SHARIAH WHITE PAPER ON ETHER

AMANIE ADVISORS

&

ETHEREUM FOUNDATION

Ethereum Foundation

The Ethereum Foundation is a non-profit Swiss "Stiftung" (Foundation) registered in Switzerland as "Stiftung Ethereum" (Foundation Ethereum). **The Foundation's mission** is to promote and support Ethereum platform and base layer research, development and education to bring decentralized protocols and tools to the world that empower developers to produce next generation decentralized applications and together build a more globally accessible, more free and more trustworthy Internet.

Amanie Advisors

Amanie Advisors has become a leading global brand in the Islamic Finance industry since 2005 with offices strategically located worldwide in leading and emerging markets such as in Malaysia, Dubai, Kazakhstan, Oman, and Morocco. It is a leading ambassador for Islamic finance and often is the first entity in new markets creating a dialogue with the various government and corporate entities. Amanie was founded by Dr. Mohd Daud Bakar, a prominent international Shariah scholar and Shariah entrepreneur, who has developed an innovative model of providing cutting edge Islamic Finance consultancy services on a truly global basis from its hubs in the Dubai International Financial Centre (DIFC) via Amanie Advisors LLC and Kuala Lumpur via Amanie Advisors Sdn Bhd (together 'Amanie'); making it the first Shariah Advisory firm established as a global company that was also founded and managed by the Shariah scholar himself, thereby providing first-hand Shariah knowledge and expertise. Amanie is teamed by professionals and subject matter experts from various backgrounds such as Shariah, legal, risk, accounting, finance, investment, IT etc., with a strong position to provide holistic advisory services.

Anchoring the firm's work is the Amanie Shariah Supervisory Board ("SSB") which provides guidance to the team. The SSB comprises of four globally renowned scholars comprising, Dr. Mohamed Ali Elgari (Saudi Arabia) - Chairman; Dr Mohd Daud Bakar (Malaysia); Dr. Muhammad Amin Ali Qattan (Kuwait); and Dr. Osama Al-Dereai (Qatar).

Table of Content

1. Introduction and Preamble 4
2. Objective Statement 6
3. **Part A – Technical Analysis**
    I. Cryptography 8
    II. Blockchain 9
    III. Ethereum 10
    IV. Smart Contract 12
    V. Ether 14
    VI. Ethereum Tokens 17
    VII. Example of Decentralized Applications and Tokens 20
4. **Part B – Shariah Analysis**
    I. Status of Ether 22
        i. Money in Islam 22
        ii. Functions of Money 23
        iii. Types of Money 24
        iv. Ether – Currency or Commodity? 26
        v. Ether as Shariah Compliant Asset 27
    II. Shariah Opinion on Ethereum Network and Smart Contract 30
        i. Ethereum Network 30
        ii. Decentralized Applications and Smart Contract 30
    III. Shariah Opinion on Mining Process 34
        i. Proof-of-Work 34
        ii. Proof-of-Stake 35
5. Conclusion 38

APPENDIX I– Letter from Virgil Griffith, Research Scientist of Ethereum Foundation

APPENDIX II – Shariah Endorsement on the Shariah White Paper by Amanie Shariah Supervisory Board

INTRODUCTION AND PREAMBLE

It has been more than a decade since the naissance of the Bitcoin as the first cryptocurrency in late 2008 which has seen unprecedented series of volatile ups-and-downs in its price. Other cryptocurrencies followed suit with different ideas and purposes; and to a certain extent, with different types of technologies and capabilities as well. Ethereum came into the industry in 2014 when the first whitepaper was published and subsequently went live in 2015, with the goal to create a *universal computer,* using technology which allows the users to develop decentralized applications and smart contracts on the network – a major milestone in the cryptocurrency and blockchain space. The Ethereum platform is now widely known for hosting most of the Initial Coin Offerings (ICO) projects thus far, which has allowed a wide range of applications to be built on the network. The boom in this aspect over the recent years led to a wider adoption and awareness of cryptocurrency and blockchain in general.

Its native coin, Ether, although designed to serve specific purposes to the network, is sometimes treated in the same way as Bitcoin and other cryptocurrencies by some people with focus only being directed to its daily value and price in the market.

Despite the volatility aspect of cryptocurrencies in relation to their prices, it will be only appropriate and logical to undertake a serious look into the DNA and the very function and behaviour of a cryptocurrency as the market sentiment is not a permanent feature. In the space of the Shariah, the market movement or market risk is not a relevant and impactful element to render something permissible or otherwise, unless it comes under the purview of uncertainty *(gharar)* or gambling *(maysir).* While the research in the legal and regulatory aspect is still on going with the majority of jurisdictions remain indecisive over the appropriate regulations to be put in place, the Islamic community is facing uncertainty over the Shariah compliance aspect of the cryptocurrency.

Some scholars and Islamic institutions have attempted to conduct researches on Bitcoin and issued Shariah rulings based on their interpretation and understandings which so far has seen various opinions ranging from favourable approval to outright rejection. However not much attempt has been done on other cryptocurrencies including Ether, although the Ethereum platform itself has the largest global community of developers. This is discouraging to say the least because blockchain has evolved far more beyond Bitcoin with the evolution of the technology going at unprecedented pace with endless potential to disrupt different sort of sectors and industries.

In October 2017, Virgil Griffith, Research Scientist of Ethereum Foundation published an article entitled "Ether is more Halal than Bitcoin"[1], which has attracted a lot of interests from

[1] Virgil Griffith, *Ether is more Halal than Bitcoin* – Link: https://medium.com/@virgilgr/eth-more-halal-than-btc-c2a2ee2d8d3d

the public. In the attempt to understand further the Islamic finance requirement and opinion in relation to cryptocurrency subject especially on Ether, he reached out to Amanie Advisors. After a series of discussion, the parties agreed to start collaboration and doing research together for the purpose of establishing a guideline and parameter to the Islamic finance market on Ether as a cryptocurrency.

Amanie Advisors has had a meeting with the Ethereum Foundation represented by Virgil Griffith, Tju Liang and blockchain advisor, Atif Yaqub in Singapore in July 2018 to discuss among others the scope and objective of research, briefing on the technological aspect of blockchain, Ethereum platform and Ether, and some preliminary Shariah thoughts from Dr. Mohd Daud Bakar who is the Executive Chairman and Member of the Shariah Board of Amanie Advisors, accompanied by Wan Hafizi Halim, a Consultant of Amanie Advisors. Another session of extensive meeting and intensive crash course on blockchain covering mainly Ethereum platform and smart contract technicalities was held in Dubai in September 2018 led by Atif Yaqub.

Dr. Mohd Daud Bakar and Wan Hafizi Halim had also attended the Devcon4 event, the largest annual gathering of Ethereum developers in Prague on 30th October to 2nd November 2018 where they authored and presented a session titled "Is Ethereum Compatible With Islamic Finance?". Dr. Mohd Daud Bakar elaborated briefly some of the key issues and provided insights on the subject, as parts of the findings from this research[2]. A series of follow up discussions between the parties has taken place since then which has led to the publication of the final outcome in the form of the Shariah white paper.

The paper is structured in two major parts: Part A which covers the technical overview on the subject of cryptography, blockchain, Ethereum platform, Ether and smart contracts, amongst others; and Part B is dedicated for the Shariah analysis based on the research and findings from the technical overview in the earlier Part A.

[2] The presentation is now accessible in Youtube – Link: https://www.youtube.com/watch?v=RElU07fmecI

OBJECTIVE STATEMENT

The main objective of the paper is to outline the Shariah parameters of Ether, the cryptocurrency of Ethereum platform based on the extensive research on the subject from the perspective of Shariah and Islamic finance industry. As with other cryptocurrencies, there are uncertainties especially from the Islamic community whether it is permissible for them to get involved in the space either in the mining or trading aspect of Ether or in the development of smart contract and decentralized applications.

The hypothesis prior to the research was that if Ether as the native cryptocurrency of the platform is deemed permissible or in a more friendly terminology in the Islamic finance community – "Shariah-compliant", then the public shall be more confident and assured to be more active in participating in the development of Shariah compliant smart contracts and decentralized applications which is now still lagging behind. It is hoped that with the findings, parameters and guideline outlined in this paper, it would serve as a catalyst to the Islamic finance market, and wider Muslim population to enter and participate in the space as well.

As described earlier, the paper is structured in two parts, namely Part A – Technical Overview; and Part B – Shariah Analysis.

Part A – Technical Overview - Although the initial research was to focus on Ether as the cryptocurrency, it is only logical to also discuss other pertinent topics which provide the underlying foundation to the birth of cryptocurrencies which are cryptography, blockchain, and the Ethereum platform without which Ether would be a meaningless token. The paper will also discuss the product of the platform which is decentralized application and smart contract to complete the technical overview part.

It is worth to highlight that the paper shall not attempt to go into the very detail discussion on each topic, as this is not meant to be an advanced technical manual and guideline for the blockchain experts, but at the same time it will not scratch only the surface because the intention is to cover at the very least the key salient features which is relevant for the understanding to the Islamic finance community and for the purpose of Shariah elaboration and deliberation. The order of topics and sub-topics sometimes follow the questions that were raised by Amanie Advisors during the research stage and later on answered by the Ethereum Foundation. A letter from Virgil Griffith to clarify some basic questions that were highlighted during the early engagement is attached herein as Appendix.

Part B – Shariah Analysis – This part will cover the discussion and analysis of the technology covered in Part A especially Ether as the main subject of the research, from the Shariah perspective. The paper shall start discussing the concept of money in Islam and some pertinent rules related to money, followed suit by the discussion on whether or not Ether fits the criteria to be considered as currency. The subsequent topic shall discuss whether Ether is

a Shariah-compliant asset in Islam by looking at the definition and concept of wealth from Shariah perspective. The next topic will provide brief guidelines of Shariah compliant smart contracts and decentralized applications. The Shariah analysis will also discuss briefly on the mining aspect of the platform, whether the concept of Proof-of-Work protocol and the upcoming Proof-of-Stake are in line with the Shariah principle.

As a general guideline, in Part B – Shariah Analysis, the paper will maintain some Arabic terminologies which are commonly used in the Islamic finance space such as *riba, ribawi, gharar, zakat,* etc. in *italic* forms, but a brief definition and description will be provided where required.

PART A – TECHNICAL ANALYSIS

Ether, and to a large extent Ethereum, are the by-products of the technological breakthrough achieved using the blockchain concept combined with the cryptography. Therefore it is logical to discuss first and foremost these subjects before we delve into the subject of Ether.

I. CRYPTOGRAPHY

Ether, as with majority of other cryptocurrencies in the market, is essentially built upon cryptography and blockchain.

Cryptography is the science of communicating securely in the presence of adversaries, who can listen in and even control the communication channel[3]. It can be simplified as the method of encryption to disguise and reveal a message (encrypt and decrypt) through complex mathematics. The purpose of encryption is to ensure the message can only be viewed and understood by the recipients and nobody else.

The encryption is the process of converting ordinary information, called *plaintext*, into unintelligible form called *ciphertext.* Decryption is the reverse process, in other words, moving from the unintelligible ciphertext back to plaintext. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret information, which is needed to decrypt the ciphertext[4].

Most of the early work in cryptography was done on the symmetric-key basis as described. A very early example of symmetric- cryptography is commonly known as Caesar's cipher[5], which was allegedly used by Julius Caesar to communicate with his generals to protect Roman military secrets. The method involved substituting each letter in the message with another letter obtained by shifting three spaces to the left. For example the letter Z is replaced by W, D is replaced by A, so on and so forth. This information is the secret key to decrypt the message.

Modern cryptography works on the same level and concept, albeit with far greater levels of complexity using advanced mathematical algorithms. The cryptography concept was essentially proposed by Satoshi Nakamoto in his white paper for Bitcoin as a tool and proof to allow any two willing parties to transact directly with each other without the need for a trusted third party[6].

---

[3] Pedro Franco*, Understanding Bitcoin (2015)*, pp. 51.
[4] See Wikipedia, *Cryptography* – Link: https://en.wikipedia.org/wiki/Cryptography
[5] Pedro Franco, Ibid. 1, pp. 51-52.
[6] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* – Link: http://www.bitcoin.org/bitcoin.pdf

Encryption is used to protect certain information, which implies that there are parties who are interested to obtain the information, or in this case *crack* the code. As people have tried and succeeded in cracking various encrypted codes, cryptography has been forced to evolve and adapt with all sort of potential attacks. The advent of computer technology today has allowed the encryption difficulty to increase drastically. Cracking an encryption involves a simple process of trial and error, and by trying all possibilities available the method is known in modern terminology as *brute force*.

In summary, the current level of difficulty used in the modern cryptography which is adopted by many blockchain including Ethereum is very high making it almost impossible to crack due to lack of existing computational power and technology. This has made cryptography an essential feature used of the blockchain technology.

II. BLOCKCHAIN

Blockchain is a new term coined by the internet community to the new technology of decentralized and distributed digital ledger in which transactions are recorded chronologically. It is a concept which was first proposed in the white paper written and published by Satoshi Nakamoto in 2008. It is used as the underlying protocol of Bitcoin and later on adopted by many of other cryptocurrencies as well. The main breakthrough of the blockchain technology was on solving the "double spending" issue which had been a big challenge in other previous digital cash projects[7].

It is originally called "block" and "chain" because of its nature where a list of transactions are recorded in *blocks* which are then linked and *chained* with another block using cryptography. A distributed ledger means that the blockchain is managed by a peer-to-peer network adhering to the same protocol. The network of computers running the blockchain is called *nodes* which perform the task of validating and relaying transactions in the blockchain. Briefly, a node is an electronic device connected to the internet which may include a computer, mobile phone, tablet, etc. that has the role of supporting the network by maintaining a copy of a blockchain and to process transactions.

The other main feature of blockchain is the concept of decentralization. Any transaction happening on the blockchain will be copied and recorded in a transparent way which is safely stored in all the nodes running the blockchain. It is like a public database managed by a global network of computers which means that it is almost impossible to hack or corrupt due to its distributed feature.

The original white paper was published to the Cryptography mailing list which is now archived here: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

[7] Double-spending is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once – Source: https://en.wikipedia.org/wiki/Double-spending

The Ethereum documents summarize the definition of blockchain as follow:

"A blockchain is a distributed computing architecture where every network node executes and records the same transactions, which are grouped into blocks. Only one block can be added at a time, and every block contains a mathematical proof that verifies that it follows in sequence from the previous block. In this way, the blockchain's "distributed database" is kept in consensus across the whole network."[8]

The basic concept of a transaction happening on a publicly distributed and decentralized blockchain is illustrated over here:-

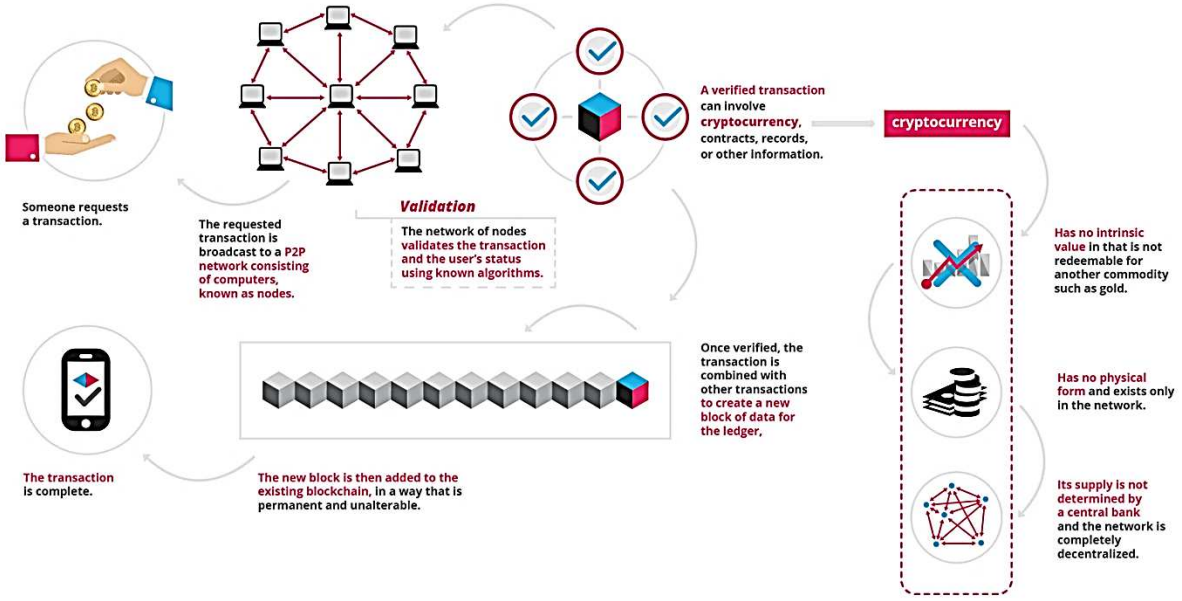

Image Source: Blockgeeks[9]

III. ETHEREUM

The Ethereum is described in the Ethereum Homestead documentation as follow:-

"Ethereum is an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology. Like Bitcoin, no one controls or owns Ethereum – it is an open-source project built by many people around the world. But unlike the Bitcoin protocol, Ethereum was designed to be adaptable and flexible."[10]

[8] Ethdocs, *What is Ethereum* – Link: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html
[9] Blockgeeks, *What is Blockchain Technology* – Link: https://blockgeeks.com/guides/what-is-blockchain-technology/
[10] Ethdocs, Ibid.

Ethereum is an "open-source"[11], public, blockchain based distributed computing platform and operating system featuring smart contract functionality. The purpose of the Ethereum platform is to serve as a base layer upon which people can build a variety of decentralized or sometimes referred to as distributed applications[12], and smart contracts, so as to enable the full potential of blockchain based applications. More information about smart contract will be described later. Ethereum envisages of becoming the *"universal computer"* which does not belong to anyone but can be used by everyone.

Ethereum was created by Vitalik Buterin, a programmer from Toronto. He published a white paper in 2013 describing an alternative platform designed for any type of decentralized application developers would want to build[13]. His idea received many interests and tractions among the public. Dr Gavin Wood, Co-Founder of Ethereum wrote the Ethereum yellow paper to elaborate the technical details and specification of the platform[14]. To get the project off the ground, he and other founders launched a crowdfunding sale in July 2014 where participants purchased Ether which is the Ethereum tokens in what was described as the first Initial Coin Offering (ICO). Raising more than $18m, it was used mainly to fund the project development and now managed by Ethereum Foundation, a non-profit entity based in Switzerland[15].

In the conclusion section of the white paper, it reads:-

The Ethereum protocol was originally conceived as an upgraded version of a cryptocurrency, providing advanced features such as on-blockchain escrow, withdrawal limits, financial contracts, gambling[16] markets and the like via a highly generalized programming language. The Ethereum protocol would not "support" any of the applications directly, but the existence of a Turing-complete programming language means that arbitrary contracts can theoretically be created for any transaction type or application. What is more interesting about Ethereum, however, is that the Ethereum protocol moves far beyond just currency. Protocols around decentralized file storage, decentralized computation and decentralized prediction markets, among dozens of other such concepts, have the potential to substantially increase the

[11] The term "open-source" refers to the program whose source code is made available for use or modification as users or other developers see fit. An open-source program is usually developed by public collaboration and it is made freely available. Examples of other popular open-source software are Mozilla's Firefox web browser, PHP scripting language and Bitcoin.

[12] The abbreviation form used in the blockchain community is DApps, but the paper will maintain the standard terminology of decentralized application throughout the document for standardization purpose.

[13] See *A Next-Generation Smart Contract and Decentralized Application Platform (Ethereum White Paper)* - https://github.com/ethereum/wiki/wiki/White-Paper

[14] See *Ethereum: A Secure Decentralized Generalized Transaction Ledger (Ethereum Yellow Paper)* - https://ethereum.github.io/yellowpaper/paper.pdf

[15] Coindesk, *Who Created Ethereum* – Link: https://www.coindesk.com/information/who-created-ethereum/

[16] Disclaimer: "Gambling" is identified in general context as one of the industries which may benefit from the Ethereum technology according to its founder. It does not mean that it is the main objective or purpose of the creation of Ethereum. The paper will provide further elaboration in Part B on the requirements for a Shariah compliant smart contract which must avoid *inter alia* the gambling element which is prohibited in the Islamic law.

efficiency of the computational industry, and provide a massive boost to other peer-to-peer protocols by adding for the first time an economic layer. Finally, there is also a substantial array of applications that have nothing to do with money at all.

The concept of an arbitrary state transition function as implemented by the Ethereum protocol provides for a platform with unique potential; rather than being a closed-ended, single-purpose protocol intended for a specific array of applications in data storage, gambling or finance, Ethereum is open-ended by design, and we believe that it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols in the years to come.

IV. SMART CONTRACT

Ethereum is currently based on the same public distributed blockchain technology used in Bitcoin with minor differences in terms of how the protocol is configured, and adds the capability of executing certain programming codes of Turing-complete language. Because of this additional advanced feature, Ethereum can also be described as a transaction-based *state machine*. In computer science, a state machine is defined as something capable of reading a series of inputs and transitioning to a new state based on those inputs. When a certain transactions are executed, the machine then transitions into another state[17]. This feature makes it easy for developers to build variety of self-executing decentralized applications, or smart contracts.

Essentially, a smart contract consists of a set of mechanistic triggerable operations in the form of *"IF-THEN"* statements. The *IF* statements can be any other event on the platform, and the *THEN* operation can be of certain specific actions which have already been setup and programmed into the code such as transferring Ether, or transferring ownership of digital assets, etc.

Effectively, smart contracts can function as digital versions of traditional contracts set between any parties, but without the need to have independent third party verification. The verification and validation tasks are handled instead by the Ethereum platform itself. Such mechanics works in the "trustless" environment, hence the reason it is popularly dubbed as smart contract, a contract which has the self-executing and self-validating ability. Smart contracts have the ability to be programmed to run various scripts and are open to be coded the way user would like to deploy set of functions.

In summary, a smart contract offers the following features:-

[17] Cointelegraph, *What is Ethereum* – Link: https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum/

- *Autonomy* — Smart contracts will offer the autonomy to the user over the control of the agreement or contract because there is no requirement to have a third-party intermediary.

- *Reliable*— The concept of decentralization combined with the cryptography will ensure trust to the network because the information and data are encrypted and safely stored in distributed and shared ledger.

- *Safety & Security* — The user will be assured that the information and transactions conducted with the smart contracts are safe and secured because the network implement complex cryptography that is almost impossible to hack.

- *Cost Effective* — By replacing the role of intermediaries thanks to the nature of smart contracts which are self-executing and self-validating, entering into a contract or transaction will be more cost effective to the parties.

- *Efficiency* — Smart contracts will help to save a lot of time, normally wasted on manually processing heaps of paper documents, sending or transporting them to specific places, etc.

V. ETHER

The decentralization nature of blockchain means that the Ethereum platform is not owned or governed by any single authority. It is the main importance of the blockchain which ensures its transparency and security. This functionality however is not free. The system needs a mechanism to provide incentives to the network or nodes which support the platform.

For this reason, Ethereum platform is designed with a reward mechanism by issuing and distributing tokens to the nodes which perform the task of validating and relaying the transactions on the blockchain. The token is called Ether, and the process of validating the transactions on the blockchain is called "mining", hence the nodes are sometimes referred to as "miners". More information about mining will be described later.

Ether[18] is the internal currency for the Ethereum platform, and its sole purpose is to compensate miners for verifying the accuracy of the transactions and processing updates on the Ethereum ledger. Because miners are the nodes which perform the task and execute the transactions on the blockchain, it can also be implied that Ether is the token used to fuel or activate the decentralized application or smart contract which generally contains variety of task and actions. Depending on the complexity of a particular decentralized application or smart contract, the number of Ether required will usually be adjusted proportionately.

The compensation amount by operations on the Ethereum platform is priced in units of *gas*. For example, in each Ethereum transaction, the sender has to specify, "I will offer N units of Ether per gas consumed", and if this amount is accepted by the miners, the transaction is processed. Depending on the value of the Ether at a particular time, the users will have the opportunity to bid different amounts of Ether to pay for their gas requirements accordingly to compensate the miners to perform his transaction.

Gas is the name for the execution fee that senders of transactions need to pay for every operation made on an Ethereum blockchain. The name gas is inspired by the view that this fee acts as cryptofuel, driving the motion of smart contracts[19]. Gas costs are paid with small amounts of Ether. Another reason it is called gas although payable in Ether is to ensure a separation between the price of computational work and the highly volatile price of Ether token which is publicly traded on cryptocurrency exchanges[20].

The correlation between Ether and smart contract is better illustrated in the following popular example of a vending machine:-

[18] The abbreviation form is ETH, but the paper will maintain and use the terminology Ether throughout the document for standardization purpose.
[19] Ethdocs, *Account Types, Gas and Transactions* – Link: http://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html
[20] Chris Dannen, *Introducing Ethereum and Solidity (2017),* pp. 59.

Image Source: Cointelegraph[21]

A vending machine is an automated machine designed to perform specific task, without a third party interference and validation. A customer simply puts the correct amount of money and select item(s) he wishes to purchase and the vending machine will perform the task automatically.

In smart contract application, Ether is required as a token to perform a specific task of that particular transaction. ERC20 in the illustration above is the token concept which represents the smart contract application. More information on ERC20 will be described later.

Therefore in summary, Ether is used mainly for the following purposes:-

- From the perspective of user – Ether is used as the transaction fee to compensate the miners to perform the requested transaction e.g. to activate a certain function in decentralized application or simply to send N number of Ether to another party (which is also a transaction happening on the blockchain).

- From the perspective of miner – Ether is essential as the reward token to incentivise the miners to keep supporting and performing the task e.g. validating and relaying the transaction on the blockchain.

[21] Cointelegraph, *ERC20 Tokens Explained* – Link: https://cointelegraph.com/explained/erc-20-tokens-explained

Issuance of Ether

There are over 100 million Ethers in free circulation to date. At the time of writing the paper, new blocks created and added to the blockchain (or simply called "mined") will be rewarded with 2 ETH, and the process will take approximately 14 seconds. The issuance of Ether is therefore done automatically by the platform. There is no single authority who "decides" the creation of Ether, nor can any one individual manipulate the network to generate more Ether. There is no maximum cap of Ether, however the issuance protocol is designed based on deflationary concept as to avoid the speculation and price manipulation of Ether. Deflationary in this context means that the number of Ether created per block mined on the blockchain will gradually decrease as the network grows.

Valuation of Ether

As noted above, the Ethereum platform automatically creates new Ether according to the rate of issuance at a particular time. Because the rate of such creation is fixed based on publicly known rules, and because no individual can control or change such rate, no one controls the rate of generation of new Ether. This is as opposed to fiat currencies where the government or central bank controls the money supply and interest rates, therefore indirectly controlling the price of such fiat currency. As a result, the price of Ether is determined solely by supply and demand in the market.

Legal Status of Ether

The US Securities Commission (SEC) recently set out their analysis of how to determine if a cryptocurrency is a security, and their determination that Ether token does not fall into the category of a security. William Hinman, Director, Division of Corporation Finance said during the Yahoo Finance All Markets Summit: Crypto:-

"… And putting aside the fundraising that accompanied the creation of Ether, based on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether ***are not securities transactions****. And, as with Bitcoin, applying the disclosure regime of the federal securities laws to current transactions in Ether would seem to add little value."*[22]

This is in fact in line with the nature of Ether which functions only within the specific scopes as described earlier on the Ethereum network.

[22] William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic)* – Link: https://www.sec.gov/news/speech/speech-hinman-061418

VI. ETHEREUM TOKENS

As discussed earlier, smart contract consists of a set of mechanistic trigger-able operations in the form of *IF-THEN* statements. Each smart contract is usually represented by a particular token (although this is not always the case because there are smart contracts which do not issue separate tokens) containing the necessary information and instructions as defined by the contract creator. A token is simply a unit of value and a simple representation of a particular smart contract application.

It has to be noted that Ethereum tokens are not the same as Ether. While Ether is the main cryptocurrency of the Ethereum platform and has its specific utilities and functions as described earlier, Ethereum tokens are created at the discretion of the smart contract or the decentralized application developers. Thus, Ethereum tokens may serve different functions and purposes according to specified intended objectives.

There are in general three types of Ethereum tokens which are commonly used in the blockchain, namely equity token, security token and utility token[23].

- *Equity token* – Also sometimes referred to as asset token, equity token represents ownership of an asset. Such token can be used to replace the concept of company stock where shareholders of a company will hold equity tokens instead of the standard paper contract. Stock trading can be made more accessible to average investor and the corporate governance process can be conducted in a more transparent way using blockchain.

- *Security token* – According to the US Securities Commission (SEC), a token is classified as a security token if it represents an investment contract. A transaction will be deemed as investment contract if it fulfils the following criteria[24]:-
  - It is an investment of money;
  - The investment is in a common enterprise[25]; and
  - There is an expectation of profit from the work of the promoters or a third party.

  A token which meets all the above criteria will be deemed as security token and therefore is subject to all securities laws and regulations.

- *Utility token* – As the name suggests, utility token refers to a token which serves one or several utilities as defined by the token creator. It usually provides the token holders access to a product or service. The majority of tokens issued today on the Ethereum blockchain fall under the category of utility token.

[23] Strategic Coin, *3 Types of ICO Token* – Link: https://strategiccoin.com/3-types-ico-tokens/
[24] Blockgeeks, *Security Token* – Link: https://blockgeeks.com/guides/security-tokens/
[25] Common enterprise is defined as a horizontal enterprise where the investors pool in their money and assets to invest in a project.

As a summary, it can be concluded that a token issued together with smart contracts on the Ethereum platform can therefore be classified into one (or several) of the categories described earlier. An Ethereum token can either represent i) an ownership of an asset (Equity token); ii) a Security token which represents an investment instrument; or iii) a Utility token which has certain utility functions as defined by the token creator or smart contract creator.

Tokens are usually used for the purpose of fund raising for a certain project or business activity where the creator distributes the tokens to their investors during a public sale. The process has now been known to the public as Initial Coin Offering (ICO).

It is not an absolute requirement to issue token when creating a smart contract. Some developers may just use Ether as native token to perform the task as defined by the smart contract. It means that a smart contract can still function and be executed using simply Ether without the need to have any Ethereum token to be issued. However, since a token to a certain extent can be used as a representative of smart contract functionalities, the majority of smart contracts will usually issue a separate token which is operated and transferred through the Ethereum network. Because many tokens are issued by the creator via ICO process, most of the tokens will have its own value and is traded as a standalone token in public cryptocurrencies exchanges[26]. This has resulted in Ethereum tokens, when they are combined together with Ether, become the biggest cryptocurrency by market capitalization surpassing the value of Bitcoin and other cryptocurrencies.

There are two types of token commonly used and issued on the Ethereum network to date namely ERC20 and ERC 721 tokens. Other types of token standards are constantly being developed and proposed to the community; however they still remain the minority and lack of the adoption in the current market.

ERC20 token

ERC20 tokens are what most decentralized application and smart contracts issued on the network use. Introduced in 2015, the ERC20 code outlines a specific list of rules that a given Ethereum based token has to deploy, simplifying the process of programming the functions of tokens on Ethereum blockchain[27]. It is a standardized form of token which has simplified the process of creation and issuing a token to Ethereum blockchain. The ERC20 standard also made it easy for the cryptocurrency exchanges to list various tokens on their trading platform according to the uniform set of rules.

[26] Cryptocurrencies exchanges are websites where the public can buy, sell or exchange cryptocurrencies for other digital currency or traditional fiat currency e.g. US Dollar.
[27] Cointelligence, *Comparing ERC20, ERC223, and the new Ethereum ERC777 token standard* – Link: https://www.cointelligence.com/content/comparison-erc20-erc223-new-ethereum-erc777-token-standard/

ERC20 is the first standardized form of tokens issued by Ethereum platform. As such, several technical issues and flaws have been discovered by the community of users over the time. There are currently on-going discussions and several efforts to introduce new sets of rules for the issuance of the tokens in the future. Regardless of the standards adopted by the users, the main concept and features of tokens remain intact as discussed earlier.

ERC721 Token

There is another form of token under the category of ERC721 which in brief is a token that is "non-fungible". This basically means that each token is completely unique and non-interchangeable with other tokens. It is mostly used for smart contract to define ownership of a specific item or object e.g. collectibles, education certificate, a pet, etc. For example, a smart contract which is used as a database of a college degree of its student, or a Shariah endorsement (*fatwa*) as in the case of Islamic finance industry - the token based on ERC721 is a better type of token where each token can be used as a unique representation of each student's degree certificate or fatwa.

VII. EXAMPLE OF DECENTRALIZED APPLICATIONS AND TOKENS

At the time of writing the paper, there are around 120,000 smart contracts based on ERC20 token[28] and around 200 based on ERC721[29]. Due to the nature of Ethereum as a fully decentralized public blockchain, anyone can build and deploy smart contract on the platform. There is no centralized platform of repository which tracks or stores all of the information about every decentralized application or smart contract on the blockchain. There are however several independent websites which provide the list of popular decentralized application such as *DAppRadar*[30] and *State of the DApps*[31].

For the purpose of this paper and better understanding of how a smart contract works, we will briefly take a look at several smart contracts and tokens as sample case studies.

a. **Bancor**[32]

Bancor is a blockchain protocol that allows users to convert between different ERC20 tokens directly as opposed to exchanging them on cryptocurrency markets. The project aims to solve the illiquidity as one of the major problems currently faced by the majority of cryptocurrencies including ERC20 tokens. Bancor's protocol uses smart contract to create Smart Tokens by using its own ERC20 token called Bancor Network Token (BNT). The Smart Token is akin to a central bank holding foreign currency reserves, where in this case it actually holds reserves of all tokens issued based on the ERC20 standard. The Smart Token essentially removes the needs to match the order between buyers and sellers. Instead, the conversion can occur directly through smart contracts on the network.

b. **Binance**[33]

Binance is the biggest cryptocurrency exchange in the world. Binance launched its own ERC20 token called Binance Coin (BNB) in July 2017 as a utility token. BNB allows the token holder to enjoy discounts on the trading fees when trading cryptocurrency on the exchange. Although BNB is primarily a utility token, it is also being traded in the open market and therefore has its own value.

[28] Etherscan, *Token Tracker* – Link: https://etherscan.io/tokens *(Last accessed: 2/10/2018)*
[29] Etherscan, *ERC-721 (NFT) Token Tracker* – Link: https://etherscan.io/tokens-nft *(Last accessed: 2/10/2018)*
[30] DappRadar – Link: https://dappradar.com/
[31] State of the Dapps – Link: https://www.stateofthedapps.com/
[32] Bancor – Link: https://www.bancor.network/
[33] Binance – Link: https://www.binance.com/en

c. **tZERO**[34]

tZERO is one of the portfolio companies of Overstock, an American online retailer. tZERO launched an ICO in December 2017 to fund the development of a licensed security token trading platform. The platform is envisaged to make securities lending activities of the users compliant, more transparent and more efficient from both cost and operational perspective. The tZERO token was issued in accordance with US SEC regulations because of its nature as a security token. It was announced that each tZERO token holder will be entitled to receive quarterly dividend from the profit generated by the company. The ICO has managed to raise $134 million from the investors[35].

d. **Hellogold Token and GOLDX**[36]

Hellogold Foundation is an entity established and registered in Singapore. As part of the foundation objectives to support blockchain technology, it tokenizes the physical allocated gold received as an endowment from Hellogold Sdn Bhd, which is an online gold retailer based in Malaysia. The gold-backed token is called GOLDX, where each GOLDX represents 1g of physical allocated gold safely vaulted by the foundation.

The foundation has issued another ERC20 token called Hellogold Token (HGT). HGT is a utility token which provides the holder discounts and benefits to products and services offered by Hellogold Sdn Bhd. The HGT holder may also receive the reward in the form GOLDX at the discretion of the foundation.

e. **Cryptokitties**[37]

Cryptokitties is a blockchain based virtual game developed by Axiom Zen that allows players to purchase, collect, breed and sell various types of virtual cats. It represents one of the earliest attempts to deploy blockchain technology for recreational and leisurely purposes. Cryptokitties is one of the popular examples of smart contract based on ERC721 token which means that each token is unique and generally serves as a collectible item. Each Cryptokitty in the game essentially is an ERC721 token built on the Ethereum blockchain.

[34] tZero – Link: https://www.tzero.com/
[35] Sarah Hansen, *Overstock Blockchain Subsidiary tZero Raises $134 Million in ICO* – Link: https://www.forbes.com/sites/sarahhansen/2018/08/09/overstock-blockchain-subsidiary-tzero-raises-134-million-in-ico/
[36] Hellogold – Link: https://hellogold.org/
[37] CryptoKitties – Link: https://www.cryptokitties.co/

PART B – SHARIAH ANALYSIS

I. STATUS OF ETHER FROM SHARIAH PERSPECTIVE

This section will primarily analyse the status of Ether from Shariah perspective. The terminology "cryptocurrency" is used widely as a generic label to Bitcoin, Ether and thousands of other cryptocurrencies currently available in the market. Although labelled as such, are all cryptocurrencies qualified to be deemed as valid currencies? This section will attempt to discuss the very concept of money in Islam followed by understanding the nature of Ether from the Islamic view, and the Shariah consideration and opinion on the status of Ether.

i. Money in Islam

Currency or money is a special item in Islam and requires special attention as it is deemed as one of the usurious (*ribawi*) items. This is described in detail in the following prophetic narration (hadith) reported by Ubadah Ibn al-Samit that the Prophet (peace be upon him) said:

"Gold is to be exchanged for by gold, silver by silver, wheat by wheat, barley by barley, dates by dates, and salt by salt, like for like and equal for equal, payment being made hand to hand. If these classes differ, then sell as you wish if payment is made hand to hand."[38]

In another narration reported by Abu Sa'id al-Khudri, the Prophet (peace be upon him) said:

"Gold is to be exchanged for by gold, silver by silver, wheat by wheat, barley by barley, dates by dates, salt by salt, like by like, payment being made hand to hand. He who made an addition to it, or asked for an addition, in fact dealt in usury. The receiver and the giver are equally guilty."[39]

From the above hadith, it is established that there are specific requirements mentioned by the Prophet when transacting with gold and silver, both of which are the official currency of the society at the time (and other items being the staple foods). An exchange transaction of the same items e.g. gold for gold, needs to be done on equal value and must be completed on the spot. If the exchange is between different items (e.g. gold for silver) but within the same category (i.e. currency), the value can be different but the transaction still needs to be completed on the spot.

[38] Imam Muslim, *Sahih Muslim* - 22/102
[39] Imam Muslim, Ibid. – 22/103

This is according to the following hadith by the Prophet (peace be upon him) as narrated by Abu Bakra:

"Don't sell gold for gold unless equal in weight, nor silver for silver unless equal in weight, but you could sell gold for silver or silver for gold as you like."[40]

In another hadith reported by Abu Sa'id al-Khudri, the Prophet (peace be upon him) said:

"… do not sell gold or silver that is not available during the exchange for the payment using gold or silver."[41]

It is interesting to understand such requirement which relates to how money is viewed from the Islamic perspective. In essence, Islam does not consider money to be a commodity, but rather as a medium of exchange. As such, money has no intrinsic utility. There is no room for making profit through the exchange of money in the same denomination. The profit earned through exchange of money (of the same currency or denomination) or the papers representing them is interest, and therefore is highly prohibited in Islam

Ibn Taymiyyah said that the purpose of money is to act as the unit of measurement for the wealth, and it should not be the main objective of the wealth[42]. It means that money by itself is not supposed to be useful or to generate any benefit except if it is spent or invested into real economic and productive activities to generate more value. He elaborated further that when money started being traded between each other for the purpose of generating profit, it is indeed contradicting with the nature of money[43].

Ibn Qayyim al-Jawziyyah, one of the prominent disciples of Ibn Taymiyyah, also mentioned similar opinion. He said that money is not intended for itself, but rather it is used as the medium of exchange to obtain other commodities. When money is being sought after because of its value, the human society becomes corrupted*."*[44]

ii. Functions of Money

According to Ibn Taymiyyah, Shariah in general does not specify any specific conditions or functions of a currency. It is instead left to the customs (*al-'adah*) and understanding of the people of the time[45]. However, the development of economic and financial system over the

[40] Imam al-Bukhari, *Sahih Al-Bukhari* – 34/125
[41] Imam al-Bukhari, Ibid. – 34/127
[42] Ibn Taymiyyah, *Majmu' al-Fatawa* – 29/472
[43] Ibn Taymiyyah, Ibid. – 29/473
[44] Ibn Qayyim al-Jawziyyah, *I'laam al-Muwaqqi'iin* – 2/105
[45] Ibn Taymiyyah, Ibid. – 19/252

time has allowed the people to understand the functions of money which can be summarized briefly as follow[46]:-

a. Medium of Exchange

As mentioned briefly earlier, money in essence is a medium of exchange. In this regards, anything that can be used as a medium of exchange is said to have the function of money and hence can be regarded as one. Conversely, if an object ceases to circulate in the exchange process, it ceases to be money. The perfect example for this is gold. It once played the role of money in many civilizations in the past together with silver. However it is now rarely used in making payments even though the gold value is still being used as the benchmark for the *zakat* calculation in many Islamic countries. Gold which has become jewellery or used as material in the industrial purposes is no longer considered as money.

b. Unit of Account or Measurement

Another function of money is the role as a unit of account. This is important in a market because goods and services can then be priced based on a proper monetary unit, instead of using bilateral exchange rates as in the case with the barter trading in the past. Effectively, this implies that money needs to have a certain degree of stability because it serves as the main reference for the participants in assessing the market information about the economic activity. Therefore, a volatile object is not a good unit of account.

c. Store of Value

Money needs to be a good store of value as well, because money is essentially a temporary storage of value in the exchange process. For example, if a person sells a product and receives money from the exchange, it is indeed a process of transforming the product into a monetary value. The money will then need to be transformed back into real form by exchanging it for other goods or services. In between these two transactions, money needs to be able to preserve its value to allow the person to obtain the same value back for the money that he has. This again implies that a volatile object will not be a good store of value.

iii. Types of Money

Muhammad Aslam summarized that there are generally two schools of thought in Islamic scholarship on what can be considered as money[47]:-

- Views that limit money to only gold and silver; and
- Views that do not limit money to only gold and silver.

[46] ISRA, *Islamic Financial System: Principles and Operations (2015)* – pp. 77-79

[47] Muhammad Aslam Haneeff, Emad Rafiq Barakat, *Must Money Be Limited to Only Gold and Silver?: A Survey of Fiqhi Opinions and Some Implications (2006)*

This paper will not attempt to analyse the differences between the two opinions, although it has to be highlighted that the views that do not limit money to only gold and silver is the more prevalent and the most supported view in the majority of the Muslim world including the International Islamic Fiqh Academy in Kingdom of Saudi Arabia and the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI) which is based in Bahrain.

Although the Islamic scholars might have disagreement on whether money must or must not be limited to gold and silver, they generally agree on the common attribute of money which is the medium of exchange and measure of value *(thamaniyyah).*

It has been well accepted by the people across history that gold and silver in their natural state possess value that follows their physical form, regardless of whatever happens to the world. When money was printed in the past based on gold and silver (including during the times of early Islamic history which used gold and silver pieces of the Roman empire until they were converted in the early years of the Umayyah empire to dinar and dirham), such types of money were assumed to have always had the intrinsic value. However, from the Shariah discussion regarding the *fiqh* of currency whether in the past or contemporary, there is no specific mention of the requirements of a specific currency that abides with the Shariah law to be backed by gold or other assets.

Other types of commodities beyond gold and silver can also be accepted as money when a society starts adopting them as medium of exchange e.g. shells, grains, etc. This includes the fiat money as we know it today which derives the *thamaniyyah* value from the government which issues the money. This is known in the modern context as the legal tender, which assigns value to a particular currency even though it is not backed by any type of commodity. It is accepted and acknowledged by a community at large, or a country as a currency.

Shariah recognizes the assessment based on *'uruf* or *'adah* which means the current practice and acceptance of the people, as long as they do not contradict any well-established principles of the Shariah. *'Uruf* and *'adah* are tools and techniques used by the Scholars to form a *fiqh* jurisdiction in Islam. Based on these concepts, a certain subject matter or commodity can be accepted as currency when its usage becomes dominant in affairs and dealings of the people or society at large scale. When this occurs, Shariah shall recognize the subject matter or commodity as a currency and thus shall be subjected to the standard rulings of currency trading (*bay' al-sarf*), rulings of *zakat, riba,* etc.

In the same vein, when a particular item or commodity which is used to be a currency, but for some reasons has ceased to become a medium of exchange by the general public, it will then no longer be deemed as a currency and therefore not subjected to the Shariah rulings of currency.

iv. Ether – Currency or Commodity?

The paper has earlier discussed in detail the subject of blockchain, Ethereum platform and Ether, amongst others. By analysing Ether's core function and the initial objective of its creation, Ether can be described as a utility token. It is created with specific utilities as follow:-

- From the perspective of user – Ether is used as the transaction fee to compensate the miners to perform the requested transaction e.g. to activate a certain function in decentralized application or simply to send N number of Ether to another party (which is also a transaction happening on the blockchain).

- From the perspective of miner – Ether is essential as the reward token to incentivise the miners to keep supporting and performing the task e.g. validating and relaying the transaction on the blockchain.

Unlike Bitcoin which does not have a particular function apart from being the token of the Bitcoin blockchain, Ether is the **utility token** needed to ensure the Ethereum platform is working properly and sustainable.

A good analogy for Ether and Ethereum is like a theme park which necessitates the usage of a specific token to enter into any games or attraction rides within that theme park. The usage of the token is limited only within the theme park ecosystem. Ether is similar in the sense that it is meant to be used within the Ethereum platform to perform a specific task. Beyond the platform ecosystem, Ether does not have any real-world application or function.

Ether is therefore a commodity which has certain value in the context of Ethereum ecosystem. It was not created to become a currency and thus far does not qualify to be deemed as a valid currency based on the discussions earlier especially in relation to the functions of money from the Islamic perspective.

It has to be noted in this paper that due to the decentralization nature of Ether, like many other cryptocurrencies as well e.g. Bitcoin, the value of Ether depends solely on the supply and demand of the public. Because of this aspect, as the network and platform grow, a minority segment of the public has started to perceive Ether as an alternative tool for the store of value and a replacement for cash. The utilization for this aspect is however very limited and not widely adopted yet.

Although it is something that was never intended and not in line with its original purpose, it can be argued that Shariah does not limit nor restrict the practice of barter trading for example between a commodity against another commodity. Similar analogies can be drawn upon such scenarios; bonus or reward points for credit card utilizations, travel points offered by airline companies, reloadable access card for public transportation e.g. train, which offers e-wallet feature to store a certain amount of value.

These practical examples share common feature among themselves namely being valuable asset and can be used as medium of exchange in a specific ecosystem e.g. reloadable access card for public transportation can only be used for the transportation service and nothing else - but they are not deemed as valid currency in the same class with other real money. No retailers accept these "medium of exchanges" for other types of products or services beyond its intended ecosystem and platform.

Based on our analysis and review of the concept and function of money in Islam earlier, as the practice of using Ether as a medium of exchange has not been recognized nor adopted widely by the public thus far, Ether cannot be deemed as a valid currency from the Shariah perspective and therefore would not qualify as one of the *ribawi* items. In technical terms, Ether can serve as a medium of exchange but not amounting to money or currency.

It has to be pointed out that the status may change in the future depending on the general public acceptance as discussed earlier. Therefore, there must be continuous research and engagement with Shariah scholars from time to time to constantly evaluate the position and have relevant updated Shariah rulings on the subject based on the latest development in the market.

v. Ether as a Shariah-compliant Asset

Ether, and cryptocurrencies in general are new inventions which are the results of advanced technological breakthrough of our times. It therefore requires the judgment and interpretation of the current Scholars to ascertain its Shariah-compliance status.

According to Muslim jurists, the originality in Islamic law of transactions is permissible unless there is a clear-cut prohibition. It means that when a new transaction or subject matter arises which is not known previously in Islamic law, such transaction or subject matter is deemed permissible unless there is an implication from the sources of Shariah which prohibits it whether explicitly or implicitly. This principle is in accordance with a maxim which provides that *"permissibility is the original state of things*", which is discussed under *istishab* (presumption of continuity) matters in Islamic jurisprudence.

It can be understood from this principle that any new invention such as Ether and to a larger extent Ethereum network; is by default acceptable and permissible, unless there is clear element of prohibition based on the general guideline of the Islamic law.

There are several major prohibitions according to the Islamic law such as:

a. Prohibition of *Riba*

The Arabic word of *riba means* "to grow; to increase; to grow up, to exceed, be more than..". In specific meaning, *riba* is generally translated into English as "usury" or

"interest", but from Islamic law it has a much broader sense. Briefly, usurious transactions in relation to *ribawi* items[48] as the subject matter are classified into two categories: (a) *riba al-fadl,* which is produced by the unlawful excess of one of the counter values; and (b) *riba al-nasi'ah,* which is produced by delaying completion of the exchange of the counter values, with or without an increase or a profit.

The paper has explained that Ether is construed as not being a currency and therefore does not fall into the category of *ribawi* items. There is also no element of *riba jahiliyyah* which only occurs in the event of late payment or extension of a debt as described.

b. Prohibition of *Gharar*

Gharar in Arabic means "danger". It is usually translated into English as "uncertainty, risk, speculation, hazard, jeopardy, danger, peril". *Gharar* is the uncertainty or indeterminacy involved in a transaction, for example when the quality and the quantity of the commodity on sale is not predetermined and known or simply when there is no uncertainty whether the subject matter exists at the point of sale. Similarly, *gharar* is involved when the rights and obligations of each party are not known or certain in sales or exchanges of services.

In this regard, the decentralized blockchain technology has eliminated the element of *gharar* as the existence of Ether is assured and can be verified independently by the public. At any point of time the existence of Ether can be verified using the independent blockchain explorer e.g. www.etherscan.io where each Ether is associated with a specific transaction hash at a particular address. In the transfer process of Ether from a wallet to another wallet address, it is done via cryptographic key which is almost impossible to hack; hence making the transaction is safe and secured.

c. Prohibition of *Maysir*

Maysir is originally an ancient Arabian game of chance played with arrows without heads and feathering, for stakes of slaughtered and quartered camels, which is forbidden by Quran. It is translated in general by scholars as gambling, or *qimar* ("to gamble, to bet") in Arabic. Islam prohibits any form of activity where monetary gains or profits are derived from mere chance whereby one party wins over the expense of others.

[48] *Ribawi* items are i) currency e.g. gold, silver, USD etc.; and ii) staple foods e.g. wheat, barley, dates, salt, rice etc.

The issuance of Ether follows a fixed protocol set by the network. Each transaction involving Ether is publicly verifiable and transparent. The utilization of Ether in the network is for specific purposes as described earlier which are in general to help and support the platform to function properly. There is no element of gambling associated with Ether in its natural form and standard utilisation.

In conclusion, Ether is a utility token which functions as the cryptocurrency of the Ethereum platform used by the users to execute certain codes or transactions of a particular smart contract. Ether exists in the digital form, virtually transparent and secure in the public Ethereum blockchain. It has certain value and function within the ecosystem and therefore can be considered as a valuable asset or wealth (*mal*) from Shariah perspective.

Mal in the Arabic language refers to anything which can be acquired and possessed whether in the physical form or its usufruct. By this definition, *mal* includes gold, silver, animals, plants and any benefit derived from assets such as living in house, transportation services, etc. Something which cannot be possessed cannot then be considered as *mal.* For example birds in the sky, fish in the water, and trees in forests are not *mal* as they are not in anyone's possession. *Mal* shall also include both tangible and intangible assets such as electricity and intellectual property, etc.

We have analysed earlier that Ether does not exhibit any feature which is prohibited in Islam. In fact, Ether is the main requirement of the Ethereum platform to ensure the blockchain can work and function properly as it is intended to be. It is impossible to have a decentralized blockchain platform and benefit from its vast potential disruptive capabilities without the presence of reward system such as Ether.

Therefore, Ether is a *mal* and a Shariah-compliant asset. Being Shariah-compliant implies that Ether can rightfully be tradable and exchangeable by the Muslim community. It is permissible for a Muslim to buy, sell, or hold Ether for the purpose of participating in the Ethereum blockhain and take full advantage of what the technology can and has to offer.

II. SHARIAH OPINION ON ETHEREUM NETWORK AND SMART CONTRACT

i. Ethereum Network

Ethereum is basically a decentralized platform or a network. In simple analogy, it is like a "computer" which allows the public as the users to develop their own applications or software using the protocol and programming codes set by the platform. Therefore, Ethereum itself is a technology which is lawful from Shariah perspective. This is based on the same principle as described earlier, where everything is deemed permissible unless there is a prohibition mentioned in the sources of Shariah whether explicitly or implicitly.

Shariah is therefore neutral in regards to Ethereum which functions merely as a platform. Shariah however will look at how the platform is used and for what purpose; hence this is dependent upon the type of applications or smart contracts being built upon the platform.

ii. Decentralized Application & Smart Contract

Smart contract is basically a new version of contract which adopts the technology available in our time. Contract in general is an essential part of the economic system of a society; hence Islamic law gives special protection and guidelines to contracts. The right to make and carry out contracts is fundamental to liberty and is protected by the Shariah.

"O you who believe! Perform your contracts." (Al-Maidah – 5:1)

The Shariah provides wide scopes to the subject-matter of contract, as well as the ultimate purpose of a certain contract. Islamic contracts may create, transfer, extinguish or release all kinds of rights and perform a variety of actions and transactions provided that they are in line with the Shariah principles.

With the advent of blockchain technology nowadays, the potential of Ethereum network to develop smart contract and applications is endless. The technology is powerful that allows wide-ranging smart contracts to be built on the Ethereum platform. For a smart contract to be considered Shariah-compliant, it needs to adhere to specific Shariah requirements which shall cover every aspect of smart contract including its purpose and its underlying assets or its terms and conditions. The paper will describe some of basic Shariah requirements that need to be observed.

The purpose and objective of a smart contract creation needs to first and foremost comply with the Shariah requirements. This is similar with the screening analysis of a Shariah

compliant business in the Islamic stock market where the core activity of a company must not be contradictory with the Islamic law, principles and rulings.

The following areas or sectors are prohibited in Islam, which means that a decentralized application or a smart contract including Ethereum tokens issuance must not be involved in any of prohibited activities in Islam such as gambling, alcohol, non-halal food, adult entertainment, conventional financial products and offerings, etc.

The list of sectors is non-exhaustive. And similar with other cases, there can indeed be some exceptions depending on a number of different considerations. It is important to analyse each smart contract or application on a case to case basis because different permutations may exist and the prospect of real-case applications using smart contract is enormous.

Apart from ensuring the purpose of the smart contract is in general in line with the Shariah principles and not involved in any of the prohibited activities as previously described, it is also a requirement for the nature and condition of the smart contract to be free from any prohibited element especially the major prohibitions of *riba, gharar* and *maysir.* In the earlier section the paper has elaborated briefly description of each of the prohibitions in relation to the status of Ether. Similarly for a smart contract, it also needs to ensure that it is not involved in any of these elements including other prohibitions as well:-

a. Prohibitions of riba

A smart contract must not be associated with any usurious transaction, which may arise from either dealing with *ribawi* items as the subject matter of transaction (*riba an-nasi'ah)*, or any increase or decrease in value on top of the original exchange between the parties (*riba al-fadl).* For example a smart contract with the issuance of security tokens must be structured properly to avoid any occurrence of *riba* which may exist in the form of guaranteed or fixed return for the original investment. Any investment either in the form of partnership venture *(mudarabah)* or agency investment *(wakalah)* shall not guarantee either a fixed return to the investors or capital protection of the investors' initial investment.

b. Prohibitions of gharar

Although it was mentioned that Ether by itself is free from *gharar,* this does not mean that a smart contract is also by default free from *gharar*. One of the features required in an Islamic contract is that it needs to have full transparency and full disclosure. With the nature of public blokchain which is transparent, the element of *gharar* pertaining to the subject matter of contract would not be present because the full contract and the actual programming code of

the smart contract must be disclosed and can be verified on the blockchain. However *gharar* may exist in the nature of the transaction itself, for example a smart "sale" contract is initiated to execute a transaction with uncertain outcomes. Another example is when the transaction of sale involves dealing in a subject matter which is not present or not in existence at the time of transaction. These aspects will ultimately render the transaction non permissible and thus making the smart contract not Shariah compliant by virtue of its underlying terms and conditions and its assets.

c. Prohibition of maysir

A smart contract which has the element of gambling is also not permissible in Shariah. Gambling in this context refers to an action of risking something of value on uncertain outcomes such as winning money or material goods. Islam does not prohibit a contest in general, where the participants get the equal treatment and similar chance of winning and there is no risk of value in participating it. However it will become a gambling which is prohibited when there is an element of "zero sum games" whereby the participants are winning at the expense of others. If a smart contract is developed to facilitate or provide services for gambling activities, it will not be permissible. Similarly, gambling in the context of speculating and betting against the price or value of a subject such as in the financial derivatives market is also not permissible.

d. Prohibition of fraud and deception

Fraud and deception have broad definitions. Both are indeed prohibited not only in Islam but also by all religions and modern laws and by all means not acceptable in any society. Blockchain technology has the ability to prevent fraud cases by being transparent and publicly verifiable. However fraud and deception may still exist in smart contract application. For example a smart contract with the issuance of asset backed tokens e.g. token backed by a commodity. The smart contract creator needs to ensure that there has to be specific mechanism to identify and to a certain extent to ensure "tagging" of the asset with the tokens on the blockchain. Without proper identification system and mechanism in place, it may open doors for fraud and cheating practices.

The paper has made an attempt to identify some of the important requirements to be adhered for a smart contract and decentralized applications to be considered Shariah compliant. As previously mentioned it is important for the smart contract to be analysed and evaluated from end to end perspective to ensure that it fully complies with all the necessary Shariah requirements.

It is highly recommended that the smart contract creators engage with qualified Shariah experts and advisors who can provide proper advisory function and Shariah endorsement based on their objective Shariah-based evaluation. This recommendation comes in line to complement the growing public demand to have smart contract independent security audits in the blockchain industry[49].

[49] Andrew Keys, Consensys, *18 Blockchain Predictions in 2018* – Link: https://media.consensys.net/18-predictions-for-2018-7a376ea7bd4b

III. SHARIAH OPINION ON MINING PROCESS

In the context of Ethereum blockchain technology to date, mining is essentially a process of adding blocks to the blockchain. Miners which are nodes in the network contribute their computational power to solve the blocks that are added to the blockchain, and the network remunerates them with the block reward and the fees collected from all the transactions included in the block[50].

Although the process is incentivized by the issuance of a new token, it is not the primary purpose of mining. Mining is in fact an important mechanism that is equivalent to a clearinghouse where all transactions occurring on the blockchain are validated and cleared. The concept mentioned herewith remains true and relevant based on the current protocol of Proof-of-Work algorithm used in Ethereum.

There has been growing demand among the Ethereum community to change the protocol using Proof-of-Stake concept. In October 2017, Ethereum's Founder, Vitalik Buterin and Virgil Griffith published a paper which described the proposal of the new concept which is given a code name of "Casper"[51].

The section shall attempt to analyse both concepts purely from Shariah perspective without trying to provide any opinion or recommendation on the technical aspects of the same. The paper shall also not delve into the details of the technicalities and arguments purported by the proponents of either of the protocols e.g. which protocol is better or more suitable for the Ethereum network, etc.

i. Proof-of-Work Algorithm

Proof-of-Work (PoW) algorithm is a protocol which was first introduced by Bitcoin blockchain and later on adopted by Ethereum as well. It is one of the most popular mining protocol used in many other blockchain network as well. Briefly, the probability of mining a block in PoW depends on the computational work done by the miner. It means that the more work or power put into the mining process by a miner, the higher its probability of solving a block.

The work of the miner here refers to the "mathematical puzzle" which needs to be solved. All the miners in the network will compete to be the first to find a solution for the mathematical

[50] Pedro Franco, Ibid. – pp.143.
[51] Vitalik Buterin, Virgil Griffith, *Casper the Friendly Finality Gadget (2017)* – Link: https://arxiv.org/pdf/1710.09437.pdf

problem that concerns the candidate block, a problem that cannot be solved in other ways than through brute force which means it requires a huge number of attempts[52].

The concept of the "more you work, the more you get or the higher chance for you to win" is generally in line with the overall Shariah principle. In this regard Quran mentions:

"And that there is not for man except that [good] for which he strives." (An-Najm – 53:39)

The purpose of such protocol is also to ensure the network is safe from malicious attack, which is important to maintain the integrity and sustainability of the entire blockchain. This is also in line with one of the verticals of *maqasid al-Shariah* (higher objectives of the Shariah) in terms of protecting the safety of the wealth from any malpractice and bad doings.

ii. Proof-of-Stake Algorithm

Proof-of-Stake (PoS) protocol is different from PoW in the sense that it is not dependent on the amount of work by the miners, but rather dependent on the *stake* that the user has. The algorithm now changes from "the more you work, the higher your chance to win" to "the more your stake, the higher your chance to win". It is completely a different protocol to validate a transaction in the blockchain. In essence, the purpose remains the same i.e. to achieve distributed consensus in adding a new block, but the process to reach the desired goal is different.

PoS protocol has already been implemented by a number of different blockchains in the market with the first one being Peercoin in 2012. There are some variations in the technical details of the PoS protocols used by each blockchain, but the general concept remains the same. Another important feature of PoS system is that there will be no block reward which is the issuance of a new token upon completion of a new block being added to the blockchain. Instead, the only reward to the network is in the form of transaction fees which are paid by the users of the network upon executing a certain contract or transaction. This is why in the PoS the miners are called "forgers" because their role now is merely to validate a transaction[53].

The salient concepts and key differences between the two protocols of PoW and PoS are summarised briefly in the following illustration:

[52] Blockgeeks, *Proof of Work vs Proof of Stake* – Link: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
[53] Blockgeeks, Ibid.

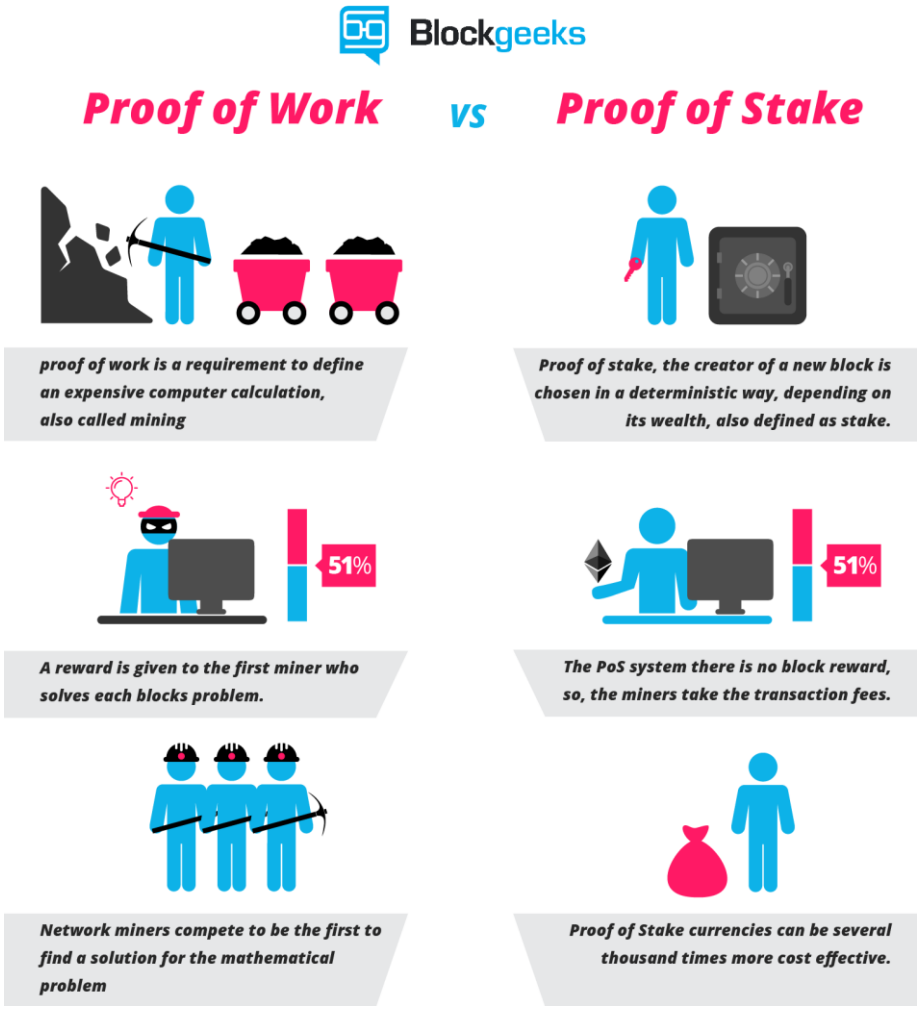

Image Source: Blockgeeks[54]

In the Casper protocol proposal, the network will have a pool of validators or forgers which will perform the task of validating the transaction and adding a new block to the blockchain. There is no priority scheme for getting inducted into the validator pool. Anyone can join the process by staking Ether to the pool i.e. depositing a certain amount of Ether as stake to participate in the validation process. The reward for each validator will be determined by the network according to a number of factors such as decreasing the reward if there are too many validators and conversely, increasing the reward if there are too few. This is to ensure the validation process occurs properly without being manipulated by anyone in the pool.

The staking of Ether into a pool is akin to the placement of security deposit to participate in the mining activity. The return is generated from the transactions fees paid by the network users. There is usually probabilistic element put in place together with the protocol which means that not everyone in the validator pool will get either fixed or the same amount of reward by the system for validating the transactions.

[54] Blockgeeks, Ibid.

To date, Ethereum has not implemented the Casper PoS protocol yet. There is no detail on how the actual implementation of the protocol will be as the discussion among the developers is still on going. Therefore the paper shall only attempt to provide general Shariah opinion on the PoS protocol from the conceptual perspective.

From the general concept of PoS protocol as explained, the return from the stake is not considered *riba* because i) Ether is not a currency, hence any return or extra payment cannot be deemed as *riba al-fadl;* and ii) staking Ether is not in the form of loan or exchange with a fixed return, hence the return generated from the process does not fall into the category of *riba nasi'ah.* Stake in the context of PoS is more like a share in the business activity of validating the transaction on the blockchain.

It is also not accurate to draw a comparison between PoS and gambling activities or betting, because the staking process in PoS protocol is essentially not a zero sum game which is strongly prohibited in Islam. The validators in essence do not have the risk of losing its stake entirely by participating in the process. The stake or deposit by the validators can be perceived as a form of collateral which is locked in the system.

In the Casper proposal paper for Ethereum, it is mentioned that the validators will lose its stake or deposit only if they act in some way that violates some set of rules which is referred to in the paper as "slashing condition"[55], for example if it creates an "invalid" block or signing off on multiple forks which can negatively impact the network[56]. This scenario does not fall under the gambling category because it serves as a deterrence to ensure all validators follow the rule of validation in the network properly. This is part of the best practices which is perfectly in line with the Shariah teachings.

The guideline outlined in this section is based on the interpretation on the general concept of PoS and current understanding of the intended proposal. It is to be noted that the full and actual implementation of PoS has not taken place nor finalized as yet. Thus, a thorough Shariah review on the protocol will be required in the future to assess its compliance and adherence to the Shariah principles once the new protocol is finalized or fully implemented.

[55] Vitalik Buterin, Virgil Griffith, Ibid.
[56] Max Thake, *What is Proof of Stake?* – Link: https://medium.com/nakamo-to/what-is-proof-of-stake-pos-479a04581f3a

CONCLUSION

The Shariah analysis conducted during the research exercise has shown that Ether as the native cryptocurrency of the Ethereum platform meets the criteria to be considered a valuable asset or *mal* from the Shariah perspective. At the same time, its existence on the platform is one of the main requirements to ensure the blockchain functions as it is intended to be. Ether does not have any prohibited element such as *riba, gharar* and *maysir,* therefore it is a Shariah compliant asset. However, Ether at the current stage does not fulfil the requirements to be deemed a currency; hence it does not follow any relevant and applicable Shariah principles and rulings related to currency in Islam, namely *bay' al-sarf* or sale of currency.

It is respectfully submitted that Shariah is neutral with regards to Ethereum which is a platform using blockchain technology. Shariah however needs to look at the purpose and nature of the smart contracts or decentralized applications being built upon the Ethereum platform to review and assess their compliance with the Islamic principles and requirements. The smart contract must not be involved in any of the prohibited sectors, and also the nature of smart contract must be free from any of the major prohibitions in Islam in terms of subject matter and investment activities.

Mining is one of the important components of the Ethereum blockchain. It functions as the mechanism to validate transactions and add new blocks to the blockchain. There are two general protocols which are relevant in the context of Ethereum which are Proof-of-Work (PoW) which is the existing protocol being used; and Proof-of-Stake (PoS) which is currently still a proposal and work in-progress. From the conceptual perspective, it has been established that both protocols do not violate any major Shariah requirements. However since the actual and exact PoS protocol is still unclear at the moment, it is recommended that a full Shariah review will take place once the full protocol is ready or implemented.

The paper has established several objectives to be achieved from the research. Among others, it seeks to provide clarity over the Shariah compliance aspect of Ether as the utility token or cryptocurrency of the Ethereum platform. The reason for this objective is to invite and encourage more participation from the Islamic finance and Muslim community to leverage and unlock the full potential of the blockchain technology offered by the Ethereum platform in the development of various types of Shariah compliant decentralized applications and smart contracts.

It is envisaged that the publication of this Shariah white paper will contribute towards achieving these objectives in a more structured manner.

APPENDIX I - LETTER FROM VIRGIL GRIFFITH, RESEARCH SCIENTIST OF ETHEREUM FOUNDATION

ethereum

August, 22, 2018

Dear Wan,

Please take a look at the following information in response to your email:

1. Overview of Ethereum
Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality (described more below).

2. The purpose of the Ethereum platform
The purpose of the Ethereum platform is to serve as a base layer upon which people can build a variety of distributed apps (dApps), so as to enable the full potential of blockchain-based applications. That's really about it---we don't know what people are going to build. But we recognize the technologies' potential for a more accountable, less-corrupt, decentralized, world.

3. Smart Contracts
A smart-contract is a program (state-machine) that runs on the Ethereum platform. A Smart Contract consists of a set of mechanistic triggerable operations, a set of IF-THEN statements. The IF statements can be any other event on the platform, and the THEN operation can be transferring Ether, or ownership of digital assets. Effectively, smart contracts can function as digital versions of traditional contracts set between any parties, but without the need to have 3rd party verifiers, instead depending on the Ethereum platform itself (the “trustless” mechanic). Smart contracts have the ability to be programmed to run various scripts and are open to be coded the way user would like to deploy set of functions.

4. Ether and Gas
Ether (ETH) is the internal currency for the Ethereum platform, and its sole purpose is to compensate miners for verifying the correctness of the Ethereum ledger and processing updates to the ledger. This internal currency is a **required** feature of any base-layer blockchain-based system---it is the only way that anyone, without caring who they are, can be compensated for processing updates.

The compensation amount by operations on the Ethereum platform is priced in units of “gas”. With each Ethereum transaction, the sender has to specify, "I'll offer N units of ETH per gas consumed", and if this amount is accepted by the miners, the transaction is processed. When the price of ETH goes up (or down), people will bid different amounts of ETH to pay for their gas requirements accordingly. It is also important to note that “gas” does not exist as a separate internal currency - all amounts are only in ETH.

As the platform has grown, we have observed that people have started using ETH as a store of value and as a replacement for cash. This was never something we intended, nor even particularly wanted people to do. But Ethereum is a permissionless network (i.e. anyone can participate without needing to get anyone's permission). As such, if people want to start treating ETH like cash, we cannot do anything about it.

5. ETH is issued automatically by the platform

There are over 100 million ETH in free circulation to date. Currently new blocks mined create 3 ETH approximately every 14 seconds. These are created automatically by the platform - there is no one who "decides" on the creation of ETH, nor can any one individual manipulate the network to generate more ETH. Deflation approach limits the supply so protects value. As the network grows block times slow further reducing the output of ETH.

6. The price of ETH is dependent wholly on the market

As noted above, the Ethereum platform automatically creates new ETH. Because the rate of such creation is fixed based on publicly-known rules, and because no individual can control or change such rate, no one controls the rate of generation of new ETH. (This is as opposed to fiat currencies where the government/central bank controls the money supply and interest rates, therefore indirectly controlling the price of such fiat currency). As a result, the price of ETH is determined solely by supply and demand in the market.

7. SEC statement

The US SEC recently set out their analysis of how to determine if a cryptocurrency is a security, and their determination that ETH is not a security.
https://www.sec.gov/news/speech/speech-hinman-061418
https://www.cnbc.com/2018/06/14/cryptocurrency-ether-soars-9-percent-after-sec-official-says-its-not-a-security.html

8. Examples of dApps

Links to examples of dApps can be found below:
https://dappradar.com/
https://www.stateofthedapps.com/rankings

So far Ethereum has mostly been for simple games (e.g., CryptoKitties), and basic financial infrastructure (IDEX/ForkDelta). There's been a recent spike in Fomo3D as a transparent gambling application / performance art. Probably the most interesting apps (i.e., "What ethereum was intended for") are the ones in the "Other" category, like Augur, 0x, Ethereum Name Service, etc.

Many dApps are being built at the moment on the network but we hope that post shariah compliance this will encourage the Islamic Finance world to also engage in building shariah compliant decentralized products on the network. It is also possible to build shared knowledge resources. The Islamic principle of Isnaad (chain of transmission) can also be used on the network to secure important documents.

9. Description of ERC20 Tokens

ERC20 tokens are what most dApps and Smart contracts issued on the network use. Not all require a token. Some may just use ETH as native token. Others mint new tokens. Anyone can launch a new application with a new ERC20 token. By coding the token and launching a smart contract they can now give value to their own token, just like HelloGold. These token operate and transfers through the Ethereum network. The network has no control on who issues the tokens, how many and what they are used for. The token transactions are validated through the network and follow the smart contract functions to stay true to what has been coded. You can view tokens that are issued as smart contracts here https://etherscan.io/

10. PoS vs PoW

Currently the Ethereum platform runs on Proof-of-Work (PoW) algorithm. PoW miners are rewarded to create new blocks with new minted ETH (as described above). There are proposals to change this to Proof-of-Stake (PoS). In the PoS model you are rewarded to validate transactions against the amount of ETH you currently hold. So the larger holders will be validating more transactions for more reward. PoS is suggested to make the network faster and more scalable to the masses as a much faster and lighter protocol.

I hope the above is helpful. Please let me know if you have any more questions or want any clarification on any of these points.

Thank you,

Virgil Griffith
Research Scientist, Ethereum Foundation

APPENDIX II - SHARIAH ENDORSEMENT ON THE SHARIAH WHITE PAPER BY AMANIE SHARIAH SUPERVISORY BOARD

In the Name of Allah, The Beneficent, The Merciful

29 April 2019

SHARIAH ENDORSEMENT IN RELATION TO SHARIAH WHITE PAPER ON ETHER

We, the undersigned, are the scholars comprising the Amanie Shariah Supervisory Board ("SSB"). We have been presented with Shariah White Paper on Ether ("Shariah White Paper") developed and prepared by Amanie Advisors in collaboration with Ethereum Foundation.

We have reviewed the Shariah White Paper and hereby confirm our endorsement on the same.

Allah Almighty knows best.

APPROVED BY:-

Dr. Mohamed Ali Elgari *(Chairman)*

Dr. Mohd Daud Bakar *(Member)*

Dr. Muhammad Amin Ali Al-Qattan *(Member)*

Dr. Osama Al- Dereai *(Member)*