Journal of Positive School Psychology http://journalppw.com
2023, Vol. 7, No. 1, 1798-1819

Use Of Digital And Virtual Currency. (Review In The Context Of Islamic Sharia)

Sana Ur Rehman[1] , Dr. Salman Ahmad Khan[2] ,Ms.Aneeba Basharat[3] ,Hafiz Wahaib ur Rehman Naeem[4] , Hafiz Hussnain Khaliq[5]

1 PhD Scholar, The University of Lahore. Sana.Rehman@ais.uol.edu.pk
2 Assistant Professor .The University of Lahore .salman.ahmad@ais.uol.edu.pk
3 Lecturer Islamic studies. The University of Lahore. aneeba.basharat@ais.uol.edu.pk
4 Lecturer Islamic Studies the University of Lahore. wahaib.rehman@ais.uol.edu.pk
5 Lecturer, PhD Scholar, The University of Lahore. hussnain.khalid@ais.uol.edu.pk
Corresponding Author: Sana Ur Rehman PhD Scholar, The University of Lahore.

Abstract:

Currency is one of the most important economic issues nowadays. Currency is the backbone of economic affairs. It is impossible to run the country's economic system without currency. In the 20th century, new standards of currency value were set. Back then, gold and silver were abolished, and tied to the market value of any country, and the market value was tied to the dollar.

After the introduction of computers in the banking system in the 1960s, new aspects of using paper currency were also introduced, such as digital use of government-approved currency through credit cards, debit cards, mobile apps, etc. It took some time, then the innovations of Easy Paya, Jazz Cash, and U Paisa were introduced. At the beginning of the 21st century, a new form of currency was introduced, which was named virtual currency.

Virtual currency has two parts. 1-Encryption. 2-Blockchain. And there are many types of encryption. There are three types depending on the use of blockchain. Virtual currency is created by combining encryption and blockchain. According to the use of these currencies, there are three types. Any type of virtual currency is used only with electronic devices. And these electronic devices are not common, they are specific. And this currency is also not common.

There are several Shariah prohibitions, in terms of creating virtual currency and using it as a medium of exchange. No government permission, virtual currency has no personal value, virtual currency includes an element of uncertainty, virtual currency is valued in dollars. It is associated with and varies from country to country on the value of the dollar, the holder of virtual currency will take it and sell it where the price is good, there is an element of gambling in it, virtual currency does not have the status of an alias. The number of people using it as a tool of exchange is 3 to 5%.

There are also disadvantages in using virtual currency as property. Virtual currency is an immaterial asset, video, naat, recitation, film etc. but the nature of virtual currency is different, virtual currency as property does not fulfill Shariah rules and regulations. 3. Virtual currency is not a property. This property is not included in Shari'a and Sati rules, it is not known to anyone except the user of the secret of its use.

Keywords : Digital virtual currency Review Sharia context.

Introduction

If we examine the economics in the present age, it is found that there is an unfair distribution of resources, illegal use of authority, and economic and financial systems are being imposed by the powerful circles as they wish, on which an atmosphere of distrust is gradually being established among the people. Gradually, this effect is appearing on people and financial institutions as well, and mistrust continues to increase. The people's confidence has gone up, be it government, private or public institutions. The issue has been debated for decades as to how to create an atmosphere of trust in a centralized or decentralized currency.

Can we create a currency in which global, regional and government financial institutions do not have their influence, the currency is not controlled by any individual or organization, can freely use this currency, use of the currency? There should be no regional specialization. There should be no global and government pressure in currency indexation.

Because after the Second World War, the Bretton Woods Conference was held in July, 1944, which led to the establishment of institutions such as the International Monetary Fund (IMF), the World Bank and later the United Nations and the World Trade Organization (WTO). So that all the resources of the world can be controlled under one central system, and all countries, big and small, and their inhabitants, all come under this central system, and all their energies and resources come under this central system.

Until 1968, one ounce of gold for 35 US dollars, this system completely failed and on August 15, 1971, the American president "Runnecks" closed the gold window so that no one can buy gold at a fixed rate anymore. Now there is no gold behind any currency, all countries are guaranteeing their fiat currency.

There is no denying the importance and usefulness of currency in modern times, currency is essential for running every system from home to country. Without currency, man is unable to fulfill his needs. Its importance in Islamic Shariah is more than any other prevailing religion.

Definition of Currency:

Currency: It is an English language word, which means a system of money commonly used in a particular country.-(1)

When these two words are used together, it will be defined.

According to the Oxford Dictionary of Currency:

"The money in general use in a country". (2)

According to Currency Feroze Ul-Lughat:

"An official note used in transactions instead of cash"

Currency is called Filos in Arabic, and the definition of Filos in Arabic is:

Except gold and silver, every metal that people set the standard of value. (3)

The economic system has had a profound impact on the society in every era, and the economic conditions of the people have been getting worse and worse, except for a few institutions and individuals, their economic conditions are getting better and better. . In the era of barter system and gold and silver coins, people were economically free and prosperous, gold coins were worth the amount they could

(1) www.dictionary.com

(2) www.dictionary.com/browse/currency #:

(3) https://terminologyenc.com/ur/browse/term/8668

use, and the financial status of these coins never decreased. But as soon as paper notes replaced gold and silver coins, the people began to suffer economic degradation and economic slavery. "Registers. Notes are now "legal tender" rather than "legal tender", which can be exchanged for gold, silver, or any other commodity.

Now it is the era of cashless currency, society's decision of paper currency system was questionable from the perspective of protection of property in the purposes of Sharia, and now virtual currency does not even have a chance to regret in this system. In January 2022, in January, 18 billion disappeared in a moment, in a way that no precedent can be given.

There have been four systems of currency or its substitutes for transactions in human history.

1-Barter system 2-Coins 3-Paper notes 4-Paperless currency

There are two types of currencies in use today.

1. Paper currency. 2- Paperless currency.

Definition of digital currency:

"Digital currency is a form of currency that is available only in digital or electronic form". It is also called digital money, electronic money, electronic currency, or cyber cash.

Digital currency as a broad term can encompass anything that represents value in digital form.

A digital currency is electronic "money", that is, money that can only represent a digital currency equivalent to government-issued fiat currency. Fiat currency is certified by the government, this currency has no intrinsic value, i.e. it is not linked to any commodity like gold, silver, it is considered as legal tender.

Digital currency has no physical properties, it is available only in digital form. Transactions through digital currency are made using electronic devices, apps or designated networks connected to computers or the Internet. Whereas physical currencies, such as banknotes and minted coins, are tangible, that is, they have specific physical attributes and There are features. Transactions involving such currencies are only possible when their holders have physical possession of those currencies.

Central banks and digital currencies

The currency system in any country is managed by the central bank of that country. The central bank can issue currency in both cases. Fiat Currency, Digital Currency Central Bank Digital Currencies (CBDCs) are digital currencies issued by the central bank of any country. CBDC can be a supplement or a replacement for traditional fiat currency. Unlike fiat currency, which exists in both physical and digital form, a CBDC exists purely in digital form. (1)

There are three types of digital currencies.

1. Digital Currency: Regulated or unregulated currency that is available only in digital or electronic form.

2.Virtual Currency: Decentralized digital currency that is controlled by defined network protocols.

3-Cryptocurrency: A virtual currency used to secure and verify transactions as well as manage and control the creation of new currency units, uses cryptography. (2)

Definition of Virtual Currency

Virtual and currency is a combination of two words virtual, currency.

(1) https://www.investopedia.com/terms/d/digital-currency.asp#citation -

(2) https://www.investopedia.com/terms/d/digital-currency.asp

Virtual:

"It comes from the Medieval Latin virtuālis, meaning "effective" (in the sense of having the effect of something without the form or appearance of it). The various senses of virtual are quite different, but they all involve something that's not quite the real thing".

According to the International Monetary Fund (IMF), it is defined as:

"VCs are digital representations of value, issued by private Developers and denominated in their own unit of account."(1)

Definition of European Central Bank:

"A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community''(2)

"

According to the European Banking definition:

"VCs are defined as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically. ''(3)

These definitions are generic and different currencies may lack any of these features or have an excess of additional features.

Substitution of virtual word:

The word "virtual" is an English word that was transferred from Latin to English in the early centuries. In computer terminology, this word is used for a specific meaning. It means: "Something that does not have a sensory existence but is made by software to appear as such. (4) The information contained in a computer cannot be perceived by human senses, but it can be stored on a hard disk and Other devices exist in some form and can be screened and viewed through software.

Introduction to Virtual Currency:

Virtual currency is a type of unregulated digital currency. It is not issued or controlled by the central bank. Examples of virtual currencies include Bitcoin, Litecoin, and XRP. Digital currency is stored and transacted in digital form through designated software, applications and networks.

Virtual currencies are usually issued by private issuers and used in specific virtual computers. The security of the software and networks on which virtual currencies stand is questionable.

(1)International Monetary Fund: Virtual Currencies and Beyond: Initial Considerations,2016,P: 7

(2)European Central Bank: Virtual Currency Schemes, Published : Oct 2012, P:13

(3)European Banking Authority: EBA Opinion on virtual currencies, Published: 2014,P:11

(4)Oxford online dictionary: https://en.oxforddictionaries.com/definition/virtual -

A traditional regulated currency is backed by a sovereign (fiat currency) or market value. In contrast, virtual currency is not backed by any external value. The value of virtual currency is mainly driven by supply and demand. As a result of its unregulated nature, a virtual currency can be subject to large price fluctuations.

Virtual currency can be issued under centralized or decentralized centralization. Decentralization Virtual currency does not have a central administrator.

The decentralized centralization of virtual currency relies on blockchain networks, which are based on cryptography. Virtual currency based on cryptography is known as cryptocurrency.

The main objective of the invention of virtual currency is to give the currency an independent and autonomous status instead of being subordinated and owned by a particular center (government or state) which is owned directly by the people rather than by a particular authority. By giving the same shape and status to the currency in the whole world, the same currency should be given universal status. The physical existence of which is stored on a computer server instead of a specific substance or a sensory object, which can be transferred from one place to another through the Internet or a digital device, and like publishing and broadcasting through the Internet is universal. There are mills, in the same way a single currency can be given the feature of globalization and thus the dream of globalization which has been circulating in the mind of a certain class for a long time can come into existence.

History of Virtual Currency

Virtual currencies appeared in the 1960s. The essence of this idea is to have a currency that can be used through the world wide internet. No metal or substance should be spent on its birth, nor should it be protected in material form.

Initially, the concept of virtual currency was similar to that of current government currency (i.e., it included the concept of centralization), but as a currency backed by multiple institutions, companies, governments, or individuals that issued it, transacted it. handle and protect it from counterfeiting. Under this point of view, many currencies came into existence like E-Gold [(1)] and London Dollar [(2)] etc.

These currencies were created and managed by a company, institution or person. The problems of these currencies were many such as legal issues, bankruptcy or runaway of the currency issuing institution, hacking protection and influence of governments on the currency etc.

By promoting the same concern of virtual currencies, various banks have made transactions of government currency (e.g. dollars, rupees, etc.) possible through computers and the Internet. This case was stronger and more durable than the first case, but the problem was that these currencies were also not protected from government influence and inflation etc. These currencies are better known as "digital currencies" rather than virtual.

This era begins in 2009 when an anonymous computer programmer invented a sustainable and robust virtual currency in the form of Bitcoin. The Bitcoin theory was presented by Satoshi Nakamoto in a paper in 2008. [(3)]

Satoshi Nakamoto presented the concept of "Blockchin System" for this. Satoshi

(1)European Banking Authority: EBA Opinion on virtual currencies, Published: 2014,P:11

(2)http://secondlife.com

(3)Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System.

Nakamoto founded Bitcoin in 2009 and worked on it with other developers until the end of 2010. (1) This was the beginning of a regular virtual currency under the blockchain system. Researchers in mathematics, computer science, and economics introduced the organized system of virtual currency in 2008 as two basic parts.

1- Cryptography) -2 :Block Chain

1-Cryptography :

Evolution in Cryptographic:

The idea of using cryptography for private business transactions originated in the 1990s with David Chaum's eCash system. (2)

In the 1990s we saw several cryptography ideas that were not directly related to the use of cryptography in financial transactions but were, such as junk email by Dwork and Naor. (3) which was published in 1992, and which used computationally expensive functions. Then in 1996, time-locked cryptographic puzzles (4) were proposed by Rivest, Shamir and Wagner using RSA-based CPU-expensive computations. In the late 1990s and early 2000s, several patent-free cryptographic concepts were proposed and implemented as open projects by an online movement and community of cryptographers and programmers called Cypherpunks. goes

Introduction to cryptographic and hash functions:

This cryptographic tool helps in secure authentication and ensures data message integrity over digital channels—here's what to know about what a hash function is and how it works. A hash function is a serious mathematical operation that plays an important role in public cryptography.

Definition of Hash in Technical Sense:

A hash function is a versatile one-way cryptographic algorithm that converts input data of any size into modified unique output data of a fixed length of bits. The resulting display data, known as a hash digest, hash value, or hash code, and the display data has its own unique identifier(5).

A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Thus regardless of the original amount of data or file size involved, its unique hash will always be the same size. Moreover, hashes cannot be used to "reverse-engineer" the input from the hashed output, since hash functions are "one-way" (like a meat grinder; you can't put the ground beef back into a steak). Still, if you use such a function on the same data, its hash will be identical, so you can validate that the data is the same (i.e., unaltered) if you already know its hash(6).

Theory of hash functions in cryptography

(1) http://www.coindesk.com/information/ who-is-Satoshi-Nakamoto.

(2) E. Hughes. (1993). A Cypherpunk's Manifesto. Accessed: Apr. 18, 2019. [Online]. Available: https://www.activism.net/cypherpunk/manifesto Html.

(3) C. Dwork and M. Naor, ''Pricing via processing or combatting junk mail,'' in Proc. Annu. Int. Cryptol. Conf. Springer, 1992, pp. 139–147

(4) D. Chaum, ''Blind signatures for untraceable payments,'' in Advances in Cryptology, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, 1983, pp. 199–203

(5) D. Chaum, ''Blind signatures for untraceable payments,'' in Advances in Cryptology, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, 1983, pp. 199–203

(6) https://en.wikipedia.org/wiki/Hash_function. Accessed Mar. 17,2023

"A hash function is a unique identifier for any piece of content. It is also a process that takes plaintext data of any size and converts it into unique ciphertext of a specified length".

The first part of the definition implies that neither of the two pieces of content will have a hash, and that if the content changes, the hash will also change. Basically, hashing is a way to ensure that any data you send reaches your recipient in the same state as it left you, completely intact and unaltered.

However, cryptography and hashing are not the same thing. These are two distinct cryptographic functions that help facilitate secure, legitimate communication. What does hashing look like in cryptography?

Cryptographic types

Post-Quantum Cryptography

Post-quantum cryptography ( ) is a system of breaking cryptography by quantum computers, which will have the effect of breaking the cryptographic security of the blockchain. Used in most blockchain applications. Digital Signatures. Research in this area is ongoing to create a Post-Quantum Resistant Digital Signature (BPQS) ( ), which is a hash-based signature, e.g.

Post-quantum cryptography is also used to create secure cryptocurrencies based on post-quantum blockchain ( ) using one-time signature chains or post-quantum blockchain ( ).

M. Lightweight Cryptography

Traditional cryptographic methods, such as RSA and SHA256, work well on systems with adequate memory and processing power. M-lightweight cryptography is a system that requires large key size, throughput, speed, and energy consumption to be used, making it difficult to use in conventional resources and limited devices. Still, there is an ongoing research on it.

Verifiable Random Function (VRF)

Primitive ( ) is a pseudorandom function that provides a publicly verifiable proof of its output based on public (input) data and a private key. In short, it maps inputs to verifiable pseudorandom outputs. VRFs can be used to provide deterministic prior commitments that can later be demonstrated using evidence. VRFs are resistant to pre-image attacks, unlike traditional digital signatures. VRF has a triple.

White Box Cryptography( )

White box attack is a dangerous cryptography model. This cryptography can be used in both negative and positive ways. This allows cyber attackers to have full control over the internal data flow of the block, allowing them to modify the blockchain's data and code. White box cryptography can also be used in a blockchain to establish trust and privacy of assets in a positive way. As in blockchain, to store the key securely, it can be obfuscated in white-box cryptography. It is used in runtime self-protection in a trusted blockchain-inspired ledger ( ) and can be used in other blockchain applications.

Incremental Cryptography( )

The idea behind making incremental cryptography is that if a document is modified from M to M r , then the result when updating M is "proportional" to the "modification amount". Should. The initial idea proposed for incremental cryptography uses the analogy of a digital signature. The idea was to have a digital signature that is easy to update upon modification of the underlying message. If M is changed to M r by adding/deleting any block, the time to update the signature from σ to σ r is the ``modification amount" to get M r ' should be 'proportionate'.

Different virtual currencies of the world

Blockchain, Bitcoin and Libra are the big international names in virtual currencies at the moment. The popularity of these types of currencies is gradually increasing. They are also called cryptocurrencies.

1.Ethereum

The Bitcoin alternative, Ethereum, is a decentralized software platform that enables smart contracts and decentralized applications (DApps) to be created and run without downtime, fraud, control, or third-party interference. . The goal behind Ethereum is to create a decentralized suite of financial products that can be freely accessed by any individual nation in the world. This aspect is more compelling for those in some countries, as those without state infrastructure and state identification can access bank accounts, loans, insurance, or a variety of other financial products.

2.Litecoin(LTC)

Litecoin, launched in 2011, was among the first cryptocurrencies to follow in Bitcoin's footsteps and is often referred to as "Bitcoin's gold to silver". It was created by MIT graduate and former Google engineer Charlie Lee. Litecoin is based on an open-source global payment network that is not controlled by any central authority and uses "scripts" as proof-of-work, which can be decoded using consumer-grade CPUs. can Although Litecoin is similar to Bitcoin in many ways, it has a faster block generation rate and therefore offers faster transaction confirmation times.

3.Cardano (ADA)

Cardano is an "Ouroboros proof-of-stake" cryptocurrency that was created with the research-based approach of engineers, mathematicians, and cryptographers. The project was co-founded by Charles Hoskinson, one of the five founding members of Ethereum. After some disagreement with the direction Ethereum was taking, he left and later helped build Cardano.

The team behind Cardano built its blockchain through extensive experimentation and peer-reviewed research.

Because of this strict process, Cardano stands out among its proof-of-stake peers as well as other major cryptocurrencies.

4.Bitcoin Cash (BCH)

Bitcoin Cash (BCH) holds an important place in the history of altcoins as it is one of the earliest and most successful hard forks of the original Bitcoin. In the cryptocurrency world, discussions between developers and miners result in a fork. Due to the decentralization of digital currencies, wholesale changes to the code underlying the token or coin in hand must be made by general consensus; The procedure for this process varies according to the specific cryptocurrency.

5.Stellar (XLM)

Stellar is an open blockchain network designed to provide enterprise solutions by connecting financial institutions for the purpose of large transactions. Many transactions between banks and investment firms that would normally take days, multiple intermediaries, and cost significant amounts of money can now be done almost instantaneously without intermediaries and There is very little cost to the transactors. The system allows cross-border transactions between any currency. Stellar's native currency is Lumens (XLM). The network requires users to hold Lumens to be able to transact on the network.

6- Binance Coin (BNB)

Binance Coin is a utility cryptocurrency that serves as a payment method for fees associated with trading on the Binance exchange. Those who use the token as a means of payment for exchanges can trade at a discount. Binance Coin's blockchain is also the platform on which the Binance options exchange operates. Binance Exchange was founded by Changpeng Zhao and is one of the most used exchanges in the world based on trading volume.

7. Tether (USDT)

Tether was one of the first and most popular of a group of so-called stablecoins, cryptocurrencies that aim to peg their market value to a currency or other external reference to reduce volatility. Since most digital currencies, even major ones like Bitcoin, have experienced dramatic fluctuations time and time again, Tether and other stablecoins try to smooth out price fluctuations to attract users who Otherwise, be careful. The value of Tether is directly linked to the value of the US dollar. This system allows users to transfer from other cryptocurrencies to US dollars more easily and in a more timely manner than actually converting to regular currency.

8.Monero (XMR)

Monero is a secure, private and untraceable currency. This open source cryptocurrency was launched in April 2014 and soon gained a lot of interest among the cryptography community and enthusiasts. The development of this cryptocurrency is completely donation-based and community-based. Monero was launched with a strong focus on decentralization and scalability, and it enables complete privacy by using a special technique called "ring signatures".

Introduction to Blockchain Ledger

Blockchain, a distributed ledger that is peer-to-peer linked in time through a centralized network, and collectively adheres to certain agreed-upon rules, is considered a cutting-edge technology. What is to be done? Blockchain technology has gained success with the financial success of Bitcoin (BTC) while this technology is being used for various purposes such as identity cards, visas, security, etc. It is widely used in more than 2140 cryptocurrencies. These currencies have created a financial market worth around $300 billion (January 2021) using this currency for secure and private transactions for payment for services such as online games, internet money transfers, internet shopping and other commercial activities.

Blockchain has been envisioned as a promising and powerful technology, but this technology is an invention of human genius, so it still faces many research challenges. For example, security, privacy, key management, scalability, analysis of new attacks, smart contract management, and an increasing trend of new cryptographic features in existing blockchains.

Definition of Block Chain

The blockchain system is the system on which all virtual currencies of the present day are working. This system connects several computers together and enables transactions and exchanges between them. There are various definitions of blockchain systems:

1. Melanie Swann in her book “Blockchain: Blueprint for a New Economy” defines “Blockchain” as follows:

> “The blockchain is the public ledger of all Bitcoin transactions that have ever been executed". [1]

2.Florian Glaser and his colleagues describe the blockchain as:

> "The Blockchain represents all verified and valid transactions between users of the network".[2]

3. "Wikipedia" states in its definition:

> "A blockchain is a distributed database that is used to maintain a continuously growing list of records, called blocks ’’[3]

Types of Blockchain

(1) Melanie Swan: Blockchain: Blueprint for a new economy, Page x (Preface), Publisher: O'Reilly

(2) Florian: Bitcoin, Asset or currency, P:2

(3) https://en.wikipedia.org/wiki/Blockchain

There are four types of blockchain in terms of design, management rules, data availability, and accessibility.

In terms of privileges, they are classified as Public and Private. While from the administrative point of view, they are defined as "authorized" and "unauthorized".

1.Permissionless Public: In this type of blockchain, anyone can join or leave the network at any time. Everyone has read and write access to the blockchain. Thus it provides minimal trust between the participants. Most cryptocurrencies and blockchain platforms are permissionless public, such as Bitcoin [(1)], ZeroCash [(2)] and Monero [(3)].

2. Permissioned public: Once a participant in this type of blockchain is granted certain privileges such as the nature of the blockchain and permission to read the data, there are certain privileges with other participants, making this particular method a system. does not make it a fully centralized authority. Examples of permissioned public blockchains are Ripple [(4)], EOS[(5)] and the latest Libra [(6)], etc.

3.Permissionless Individual: This type of blockchain gives organizations access to public blocks. Being permissionless, anyone has the freedom to join or leave the blockchain at any time. Some permissionless private blockchains include the LTO [(7)] network.

4. Permissioned Individual: These blockchains are mostly used in organizations where data/information is stored in the blockchain with permissioned access control by members of the organization. Membership in a network is granted by the network administrator or some other membership authority. Read and write access to data is also provided by the network administrator. Hyperledger fabric [(8)], Multichain[(9)] are examples of permissioned private blockchains.

Types of Blockchain:

There are three types of chains in a node.

1-Primary chain 2-Secondary chain 3-Orphan blocks

Mechanism of Blockchain System: Blockchain is used in three different ways.

1. Protocol

Protocols: What is the language used in blockchain, how nodes are part of the system, how money will be standardized and exchanged, how consensus will be reached, etc.

2. Network: How will blockchains be interconnected? included.

3. Application: How will data, mines, nodes and applications interact?

Characteristics of Blockchain: Blockchain has seven different characteristics.

1- Secure 2- Anonymous 3-Agree 4-Timestamp

(1)S. Nakamoto. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: http://bitcoin.org/bitcoin. pdf

(2)E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, ‘‘Zerocash: Decentralized anonymous payments from bitcoin,’’ in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 459

(3)https://en.wikipedia.org/wiki/Blockchain.

(4)The Monero Project. (2014). Monero. [Online]. Available: https://web.getmonero.org

(5)R. F. A. Britto and D. Schwartz. (2012). Ripple. [Online]. Available: https://ripple.com.

(6)EOS. IO. (2017). EOS. IO Technical White Paper. Accessed: Dec. 18, 2017. https://www.github.com/EOSIO/ Documentation.

(7)Libra Association. (Jun. 2019). The Libra Blockchain. Accessed: Jun. 24, 2019. https://www.developers.libra.org/ docs/assets/papers/the-libra -blockchain. pdf

(8)LTO Network.(2014). Blockchain for Decentralized Workflows. https://www.lto.network.

(9)G. Greenspan. (2015). MultiChain Private Blockchain. https://www.multichain.com/download/MultiChain-White-Paper. pdf

5-Immutable 6-Distributable 7-Authority to create a new program

Interworking of Computers (Network Architecture)

Computer networking can be classified into a group or group based on the functional relationship between the elements in them. For example, Active networking, Client-Server and Peer-to-Peer/P2P architectures. From this point of view, the interaction of computers can be linked in the following ways. With which they can relate and work together.

Blockchain Network Infrastructure-

Blockchain is maintained through a peer-to-peer (P2P) network. A P2P network is an overlay network built on top of the Internet. A P2P blockchain network can be modeled as structured, unstructured or hybrid based on different rules and regulations such as consensus mechanism and type of blockchain

Almost all cryptocurrencies and blockchains such as Bitcoin, Ethereum, Litecoin, etc., use unstructured P2P networks. A P2P network can follow a flat or hierarchical organization to form a random graph between peers. This graph is not fully connected, but to capture all communications and maintain a ledger, each peer maintains a list of peer addresses. Thus, if a peer advertises a message in the network, all blockchain members receive it through their available connections.

Different components of blockchain.

Blockchain relies on different components that serve different purposes. Kiln and Fork.

Forking

Years after Bitcoin launched and its source code was published as open source on Github, blockchain designers began to clone and fork its core.

A blockchain fork is basically created when two miners get a block around the same time due to a software update or version. In a blockchain network, each device or computer is considered a "full node" that uses software to secure the blockchain by verifying the ledger. The software is updated to adjust certain parameters and install new features in the blockchain. This updated software is not compatible with older software. Consequently, older nodes that have not updated their software and newer nodes that have updated their software can cause forks in the blockchain when they create new blocks. There are two types of forks:

1-One that is incompatible with previous software versions, called a hard fork.

2-The second one which is compatible with the previous software version, called Soft Fork.

A hard fork occurs when a significant change occurs in the software, such as a change to the rules and regulations in a block or a change in the consensus mechanism. In the case of Ethereum (white paper), a hard fork will occur when it transitions from proof-of-work to proof-of-stake[(1)]. An example of relaxation is the Segregated Witness (SegWit) fork that was implemented in Bitcoin by changing the transaction format. Recently, the privacy coin Beam[(2)] (an implementation of the Mimblewimble privacy protocol) took its first hard fork away from ASICS. A blockchain forking scenario is shown where the correct chain can be either of these two forked chains, depending on the case of a hard or soft fork.

Mining Incentive System (to create a new block or program)

The process of creating new transactions and new currency in the blockchain is done by the mining process. In the mining process, a puzzle is solved by repeatedly computing a number of hashes (Equation 2) with different values to

(1)C. Lee. (2011). *Litecoin*. https://litecoin.org

(2)Beam Development Team. Beam. 2019. https://www.beam.mw

satisfy the condition. By keeping When a miner is the first among all miners to successfully solve a puzzle, he receives a monetary incentive for solving the puzzle. Due to this incentive process, all consensus nodes or miners follow the blockchain state transition rules during the puzzle competition.

Mining is a resource-intensive process, there are two main resources for mining. One is computational power and the other is memory. Mining is done in two ways.

1. Solo Miner (individual)

Solo or individual mining involves solving hash puzzles individually, this way the currency that is created can be used in different mines.

2. Pool Miner (Collective)

who collectively try to solve the puzzle. The mining ocean works on various mining techniques and incentive mechanisms. These incentive systems may vary based on the mining technique used or the decision of the pool operator. [(1)]gives a brief overview of mining strategy management in blockchain networks, providing a strategic study of mining through stochastic games[(2)]. Various incentive systems have been proposed and tested in blockchains. Bitcoin Pooled Mining presents an analysis of reward systems, and a reward system based on the dissemination of information in the blockchain network[(3)].

Difference Between Digital and Virtual Currency.

The journey of currency began with the era of barter sale. Moving forward it took the form of gold and silver coins. After that it took a new direction. Which was to be changed from "real price" (gold and silver) to "nominal price". This nickname exists today in the form of currency notes, but this journey of currency does not stop there, rather this journey continues and with its continuation has now become a form of "digital currency".

Digital currencies and their use.

Definition of digital currency according to World Bank

"a numerical representation of a specified value, a unit of account"

According to the Bank of International Settlements (BIS):

“Digital currency defined as the value of fiat currency.

Digital currencies are similar to digital money and represent any existing payment method that is purely electronic in nature, and therefore not physically tangible like notes or coins, and currency calculations, transfers And exchanged between computers and internet devices, digital money also represents fiat currencies, such as dollars, euros, rupees or other currencies.

Digital currencies are digital money exchanged over a network using technologies such as smart phones and credit cards. The Internet, and some machines, can convert money into physical cash through ATMs that represent values. . or branches of banks that accept such currencies.

1-Digital money is an existing currency in paper form, and is not a tangible physical asset such as cash or other commodities

2-Most digital money in the world is owned by banking institutions, and online payment providers can be considered. Like Alipay, WeChat Pay, and M-Pesa are digital money.

(1)W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, ‘‘A survey on consensus mechanisms and mining strategy man-agement in blockchain networks,’’ 2018. https://arxiv.org/abs

(2)A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, ‘‘Blockchain mining games,’’ in *Proc. ACM Conf. Econ. Comput. (EC)*, New York, NY, USA, 2016, pp. 365-

(3)M. Rosenfeld, ‘‘Analysis of bitcoin pooled mining reward sys- tems,’’ 2011, https://www.arxiv.org /abs.

3-Banks have been able to keep their cost of doing business low thanks to digital money as they don't need to pay rent to websites.

The term digital currency is the term for all legal digital currencies, and these currencies are called digital. It has no tangible physical existence,but is evidenced with tangible paper and coins.

Cryptocurrencies and their uses:

Cryptocurrency is a special type of digital money, controlled by cryptographic algorithms. It does not have a central authority that controls money in its traditional form, as does the authority of central banks. A cryptocurrency is called a currency, unless it is defined as an intangible currency for a tangible or centralized currency. It is purely cosmological and encrypted, although it does not have its own encryption tools and is difficult to secure ethically. In order for cash to represent and act as a substitute for cash, a centralized control and other equipment needs to be substituted for traditional cash. -

The Financial Action Task Force (FATF) defines it as:

"A paper representation of value that cannot be electronically or digitally traded and exchanged acts as a source of, and is a legal unit.

These currencies are divided into three categories according to the classification of the European Central Bank.

First type: Currencies used in specific situations.

Second Type: Fixed and Fixed Currencies: These currencies are convertible, and are linked to fiat currencies or the economy, and currencies that have no exchange rate against legal currencies and are used as exchange currencies to buy necessities of life. There are

The third category: are the additional currencies that are linked to the legal currencies or the real economy, and have an exchange rate for them.

Contradictions and necessities can be used as currency to buy life.

- Difference between Digital and Virtual Currency:
- Digital currency is a broad concept.
- Which are exchanged for all financial assets in digital form.
- Virtual currency is a subset of digital currency, and cryptocurrency is a subset of virtual currency.
- Digital currency is regulated.
- A regulated digital currency is issued by a country's central bank and can be converted into a sovereign currency.
- The regulated type of digital currency is thus subject to the country's monetary policy.

Virtual Currency:

- Virtual currency is a type of unregulated digital currency.
- Virtual currency is issued and controlled by a private issuer rather than a central bank.
- Virtual currency is not subject to any monetary policy.
- Virtual A virtual currency can be either centralized or decentralized.
- Cryptography is used in virtual currencies.

Virtual and Digital Currency in Islamic Sharia

Islamic Shariah guides its followers, for guidance, Shariah Motahara has formulated various Muslim principles, which solve the problems that have arisen and are ordered after research. Which are practicable and Corruption comes from the society. A review of some of these Shariah principles is presented.

Powers of ruler in expediency

How many nights do the ruler have in expediency? Does the ruler have full powers to enforce all kinds of orders or are there some rules and regulations? There are two conditions for disposing of the ruler's concession.

1- There should be expediency in the lawful matter

2- There should be expediency in the matter for the people and there should be no oppression.

Any command in which there is no benefit to the people in this world or the hereafter, but if it is a command based on cruelty and lust, then it is not obligatory to obey it.

Maulana Taqi Usmani Sahib in "Islam and Modern Economic Problems" mentions four (4) conditions of ruler's powers in the interests.

1-The order should be in the realm of arguments.

2- In the order, it is not necessary to violate any order of Quran and Sunnah.

3-Do not oppress anyone by order.

4- The order should be in accordance with expediency. (1)

It is clear from this that the ruler of the time does not have unlimited powers and can implement any order under the guise of interests.

Prophet Muhammadﷺ said:A servant whom Allah makes a subject (ruler) of a subject and he does not wish him all the best, then he will not be able to get the scent of Paradise". (2)

Hanafia and Shafia

Most of the usulists and researchers agree about Hanaf and Shuafi jurists that it is not correct to argue the expediency here. Therefore, Allama Amadi says:"The Shafi'i, Hanafi and other jurists are in agreement on not making this (Muslahat Mursala) a proof and this is correct." (3)

Dr. Mustafa Zaheili has also said the same thing. (4) Some scholars have considered the "Istihsan" present here of Hanaf as expediency, but this does not seem to be correct. The Hanaf usulists have called Istihsan a type of speculation. Also, the Hanaf jurists use this term to refer to the existing texts and gatherings as compared to Qiyas. Allama Shami says:

" Then in the term of principle its use for Qiyas Khafi is dominant as the name of Qiyas Jali is often used to distinguish between the two Qiyas. It is well-known that Istihsan is applied in Al-Faroo to the text and Ijmaa as opposed to the hypothesis. (5)

Most of the present-day researchers have adopted the creed of Masal-Mursla being the authority. The following are the conditions for their validity:

1. Expediency will be considered as a Hujjat in matters, not in worship.

2. There is no profit motive or corruption in it.

3. Whether the intention is real and complete, partial interest of one or some persons) or illusion and imaginary interest will not be valid. It should not be against the regular Shariah order of expediency. (6)

Review of administrative rules:

According to the rules of jurisprudence, some other order can be imposed on it administratively. Some of the well-known rules are:

Hardship brings ease:

This rule is one of the "Imahat al-Qasear", where there is real hard work, the ease of people will be seen.

The purpose of Shariat is not hardship but ease. Whether these authorities are related to worship or matters, the order will be reduced and a way of ease will be found.

The order of virtual currency (Blockchain, proper information about crypto, electronic devices, internet, full accessibility) is labor for the people.

The origin in the accidental attributes is non-existence

(1)Osmani, Muhammad Taqi, Islam and modern economic problems, Islamiyat Institute, vol.8: p.31

(2)Mishkat al Msabih:3687

(3)Amdi,Al Ahkam fi Usool al ahkam,vol.4:p.160

(4) Zohili,Whba,Alwjeez fi usool alfqha,vol.1:p.255

(5)Ibn Abdin,Tsmat al shar,vol.1:p.224

(6)sheikh Ebdhoo Umer,Mujlh Majmeh Alfqh Alislami,vol.6:p.1467

Attributes of disorder will be considered extinct. Attributes of disorder are the attributes that are not found in it at the time of creation. Apply later. The law regarding the attributes of disorder is that they will be considered extinct, and if any argument is established on the stability or negation of these attributes, then the order will be applicable according to this argument.

Blockchain, cryptography, internet, etc., do not have the attributes of currency, combining them and presenting them in the form of currency is the attribute of "Taira".

bears the special damage to pay the Ho general damage

If there is harm to all Muslims in a place and it can be removed by the harm of one person, then the harm of that person will be tolerated. An example of this is that if the traders in a place have made the commodities too expensive, then the ruler has the power to fix their prices. This will harm these traders but the harm to all the people will be removed. As a general rule, it is the seller who is the actual owner of the thing to determine the price of the thing sold.

العادة محكمة:

If there is no clear order of the Shariat about a work, aliases and people's habits will be taken into account. Based on this, the real meaning of a person's words is discarded and replaced by the meaning that the people of that area take to mean. (1)

Alias:

Literal definition of alias

``Araf'' and ``Habitat'' are the same thing. ``Habitat'' is derived from ``Aud'' and ``Mawaudah'', literally, it means method, style, and doing something repeatedly.

مأخوذة من العود أو المعاودة بمعنى التكرار، والعادة: اسم لتكرير الفعل أو الانفعال حتى يصير سهلاً تعاطيه كالطبع.(2)

Terminological definition of alias

Those who gain a place in the hearts by accepting the right thoughts and good nature. (3)

Habit refers to those things that are repeated which are acceptable to nature. It means every action and speech which has become a habit among common people. (4)

Alias are of two types according to their types. 1. Alias Sahih. 2. Alias irregular.

Alias Sahih

The one who is not opposed to anyone in the Shariah texts, nor does any valid Shariah expedient die from it, nor is it a means of attaining any dominant evil. Sweets are distributed. Similarly, the clothes given to a girl on engagement and other items given to a woman called Hadiya are not included in the dowry.

URAF Irregular

Those who are against a text, or it causes harm or loss of an interest, such as illegal things are common among people. For example, taking loans on interest, betting money, playing cards and taking part in horse races. (5)

Conditions for an alias to be valid

(1) Al Gargani,Ali Bin Muhammad,Kitab Alteriftat,Vol.1:p149

(2)Dr,Muhammad Siddique,Ahmd,Alwajiz fi eizah qwaed alfqh alkulih,vol.1:p273

(3) Al Gargani,Ali Bin Muhammad,Kitab Alteriftat,Vol.1:p149

(4)Zain ud Deen AlHnfi Al ashbah w Alnzaer,Vol.1;p79

(5)Dr,Muhammad Siddique,Ahmd,Alwajiz fi eizah qwaed alfqh alkulih,vol.1:p282

1-In order for an alias to be valid and to base rulings on it, the following conditions must be met: The first is that the alias should not be against any provision of the Shariat. If that alias is against any text, then this alias will never be accepted. Just as there is a custom of usury in a country, then this alias will not be accepted. The situation will not be permissible. Or if there is a practice of drinking alcohol in a place, then such alias will not be accepted at all and it will not have any validity in Shariat. And if there is no opposition, this alias will be declared valid. (1)

2- Alias Mighty and Famous:

That is, his habit should be common with the meaning that no one opposed him, meaning that this nickname is common and common among common people and this nickname is often found among them, meaning that those who oppose him There are very few.

3-Thirdly, that alias on which a disposal is to be transferred: That alias exists at the time of the matter, or that the alias existed before the time of disposal and then continued until his time(2).

4- That there should not be any word or action that gives an advantage against the alias. As when the alias in the market is for payment of the price in installments, but the contracting parties agree that the payment should be made in cash or that the alias is on the fact that The cost of exportation of the goods is borne by the buyer whereas the parties agree that it shall be borne by the seller. And the rule in this regard is that what is proved without alias, then alias will not be proved if any condition is imposed against it. (3)

Alias implementation of rulings is a matter of relegation

Accidents and minor incidents have been relied upon to apply rulings. An example of this is that the condition of the court is necessary for the testimony to be accepted. The argument is Irshad Rabbani. There is a queen nearby who inspires the man with the queen to stick to piety and piety. What disturbs the piety is the same thing that causes harm in the court, and what disturbs the piety changes due to the change of time and place.

The case of changes in rulings due to change of times

Those rulings which are based on custom and habit are changed by the change of habit. This is the goal of the jurists that changing the rulings due to the change of time cannot be denied. That is why it is said that the rulings are Established by custom, they move with them wherever they move.

And these become invalid with aliases when they are invalid. Such as in the case of coins, the merchandise being defective and defective and other such cases. The price will be the value of the coin which is new due to habit, not the old coin. And similarly, when a defect in the cloth is considered a defect, the merchandise could be returned due to this defect. So when the habit changes and this defect is liked and it is also the cause of excessive price, it will not be returned and this law will be considered valid in all the rulings that are established due to custom and habit. And all the scholars. There is a consensus on this and this law will be respected in fatwas in every age, so when ever a new name is born, it will be valid and when it is invalidated, the order of Tawas will also be invalidated. (4)

In modern times, this is the name of the currency that it is issued with the guarantee of

(1)Zain ud Deen AlHnfi Al ashbah w Alnzaer,Vol.1;p79

(2)Syed,Abdul Kareem zedan, Alwajiz fi usool alfqh,p316

(3)Dr,Salh Bin Ganm alsdlan,Alqwaed Alfqheyh Alkubra,p357

(4)Shab Ud Dein ,Ahmd Bin Idrees,Al-Malki,Alfrooq lifraqi,vol.1:p176

the government, and this currency gets legal status. Otherwise, it has no credibility, nor does it have any financial status.

Blocking the means

Saddi' Zaree' refers to those permissible and permissible things that become a means of a forbidden and illegal act or there is a strong apprehension of becoming one.

The meaning of Saddi'-Zar'i is to prevent a person from a means that leads to something forbidden, even though that means is permissible and permissible per se, but the reason for its being Mufadhi al-Haram (i.e. leading to the forbidden). There will be sanctity in it. That is, in Saddi' Zare'a, a permissible and permissible action is prevented because this action involved a forbidden act, and this is Saddi' Zarie'a.

Arguments related to virtual currency are presented based on these sources, that there is no Shariah corruption in virtual currency per se, its use is correct. It is claimed that there are no Shariah problems in virtual currency. However, there are some administrative and practical complications. Also, since users of virtual currency currently have no legal protection, there is a fear that the use of virtual currency will sink public capital.

Therefore, using the argument of the sources, they are currently giving the opinion of pausing the use of virtual currency at the public level in order to ensure the protection of the wealth of Muslims, which is one of the purposes of Maqasid Al-Shari'ah. That is, if the legislation is passed and the government of Pakistan makes the use of virtual currency legal, then the use of virtual currency will be free from all objections. Just creating a virtual currency law will not solve the problem and the reason for this is that the law in the country is also for usurious banking system, so has usury become legal? No, not at all. Even if virtual currency is legislated in the countries and the use, sale and transaction of virtual currency is legalized, there are still many fundamental defects in virtual currency due to which the Mufti-e-Karam in the presence of these shari'ah evils, virtual currency. will exercise caution in issuing legal fatwa and will not issue a legal fatwa unless a fully Shariah-compliant virtual currency is in opposition to any Shariah rule and rule.

> Preventing from an act which itself is permissible but leads to a forbidden act is called "Sad al-Zar'ee".

There are two types of functions based on results.

1-Prohibited actions per person- 2-Prohibited actions per person.

1-Prohibited actions per se.

Those actions which are illegal and haram in themselves. Like drug addicts. There is no difference among the scholars.

In the first category, everything is agreed, but in the second and third category, there are two schools of thought:

Malikiyyah and Hanabillah:

According to Malikiyyah and Hanbalah, there is the validity of sad means, that is, every work that becomes a means of a forbidden work will be impermissible. Allama Baji Maliki says: [1]

"Imam Malik's school of thought is to stop about the sources. This is an issue that is obvious and should reach a certain person. Imam Abu Hanifah and Imam Shafi'i have declared the sources as permissible." Allama Ibn Najjar Hanbali says:

"And it will be prevented by the means. It is the plural of the means, i.e. any means from the actions and sayings which are manifestly permissible and through which they reach the forbidden. To prevent it means that because of its haraam. It will be forbidden to do it. It has

(1)Salman bin Khalf Baji,Alasharh fi usool alfqh,vol.1:p.80

been declared permissible by Abu Hanifa and Shafi'i." (1)

Hanafi and Shufi'a:

According to the imams of Hanaf and Shufi'a, the hadith source is not reliable. But if a work conveys another prohibited act, it will not be prohibited merely because of this conveyance, but it will be permitted. Allama Qur'ani and others have claimed that the principle of Sad-ul-Zar'ee is according to all the jurists, but according to some it is less and according to others it is more. Allama Tajuddin Subaki has strongly rejected this and cited different types of sources. He used to say

(Taqiuddin Subaki) said: There are three types of sources:

1- Permissible and permissible actions that sometimes cause great corruption or damage. This is forbidden according to Hanaf and Malikiyya.

2-Personally permissible and legitimate actions that often cause corruption or damage. Do not necessarily lead to the Haram, but mixed with something that leads to the Haram. It should be addressed and this rare situation should be reconciled. (2)

Scholars have said at different places that whatever leads to haram is also haram itself. In contrast to them, in the issue of selling grape juice to a winemaker, the Imams of Hanaf have stated that it is permissible. Allama Shami applies to both types of problems as follows:

> "Writer's statement: Everything he delivers. Hey, in this and in the issue of selling Shira to a drunkard, the imams should be considered in their opinion. The difference is possible in the way that will come next that the sin is not related to the character of the Shire. Rather, it will be related to him after his caste has changed." (3)

The result of this also comes out in accordance with the saying of Sigi that if something is haram in itself or there is a belief or strong belief that it will lead to haram, then it will be haram otherwise not. In this sense, the school of Hanafia and Shuafi agree on this issue

3- Individually permissible and legitimate actions which the obligee uses against the purposes for which they were created, may lead to harm.

General riots

What is meant by general rebellion is that all people will not follow the order if it is difficult to give up what they are doing and which is supposedly illegal. For example, it is difficult to avoid road water and mud in the rainy season, so it is excused if it gets on clothes etc. Permissible under Balwa. While the scholars say that crypto-currency is not yet so popular that a fatwa of its justification can be given under general law. Also, general law is not valid in every prohibited matter, but it is valid in various fiyh issues, and it is also not valid in halat and sanctity, but it is valid in impurity and purity.

Another problem is that since computer scientists and experts have different opinions about cryptocurrency. See, the principle thing is that computer scientists have no disagreement about cryptocurrency.

Price introduction.

Price (Rate): Market Price(4).

Price means the price of any goods that is of a standard or the market value of a similar item,

(1) Taqi ud Deen Muhammad Bin Ahmad Alnjar,Sharha Mukhtasar Althreer,vol.4:p434

(2) Taqiuddin Subaki,Al Ashbah w Alnzair,vol.1:p120

(3) Ibn Abideen,Rad Ul Almukhtar,Vol.6:p360

(4) https://shariahandbiz.com/index.php/miscellaneous/409-kharido- farokht-ki-fikhi-istlahat-ka-matlab

i.e. anything bought or sold at market value rather than by mutual consent.

Difference between cost and price.

'Price' is the price which is determined by mutual consent between the seller and the buyer. "Price" means the price at which a thing is usually sold. (1)

Difference between price and value: That the price is equal to the appraiser's value, without any reduction or addition.

And the price may be a small thing, and it may be according to it or more, and the property does not indicate the price, because all its money is the price of the property, and not every property has a price.

(1) Therefore, he included the sale in the verses and said in Surat Yusuf: And buy it at a cheap price.

(2) So he included the sale in the price, Imam Fara' says:

It is clear from these expressions that there is a difference in price. (2)

Terms and Conditions:

We have discussed the terms of the price in detail in the third chapter of the second chapter. These conditions are briefly mentioned here. Generally, there are no attributes of price in the holy Shari'ah, however, there is an additional mention of these attributes in sale. The same attributes that are found in gold are counted in the price, which are mentioned in the statements of the jurists, basically there are four.

Public acceptance.Medium of Exchange.Standard of Value.Store of Value

(Attributes of Cash (Zar) to the Economists

Zarki mentions three features.A means of preserving wealth

Medium of Exchange.Standard of Value

Additional condition for currency: Currency can only be issued by the government.

In modern times, only the government has the authority to issue money as currency because the entire system of financial transactions is based on currency. In the Encyclopedia of Jurisprudence:

"No one is allowed to make currency except the Imam, because it is injustice to him. And the imam has the right to punish the one who takes away this right from him, even if the currency he made is pure gold and silver. Imam Ahmed, may God have mercy on him, says that dirhams can only be made in the mint with the permission of the ruler of time, because if people are allowed to do so, they will suffer great suffering." (3)

Imam Nawi, may Allah have mercy on him, says:

"No one except the Imam is allowed to make dirhams and dinars, even if they are pure, because this is the Imam's right and this other is not allowed because there is a fear of forgery and distortion in it."

From the Islamic point of view, no one except the government of the time has the authority to issue currency, because in this way there is a danger of fake currency coming into being, which is the cause of corruption. Every country has a central bank that issues a currency with the permission of the government, this note bears the words "Issued on the guarantee of the Government of Pakistan".

"The State Bank also acts as an agent for the Government, therefore, under sub-sections 13 (a) and 13 (f) of section 17 of the State Bank of Pakistan Act, 1956, the Bank may sell gold, silver or approved currency. Authorized to purchase swaps and transact Special Drawing

(1) As abve

(2)Abi Helal Aleskre,Alfrooq Al Lgwyh,p237-238

(3)Encyclopedia of Jurisprudence,vol.41:p178,79

Rights with the International Monetary Fund. [1]"

Not all types of currency, only government approved currency can be used as exchange currency.

Two types of property:

1- Uraf non-mutaqum

By default, anything that cannot be profited from. (Insects, lions, etc.) [2] But the reason for the prohibition is not because they are unprofitable[3].

2- Sharia non-mutaqum

Every such thing that is not allowed to be used is honorable and non-permissible, its sale is not permissible, these are things that are used in a prohibited work[4].

Sale of alcohol by a Muslim will not be permissible in both cases (property and price).

According to the Imams of Hanaf, owning something is a different thing and being a Mutaqum is a different thing. If something is property but not a property, then by making it a price in the sale, the sale is held but invalid. According to Malikiyyah, Shufa'i and Hanbalah, it is included in the definition of non-saleable. So Allama Zarkshi says:

> "Worth according to Sharia is that which can be used for usufruct, that is, it is capable of usufructuring from it." [5]

Allama Bahuti says:

"Mal Shar'a is the one whose benefit is absolutely permissible, that is, it is valid in all circumstances or without necessity." [6]

The Companions of al-Masua al-Fiqhiyyah al-Quwaitya say:

"Malikiyyah and Shafiyyah have interpreted this condition as the word profit or benefit." Then they say: What is not profitable is not wealth, so wealth cannot be given in exchange for it, that is, transactions through it are not permissible. [7]

So the aid is in Imdad al-Fatawi:

"Electricity is also wealth as mentioned"[8].

Mufti Muhammad Taqi Osmani says:

"Electricity and gas have become among the major assets that people desire. It is difficult to include them in the values that are established by themselves. Nevertheless, their buying and selling is valid and people interact with them without any change. [9]

Electricity and gas are not recognized as property, but profit is obtained on their services. That is, they are considered in Kitab Al-Ijarah. Electricity and gas are property, but they are not used as currency or legal tender. can do

Some people liken virtual currency to electricity,while electricity and virtual currency cannot be compared. Electricity as a commodity and its profit is treated as a lease. There are many goods of services like wires, poles, meters etc. for the utilization of electricity, there is no example of virtual currency services, so there is no similarity between the two.

---

(1) https://www.sbp.org.pk/urdu/about/Func.asp

(2)Muhammad Taqi Osmani,Fiqh Al Buywe,vol,1:p402

(3)Mansoor Bin younas Bin Idrees,Al-Behoti,Kshaf alqnae en mn la qnae,vol.4:p152

(4)Muhammad Taqi Osmani,Fiqh Al Buywe,vol,1:p403

(5)Allama Zarkshi,Al-Mansoor fi Al-qwaed Alfqh,vol.3:p222

(6)Allama Zarkshi, Dqaiq ala alnha l sherh Almntha Al Meroof B Sher Muntha.vol,2:p7

(7)Encyclopedia of Jurisprudence,vol.14:p9

(8)Ashraf Ali Thanvi,Imdad ul Alftawa,vol.4:p498

(9)Muhammad Taqi Osmani,Fiqh Al buooe ela Mzahib Al-Arbeh,vol,1:p27

Virtual currencies are created, but virtual currencies are not real assets and they are often used in prohibited matters (smuggling, betting). It is related to two external factors.

One: Dollars. A global currency that has the status of an alias.

Second: What is the market value of the currency of the country in which it is being used, because the virtual currency is converted into the currency of that country and used.

In these ways the value of virtual currency comes into being. And just as dollar, riyal, rupee have personal face value, virtual currency face value is not personal. When virtual currency has no value of its own, how can it become a property?

Virtual currency as seller:

The history of keeping human assets is very old. Man has been accumulating more wealth than his losses in his life. He has been saving these assets in different forms. These assets include rides, jewellery, dirhams, dinars, currency, gold, agricultural land, houses, their implements and other commodities, and in the two present cases where material and tangible assets are included, intangible assets are included. or intangible assets, including images, online articles, videos, speeches, etc. Man sells them when necessary. There are four types of wealth.

1- Real estate and non-real estate.
2- Allowed wealth and forbidden wealth.
3- Homosexual and valuable.
4- consumables. (1)

Property or assets and their forms:

Assets are of two types. 1- Existential. 2- Material

Existential assets refer to those assets that have a physical existence, and they are of two types.

1-Fungible Assets.

2.Non-Fungible Assets.

Fungible assets:

They are those that are similar and easily exchangeable if the quantity and type of these assets are the same, eg minerals, metals (gold, silver) and physical currency as finable assets. are seen. These assets are also called tangible assets.

Tangible assets refer to assets that exist in one form or another. That is, those assets or wealth that have value and attributes.

There are four methods of estimating the value of fungible assets.

1- Weight: Goods that are sold and bought by weighing are called weighted property like gold and silver.

2- Measurement: The property sold and bought by measurement is called measurable property. Like wheat, barley and dates are measurable properties.

3- Rod Meter: The property which is sold and bought as clothes by rod meter and scale.

4- Counting: The property which is sold and bought by counting dozens like eggs, bananas and sold by counting them (minor).

Non-Fungible Assets:

Assets whose financial value is not equal to each other, rather such assets have a special individual status. Its value is very specific to it, e.g. a diamond will be of a particular cut and cannot be exchanged with any other diamond, real estate (house, property etc.), diamond Fin gable assets count.

Intangible assets

Intangible assets refer to assets that are not physically present. For example video, audio, image, jpeg image, document or cryptocurrency and these digital assets etc.

These assets have as much financial value as tangible assets, these assets can be owned by a

(1)Dr.Wahba Zouhili,Fiqh Al Islami,vol4:p624

single person and can be held by several people in partnership. Also these assets can be bought and sold. Under the Law of Inheritance (Ilm al-Farayz), the assets of a deceased person are transferred to his heirs.

Along with this, these assets are transferred for sale and partnership. The method of buying and selling of virtual assets is different and there is a separate virtual market for it.