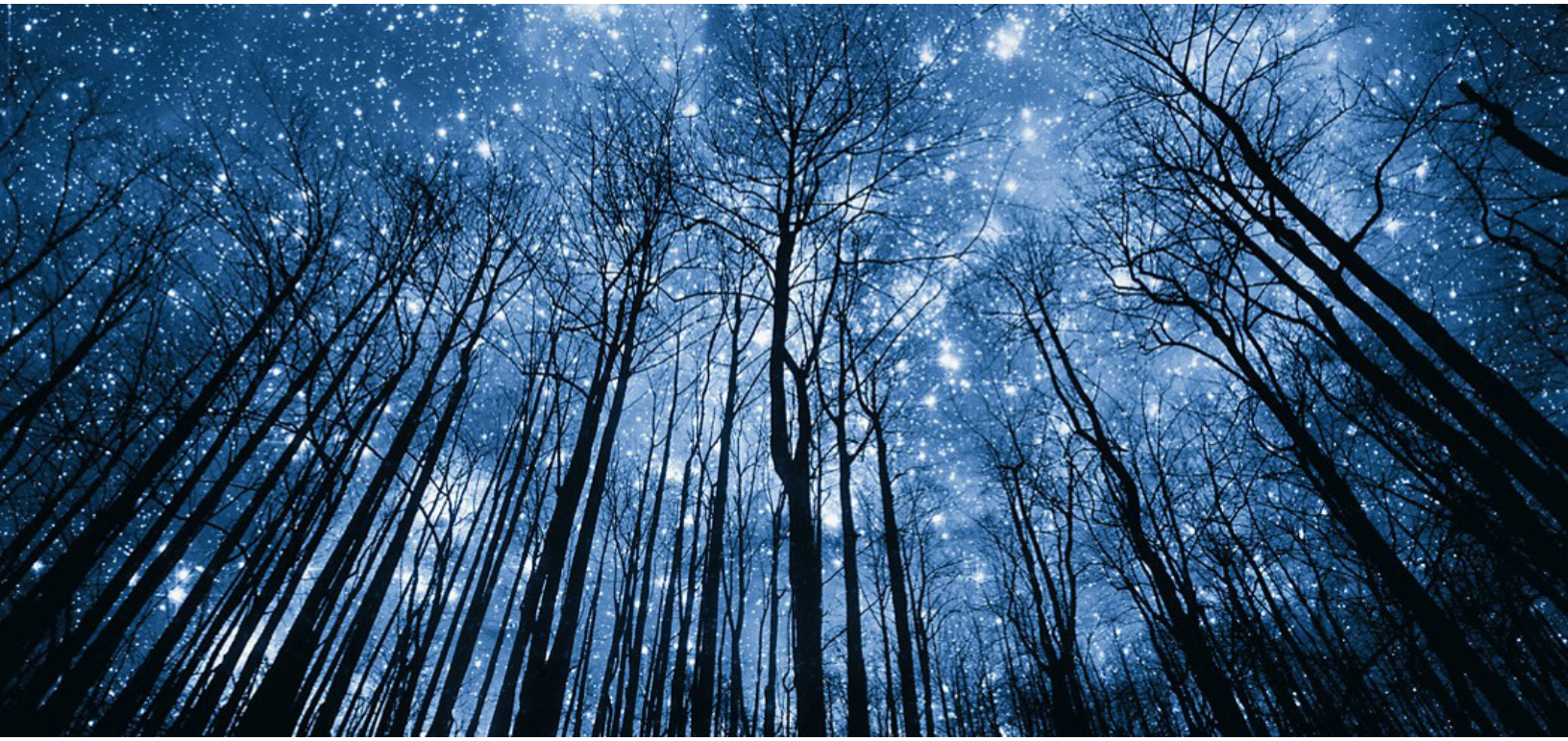
DELL Technologies

BLOCKCHAIN REVOLUTIONIZING CURRENCY



Janani Pokkuluri
Specialist 2, Inside Product
Dell Technologies

Vagdevi Kaligotla

DELL Technologies
Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across Dell's multiple technologies and products with both skill and outcome-based certifications.

Proven Professional exams cover concepts and principles which enable professionals working in or looking to begin a career in IT. With training and certifications aligned to the rapidly changing IT landscape, learners can take full advantage of the essential skills and knowledge required to drive better business performance and foster more productive teams.

Proven Professional certifications include skills and solutions such as:

- Data Protection
- Converged and Hyperconverged Infrastructure
- Cloud and Elastic Cloud
- Networking
- Security
- Servers
- Storage
- …and so much more
-

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Contents

INTRODUCTION

Information and communication technologies has created many opportunities for the fields of financial and business sector. With the increase in the number of online users, the need for new types of trading, transactions and currencies is rising. The necessity for a decentralized currency was previously more of a theoretical idea, but in the last ten years, it has become a reality owing to Satoshi Nakamoto's well-known article from 2008, which introduced Bitcoin and blockchain technology. Although there are multiple controversies about the paper he has written, it is undeniable that this is a revolutionary concept with which users can either develop applications or invest money and trade.

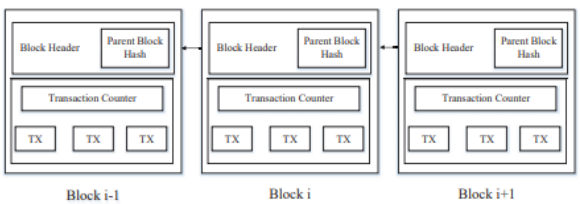
Cryptocurrency is one of the new financial instruments that has developed in recent years. Any form of currency (other than fiat money) that may be utilized in a variety of financial transactions, whether they are virtual or physical, is referred to as cryptocurrency (CC). Utilizable digitally or in a variety of applications and networks, including peer-to-peer networks, online social networks, online social games, and virtual worlds, cryptocurrencies symbolize valuable and immaterial objects. Decentralized control is a feature of cryptocurrencies, making it impossible for a single individual or institution to have authority over them. The idea of digital currency is not new, but it could not be implemented as the approaches either needed a trusted third-party bank or were not able to resolve the double expenditure issue. In a centralized solution, banks or other reliable authorities can stop attempts to issue two transactions in tandem, but in a decentralized system, like a cryptocurrency, this issue is very significant. Additionally, because there is no central authority, users are required to keep the P2P network's state consistent, making it more difficult for potential attackers to compromise the system by providing fake data. Blockchain is the key technology used to establish the Bitcoin network and allows transactions to occur without the involvement of a third party. Four key characteristics of blockchain technology are decentralization, persistence, anonymity, and auditability. These characteristics allow blockchain to significantly reduce costs and increase efficiency.

BLOCKCHAIN TECHNOLOGY

Blockchain technology is a cutting-edge computer protocol that is used to digitally record and store data across many computers, or nodes. A "Ledger," which resembles a relational database, is one of the most crucial components of blockchain Walport (2016). Known as a block, a blockchain is a collection of encrypted digital records or transactions. Using a cryptographic signature, each block is then chained to the one behind it in a straight line and chronological order. Each block has a copy of the most recent transactions since the previous block was added. This eliminates the need for a third party by connecting the shared block, or ledger, to every user of a network of computers to check or confirm transactions.

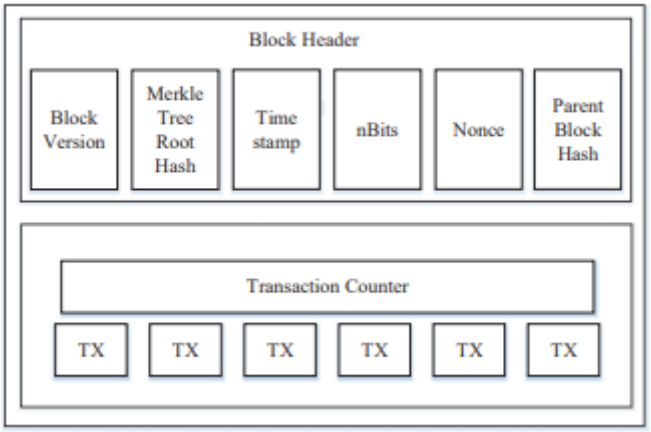
Blockchain is used in a novel and distinctive way to distribute and safeguard data. Direct transactions between non-intermediaries or intermediary services are assumed to take over because of the disappearance of a central instance in the dispersed network. Thus, a transaction can never be changed or destroyed in Blockchain, and updates can only be made by system participants coming to a consensus. In contrast to a conventional, centralized database with a user-controlled access mechanism, its distributed database cannot be breached, altered, or otherwise disrupted.

Since the data is immutable, no one, not even a system administrator, is able to edit or remove it from the ledger after it has been entered into a Blockchain. Considering that every data block has a time stamp and is connected chronologically by a cryptographic signature called Walport. Almost any transaction involving value, including those involving money, goods, land ownership, medical information, or even votes, can be made using blockchain technology. There is no single point of failure because Blockchain is a distributed system that is not governed by a single control centre as there might be with system administration. So, in theory, an enterprise would not require an IT specialist to keep an eye on the security of a blockchain database.



BLOCKCHAIN ARCHITECTURE

BLOCK:



A block consists of a block header and body of which a block header includes:

i. Block version
ii. Merkle tree root hash
iii. Timestamp
iv. nBits
v. Nonce
vi. Parent block hash

A transaction counter and transactions make up the block body. Depending on the block size and the size of each transaction, a block can contain a maximum number of transactions. Blockchain verifies the authenticity of transactions via an asymmetric cryptography technique.

Asymmetric cryptography-based digital signatures are utilized in an unreliable setting.

DIGITAL SIGNATURES:

Each user is in possession of a set of private and public keys. The transactions are signed using a private key that must be kept secret. The transactions that have been digitally signed are broadcast across the entire network. The two steps of a typical digital signature are the

signing phase, and the verification phase are broadcast across the entire network. The two steps of a typical digital signature are the signing phase and the verification phase.

For example:

User A wants to communicate with user B.

(1) A uses her private key to encrypt the data she wants to sign, then she gives B both the encrypted data and the original data.

(2) B verifies the value with A public key during the verification stage. B may then quickly determine if the data has been altered or not.

The elliptic curve digital signature technique is the common digital signature algorithm used in blockchains.

CHARACTERISTICS OF BLOCKCHAIN:

DECENTRALIZATION:

Theoretically, blockchain does not depend on any centralized node or authority, enabling distributed data recording, storing, and updating. Some blockchains do, however, centralize to some extent. No centralized authority or entity (other than Bitcoin) has more power than the others in the case of a public, permissionless blockchain, and everyone has the right to validate a transaction.

Only a small number of nodes (PoS and DPoS-based ones like EOS) are given specific privileges over validation in the event of a consortium, permissioned blockchain. A blockchain that is completely private has a centralized organization with the authority to make decisions and manage the validation procedure.

PERSISTENCY:

Transactions can be verified fast, and sincere miners would not accept any invalid transactions. Once a transaction is added to the blockchain, it is very difficult to remove it or roll it back. Blocks with invalid transactions could be found right away.

ANONYMITY:

With a randomly created address, each user can communicate with the blockchain without disclosing their true identity. Be mindful that due to an inherent constraint, blockchain cannot completely ensure the preservation of privacy.

AUDITABILITY:

Based on the Unspent Transaction Output (UTXO) architecture, the blockchain for Bitcoin retains information on user balances. Every transaction must refer to some earlier unpaid transactions. The status of those referred to unspent transactions changes from unspent to spent once the current transaction is added to the blockchain. Therefore, it would be simple to verify and follow transactions.

TYPES OF BLOCKCHAIN:

PUBLIC BLOCKCHAIN

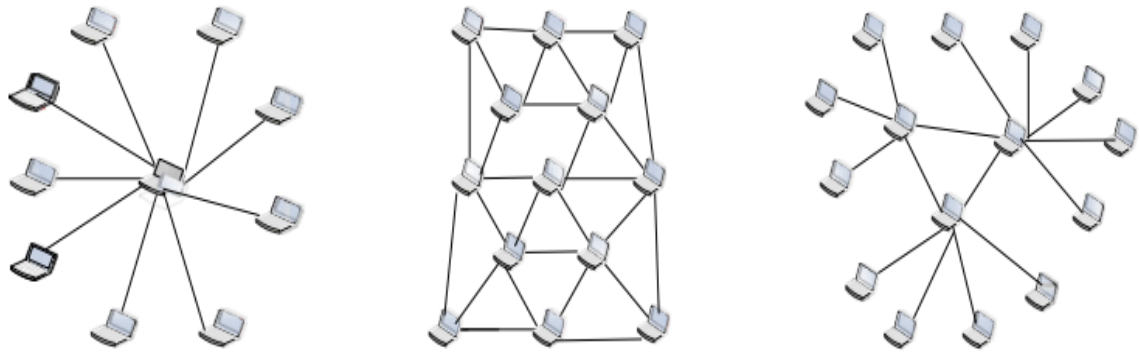
On the network, transactions that are transparent and anonymous can be made by anyone. A public blockchain is totally decentralized, like bitcoin. There is no single point of failure in the system, which relies on user consensus to function. Public Blockchain is susceptible to system intrusions, nevertheless. Without the participants' knowledge, an attacker may, for example, replicate and properly link all the modified blocks.

PRIVATE BLOCKCHAIN

The members are known, but the transactions are private, and the data is not accessible to the general public. In a private Blockchain network, a participant cannot read or write the Blockchain unless the participant has a permission or an invitation to join the network. Large businesses typically employ private blockchains with permissions set amongst different corporate blockchain stakeholders. For instance, a bank can have its own Blockchain network for internal usage, with access to its many stakeholders—including clients, staff members, and suppliers—restricted.

CONSORTIUM BLOCKCHAIN

It uses both a public and a private blockchain in a hybrid fashion. By selecting this architecture, businesses or organizations can create their own Private Blockchain network to distribute data among consortium members (such as banks, institutions and other enterprises or firms).



Public Blockchain Consortium Blockchain Private Blockchain

SWOT ANALYSIS OF CRYPTOCURRENCY (BITCOIN)

STRENGTHS:

More specifically, the set number of bitcoin that will ever exist, bitcoin has strength by design to make it a viable currency that has increased it in status over the years. Every four years, bitcoin will be mined with decreasing returns to reach its maximum supply of twenty-one million coins. The value of Bitcoin depends on this feature. It will not ever get inflated from an overabundance of bitcoins because there are only a finite number of them. Additionally, bitcoin and other cryptocurrencies are typically seen as being shielded from inflation brought on by changes to or limits imposed by national governments. As a result, investors have a "safe haven" to invest their money because it often does not depreciate due to inflation.

WEAKNESS:

Numerous internal flaws in Bitcoin are inherent to its design and are therefore difficult to fix. Every user may view every transaction thanks to the public ledger, also known as the block chain. Although there is a degree of anonymity because bitcoin wallet owners cannot be directly traced, some potential adopters find it unsettling. Since everyone may view the public block chain, it is vulnerable to attacks because of the ease of access (King, 2013). The Bitcoin network has already experienced a number of "stress tests" that were simply DDoS assaults (Hileman, 2016). Exchanges and miners conducted these “tests” to demonstrate a design flaw in Bitcoin: the network's inability to support huge transaction volumes. An unpleasant design choice in the code is the ability for Bitcoin users to just shut down the network to demonstrate their point. These two features are fundamental to how Bitcoin works and cannot be modified. Reluctant users must adopt despite these characteristics. These scenarios bring the reputation of bitcoin online.

OPPORTUNITIES:

Businesses are starting to recognize the benefits of adopting cryptocurrencies for cross-border exchanges, particularly when transactions must be completed swiftly in response to an emergency. Due to the speed and simplicity of transactions in the peer-to-peer system, cryptocurrencies are uniquely positioned to address this issue. Cryptocurrencies might end up dominating the market for commodities. They have the distinctive quality of being bought directly online, which makes it simple for customers to enter the market. Bitcoin will acquire credibility among investors and move closer to becoming more widespread if it remains a viable haven for devaluing currencies.

THREATS:

For Bitcoin to gain widespread user adoption, it must first overcome a number of obstacles. Users and investors are sceptical of cryptocurrencies due of their value swings. The general adoption of cryptocurrencies is ultimately a limiting factor. The problems with investors are also a result of this lack of trust. The number of dead companies has risen to twenty-four, with the majority claiming "security" as the primary cause of closure. Future investors might

use this metric as a benchmark when deciding whether to buy bitcoin. Along with the trust issue, there are other cryptocurrency rivals working to offer a substitute for the virtual currency.

STEPS TO CREATE YOUR OWN CRYPTO CHAIN:

DETERMINE THE PURPOSE:

The obvious but crucial first step in developing a cryptocurrency is: A convincing purpose for the proposed digital currency must be identified by developers (the phrase used to describe cryptocurrency producers). Both conventional currency and cryptocurrencies have a variety of uses like data verification, smart contract support, transfer of money etc.

SELECT A BLOCKCHAIN PLATFORM:

A blockchain platform serves as the foundation of all cryptocurrencies. As a result, a system of accountability is established, and every transaction is guaranteed to be documented and spread over the blockchain. Some transactions might be fraudulent for which you need a screening process. Ethereum, EOS, NEM etc are a few blockchain platforms.

PREPARE THE NODES:

The nodes that make up the blockchain must be created after you have chosen a blockchain. Nodes are often quick computers that join a blockchain network to process and validate transactions. Nodes record and share data that is eventually added to the digital ledger while maintaining the currency.

CHOOSE A BLOCKCHAIN ARCHITECTURE:

Centralized, decentralized, and distributed are the different types of architecture formats of blockchain. Blockchains do not all function in the same manner when it comes to sharing data. Like conventional architecture, digital architecture must consider both design and how everything fits together to function as efficiently as possible.

ESTABLISH APIs:

An interface connecting to a client network or a blockchain node is known as an application programming interface, or API. For instance, an API can act as an interface between a currency exchange and a program that gathers information about that currency. In the world of cryptocurrencies, APIs can be used for a variety of tasks, but the most frequent ones are currency trading, data security, and currency analysis.

Developers can choose from a variety of blockchain APIs, such as the Ethereum APIs from Bitcore, Factom, and Infura.

CREATE A SUITABLE INTERFACE AND UNDERSTAND THE LEGAL CONSIDERATIONS:

Developers must take the user interface (UI) and user experience (UX) into account if they want to make it simple for others to engage with their coin (UX). Consumers and miners are more likely to be able to simply setup their settings and manage their investments the simpler the UI and UX. Interfaces need a server and database to function, and someone needs to be prepared to create a website or software that enables data configuration and inspection. After this acquire legal permissions from the local governments.

In the end, it takes time and effort to create a proper cryptocurrency that is both reliable and viable. Any developer's chances of success can be made or broken by their access to the technology required to deliver the highest level of security with the most straightforward user interfaces.

RISKS ASSOCIATED WITH CRYPTOCURRENCY:

TECHNOLOGY RISKS:

The term "technology risk," often known as "Information Technology (IT) risk," generally refers to the likelihood that a firm would experience technological shortcomings that could interfere with its capacity to do business as usual, such as cybersecurity incidents, service outages, etc. A restriction of cryptocurrency technology is crypto scalability, which is defined as the quantity of transactions handled by the network.

FRAUD RISK:

Identity theft and fraud are particularly common with bitcoins. A distinction is made here; identity fraud is the use of stolen information to engage in unlawful or unethical activities, while identity theft refers to the theft of cryptotraders' identities, including their personal

information, banking information, and other details. Identity fraud, according to Koops & Leenes (2006), is a more general phrase that includes "identity theft"; it is all about "identity related crime". The fakeness of trading volume is one of the major scandals of identity fraud in the context of cryptocurrencies.

LEGAL RISK:

Cryptocurrencies cannot be categorized as a specific asset class. They mix the qualities of money, goods, payment methods, and security. Additionally, cryptocurrencies come in a variety of forms (coins, tokens, stablecoins, etc.), each of which has a unique legal status. This results in uncertainty on the appropriate regulatory framework to use. Governments across the world are regulating cryptocurrencies differently and using various legal strategies in response to these difficulties. While some countries do not have a defined regulatory policy and others have outright outlawed the use of cryptocurrencies, several have implemented special legislation to control cryptocurrency activity.

ENVIRONMENTAL IMPACT OF MINING CRYPTO:

Climate change is one of Bitcoin's negative effects on the environment. This is because electricity used to create bitcoins was produced in part by coal- and gas-fired power stations. Burning coal and natural gas releases greenhouse gases that warm the planet and alter its climate. According to estimates, such bitcoin mining will account for 0.1% of global greenhouse gas emissions as of 2022. The second environmental impact of coal-fired electricity generation is air pollution, and the third is e-waste because of the short lifespan of bitcoin mining equipment.

By 2021, it is anticipated that the yearly e-waste generated by bitcoin will exceed 30,000 metric tonnes, which is like the Netherlands' waste from small IT equipment. 270–380 grams of electronic waste are produced when one bitcoin is created. According to estimates, the average life expectancy of bitcoin mining equipment is 1.3 years. The employed application-specific integrated circuits are only used for bitcoin mining, unlike most of the computing hardware. It is challenging to lessen bitcoin's environmental impact; potential solutions include producing bitcoin solely in locations or during periods with

sufficient clean electricity. Some legislators have demanded stricter limitations or outright bans on bitcoin mining.

CONCLUSION:

The use of blockchain technology has great potential for addressing issues with data integrity, increasing transparency, enhancing security, reducing fraud, and establish privacy and trust. Blockchain technology has the potential to revolutionize several industries, including finance, accounting, e-government, business process management (BPM), insurance, entertainment, trading platforms, healthcare, the internet of things, law firms, and others.

Because technical innovation and applications can be used to achieve economic efficiency and societal benefits, Blockchain Technology has a significant potential to introduce novel solutions, depending on the field or industry in which it is used.

However, adopting blockchain technology at businesses in several industries could be highly expensive. Organizations must invest a large amount of money in transferring or migrating outdated systems. It is possible that legacy apps or systems will not be quickly replaced by blockchain technology. Blockchain can, however, be used in conjunction with existing systems and, soon, might even inspire the creation of new ones.

With technology developing at a rapid phase, and the environmental impact crypto causing, where is this new technology headed to? One thing all of us know and should believe is that physical cash going extinct is a possibility soon.

REFERENCES:

[1] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1-2016/

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto currencies and blockchain technologies: A monetary theory and regulation perspective,” 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 264661

[4] Ahram, T. et al., (2017). Blockchain technology innovations. 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (Jun. 2017), 137–141.

[5] Angraal, S. et al., (2017). Blockchain Technology: Applications in Health Care. Circulation. Cardiovascular quality and outcomes. 10, 9 (Sep. 2017), e003800. DOI: https://doi.org/10.1161/CIRCOUTCOMES.117.003800.

[6] Aru I., (2017). Full Stack Development Tools Lowering Blockchain Entry... News Cointelegraph. Available at: https://cointelegraph.com/news/fullstack-development-tools-lowering-blockchain-entry-barriers.

[7] Bahga, A., Madisetti, V., (2016). Blockchain Platform for Industrial Internet of Things, Journal of Software Engineering and Applications, No. 9, pp. 533-546