SHA256 9884192D0D9B0675F4F5CA37264E0E8604A7EC54CE417A22390DEB45203E7B51

WorldLand

Academic grants proposal sent to: academic-grants@ethereum.org.

Submitted by Blockchain Intelligence Convergence center

Director Heung-No Lee

1 Project name: WorldLand

Project cost: $100,000

Project duration: 12 months

Proposed starting date: June 1st, 2022

Submission date: May 8, 2022

Principle investigator: Prof. Heung-No Lee

Contact information: +(82) 10-4946-4710, heungno@gist.ac.kr, heungno@gmail.com, hnlee@ieee.org
Web-page 1: PI's lab home page: https://infonet.gist.ac.kr/
Web-page 2: PI's BIC center home page: http://www.gist-itrc.org/eng/.
Linkedin: https://www.linkedin.com/in/heung-no-lee-4808b38/
Twitter: @fighterkerry
Telegram user name: heungno

The Blockchain Intelligence Convergence (BIC) center was started with national funding by The Ministry of Science and ICT (MSIT, https://www.msit.go.kr/eng/index.do) in 2021 in the area of Blockchain Foundation. MSIT is a primary administrative agency of the Republic of Korea's government that sets, coordinates, and evaluates science and technology policies; and undertakes scientific and technology research, development, collaboration, and promotion. The BIC center's objectives are twofold: research and education. The research goal is to develop innovative new technologies in the converged field of blockchain and artificial intelligence. The center's researchers are working to advance technologies such as Zero-Knowledge Sensing*, Cryptographic Authentication, and Federated Learning. The educational goal is to create new graduate-level courses and programs that will teach advanced masters and doctorate-level scholars in the unique technologies that will be produced at the center.

* Zero-Knowledge Sensing is referred to as a novel technology invented in the center which aims at preserving the physical uniqueness of real-world signals such as human voice, radio waves, and visual feeds while protecting personal information when these signals are converted into data via relevant sensors. Such preserved physical uniqueness can be utilized to authenticate an individual, a material, a location, and a height.

2 Executive summary–Blockchain technology is envisioned to transform the Internet from an information-sharing platform to a metaverse in which citizens worldwide can gather,

dwell, and transact directly with each other. Transactions will not need to be arbitrated by a trusted third party thanks to the blockchain. Enriched will be person-to-person interactions among individuals and improved the lives of people throughout the world. For such a vision, it is crucial to continue innovation in the blockchain technology. Consensus, virtual machines, and peer-to-peer networking are the three primary components of a blockchain. One of the most pressing demands at the moment is to 1) update the consensus mechanism that allows a new scalable, secure, and decentralized blockchain network, and 2) upgrade the cryptographic primitives used in consensus and virtual machines so that they are post quantum-computer (PQ) safe.

In this project, we aim to develop a novel consensus mechanism called WorldLand. WorldLand consensus is composed of two major parts, a verifiable (self-election) coin-toss function (VCT) and a novel proof-of-computation (PC) primitive. WorldLand will base its PC part on a newly published finding known as the error-correction code proof-of-work (ECCPoW). The main upgrades are to make the PC primitives PQ safer than ECCPoW and to address environmental concerns about energy expenditures. A critical component of the virtual machine will also be enhanced; particularly, the elliptic-curve cryptography and other parts built on it will be replaced with our PQ-safe cryptography.

Ethereum 2.0 is scheduled to migrate to a Proof-of-Stake (PoS) system with the Merge. It can benefit from the WorldLand consensus and virtual machine. To further contribute to the Ethereum foundation's efforts, we want to incorporate a PoS option into our WorldLand consensus. Using PoS embedding, one may regulate the barrier to entry into the pool of peer-to-peer nodes and strike a strategic balance among security, scalability, and energy consumption issues.

WorldLand protocol suite will be developed into an existing open-source version such as the Ethereum Instanbul. A proof-of-concept network will be created for validation and testing. All project outcomes will be made available to the global community through open-source code and paper publications.

3 Grant scope

- What are you going to research?

- What is the expected output?

We envision developing a new protocol suite called WorldLand for a global-scale blockchain. The WorldLand suite is quantum safe, energy-efficient, decentralized, secure, scalable, and Byzantine fault-tolerant (BFT). Our goal is to use it to build a new strong, decentralized, and secure global blockchain network. This network will have a worldwide footprint that includes all five continents, allowing for the connection and support of a many number of sidechains, shards, and plasma chains.WorldLand aims to seek simplicity in design but not to meet all the needs out there in terms of scalability. Faster transactions per second (TPS) services, for example, are aimed supported at the 2nd layer. WorldLand will build on the virtual machine of the Ethereum Istanbul.

A set of key performance metrics of the WorldLand network will be set as follows:

- M1. PQ security. We aim to make sure that the WorldLand consensus passes all the security check vectors for PQ security.
- M2. Scalability of more than 1 million nodes: The number of peer-to-peer nodes participating in the global consensus is expected to exceed one million. There will be four modes: 1000 node testing mode, 10K mode (10,000 nodes), 100K mode, and the complete mode (more than 1 million nodes).
- M3. Energy consumption efficiency (ECE). Ethereum 2.0 aims to achieve an ECE of approximately 99.8% in comparison with today's Ethereum mainnet [1,2]. We aim at achieving the same order at the complete mode. For the first three scalability modes, ECE can be set smaller, i.e., 50%, 70%, and 90%, respectively.
- M4. Byzantine fault tolerance (BFT): How tolerant is the consensus mechanism as to the percentage of fraudulent nodes compared to the total number of nodes?

  WorldLand supports BFT of 1/2.
- M5. Block generation time (BGT): What is the block interval? It is a random variable. The average BGT is set to 12 seconds per block. Let the standard deviation of the random BGT be called *d*. We aim that the event of BGT deviating from its average BGT greater than 5*d* occurs very rarely (say less than .1% of the time).
- M6. Block size: How large a single block should be? We aim it adaptive to the demands as Ethereum 2.0 does: the block size is to be limited to the maximum allowed gas (a target size of 15 Million gas and the limit of 30 Million gas).

Algorand and Ethereum 2.0 support BFT of up to 1/3. Whereas the hash PoWs, such as Ethereum Classic, Bitcoin, and Bitcoin Cash, can support BFT of up to ½. In comparison to the BGT values of Algorand, Ethereum Classic, Ethereum 2.0, Bitcoin, and Bitcoin Cash (which are 5 s, 13 s, 12 s, 10 m, and 10 m, respectively), Wordland is set to take 12 s. Algorand, Ethereum Classic, Bitcoin, Bitcoin Cash, and Polygon are not quantum safe. Whereas Worldland will be quantum safe. In comparison to previous schemes, the WorldLand suite will have the system complexity minimized owing to its plain and straightforward architecture.

4 Project goals & success factors

What are you hoping to accomplish with this grant?

How do you define and measure success for this project?

Project goals are to

- G1: Design a novel WorldLand PQ secure cryptographic primitives. A novel verifiable random function (VRF), a verifiable self-election coin toss (VCT) function, and a verifiable computation function are among them.

  Each of these new primitives must be PQ secure.

- G2: Integrate the WorldLand cryptographic primitives into Ethereum Istanbul. The integration affects the consensus mechanism as well as the sign/verification component. Let us call it the WorldLand suite. Create the WorldLand suite in the Go programming language.

- G3: Develop a real-time WorldLand testbed on AWS. Carry out extensive testing and validation. Demonstrate that all six key performance metrics in Section 3 are met.

Success factors

- We are a group of well-known cryptography, security, and information-theoretic/coding theoretic mathematics specialists.

- We have a team of programmers who can develop the novel WorldLand protocol into the existing protocol suite of Ethereum Istanbul.

- We are an experienced team with a track record of journal and conference publications. They are the world's top journals and conferences in their relative fields.

- We have completed relevant work and presented our findings in public areas such as GitHub, open journals, archive repositories for prepublication, and our lab website.

Measures of success

- (Proving PQ security) We aim to prove all primitives are PQ secure. We aim for submitting a complete journal paper with the cryptanalysis result.

- (Building testbed) As a result, we plan to complete developing, constructing, and testing the WorldLand protocol throughout the project duration.

- (Having all the six key metrics satisfied) We will measure all six key performance metrics M1 through M6 off from the live WorldLand test network. The real-time network will be powered by AWS nodes. We aim at building a large-scale network of up to 1000 nodes. These nodes will be distributed as evenly as feasible around the world.

- (Testing via a hacking bounty) We will conduct a hacker bounty festival, publicize it, and actively invite hacking bounty hunters. They want to start assaults against the live WorldLand test network.

5 What problems are you trying to solve?

5.1 Problems

Today, blockchains are not PQ secure; there are environmental concerns; there are

scalability issues. To solve these concerns, several major projects are implementing a PoS paired with a Byzantine agreement (BA) algorithm. PoS and BA algorithms are good; but they are not secure enough for a global monetary grade blockchain network. The ideas are not new. A BA algorithm (developed in the 1980s [35]) relies on communication across committee nodes to obtain a consensus, rendering it subject to a variety of assaults, including DDoS and network partition attacks. To make it scale well in terms of the number of nodes, the size of the committee be made small; hence, decentralization is compromised.

- P1: To date, current blockchains and cryptographic primitives used in them are not quantum computers safe.

- P2: A innovative scalable consensus mechanism that does not jeopardize security or decentralization is required.

- P3: A novel and solid technologically advanced solution is needed. PoW was technological innovation. It has enabled globally decentralized consensus; decentralized consensus is achieved while each node simply does its own work of validating transactions, forming a new block, and attaching PC to the block. PoS is a long-standing sociopolitical solution. PoW is simple and strong, allowing for decentralization. While keeping the desired properties of PoW, we aim to address the energy and scalability issues.

- P4: The safety of migrating to PoS with the Beacon Chain and 64 shard chains has not been proven nor carefully delineated with its robust counterparts. At least in academic terms. Its security should be examined and compared to the current Ethereum mainnet, Algorand, and a new one like WorldLand.

5.2 Challenges

(It is hard to satisfy dual mandates.): Blockchains are a deer but expensive solution. Blocks are redundantly stored within every consensus participating node. All nodes are doing the same work. Each new block is made with an effort–an enormous amount of time and energy spent–by the entire network. This is the source of the immutability of the record stored in the blockchain. The network needs to be decentralized as much as possible. The greater the number of individual nodes participating, the more secure the network is in terms of censorship resistance and thwarting Sybil and double-spending attacks. Consider bitcoin: Each block has a massive quantity of computational energy is stored in each block. On the one hand, the huge redundancy, numerously many independently working nodes doing the same work, can be viewed as a source of security. On the other hand, it can be viewed as a waste of resources and a waste of energy. The blockchain trilemma represents the scalability challenge caused by inefficient resource consumption. The complaint on the energy issue leads to environmental concerns.

(It takes a simple protocol to withstand attacks and perform robustly for years to come.) The consensus mechanism should be basic to maximize resilience to numerous attack vectors. How can we make it simple while accommodating a large number of p2p nodes

working together to reach a consensus? The participating nodes must make timely judgments, agree on those decisions, and choose one block from among several candidate blocks to be the new block attached to the status-quo chain. The timely consensus decision should be made in a distributed manner among numerously many independently working nodes over the Internet. As a result, an agreement must be reached with as few contacts as possible among the p2p nodes. Internet is an environment in which frequent network delays and network partitions occur. They might be caused by momentary router failures and traffic congestions, but they could also be caused by purposeful antagonistic activity. A global blockchain network must be robust to such possible attacks and losses. To date, the consensus mechanism using the hash function-based PoW [3] has been shown to provide the most decentralized and secure operations. Thus, it is a challenge to design such a consensus mechanism that does achieve all these needs–a huge number of p2p nodes, making timely decisions, while working independently, with minimal intranode communications–simultaneously.

5.3 Merits of PoW

(Bitcoin's hash PoW is plain, simple, and secure.) The nodes in the bitcoin network are not divided according to their jobs. The time axis is also not split by time epochs. Each node simply performs the necessary work, confirming transactions, grouping them into blocks, adding the PC, and publishing the block as quickly as feasible. Consensus is reached as the result of each node's simply doing its work for its own benefit. Each node is not forced to work in a time-division schedule. To obtain a consensus, each node does not need to adapt to the progress of other nodes (therefore requiring no contact with each other). Every node makes blocks; every node validates blocks. The protocol is plain and simple. This results in stable performance. As a result, blocks cannot but be kept on produced. Rewards are given as incentives to nodes. More effort a node makes more opportunities it earns for rewards. There is no need for node righteousness. No punishment is needed.

(BA algorithms are not decentralized.) Under a BA algorithm, jobs are divided. A set of nodes, under the name of proposers, make blocks. They announce them for the vote. The proposed blocks are validated by another group of nodes, such as attesters. They voted for each candidate block. The cast votes are gathered and counted. The block with a satisfying number (i.e., supermajority) of votes is selected and connected to the status-quo chain. To complete all these, each node needs to fit itself to a tight schedule. As a result, the time axis must be separated into slots and epochs. For this to operate properly across a hostile environment like the Internet, the number of nodes engaged in consensus must be limited to a few hundred at most.

(Time-energy borne wealth) Bitcoin is a stored wealth transformed from time and energy. Each block header, released information, contains information on time and energy cost. Take any block from the past. The block header contains the date and time when the block was created. The puzzle's difficulty level is also specified. Using this information, one can calculate how much computation (hash cycles) was needed to solve the hash puzzle. It would have taken more than 3 years for a single node working

alone to solve the hash challenge, yet it only took 10 minutes for a network of distributed independently operating nodes all over the world (average sense of course). See the alone impossible together possible (Al-Im-To-Po) theory [36]. Thus, it is an indication hundreds of millions of computers had to work together at that time to produce that block. Given the energy efficiency of a mining node, the amount of energy expended to create that block can be calculated. A predetermined number of bitcoins were minted on the block. At this moment, we can claim that the blockchain network has converted the energy expended into the bitcoins minted in the block. The miners spent time and energy. Mining rewards and transaction processing fees were paid to them. In this approach, each block may be considered as a new way of storing wealth that has been changed from the most basic resource of time and energy. Time and energy are the most valuable resources humans have; they may be considered the most fundamental type of wealth. As a result, the coins created in each block have monetary value. The energy and time were not squandered; they were converted into something useful, a bitcoin. Others have used their time and energy to create important commodities and services, such as food and building a house. One can give bitcoin to purchase the goods and services others have produced and offer.

5.4 PoS alone is not enough. The addition of the BA algorithm does not help much.

To address the energy and scalability concerns, PoS was adopted as an alternative to PoW. But PoS is well known to have many obvious concerns of its own [4,5]. PoS is being introduced to address the energy concerns and to increase TPS. However, the penalty may be significant: it is not decentralized and is not secure. PoS is not a technological advancement. It lacks the advantages of PoW. It instead resorts to a sociopolitical solution: plutocratic politics. Because PoS does not retain any energy on a block, blocks may be readily rewritten; hence, it is insecure. Your stake will be confiscated if you act badly. This is a “fixing a barn after losing a cow” approach. The richest few can make confidential agreements off-chain and take the control of a blockchain. These off-chain conspiring operations leave no on-chain trace, thus no one can even become aware of them. As a result, it is known to be sensitive to bribery or collusion [6]. There is a famous now, nothing-at-stake problem [7]. There is a risk of grinding attack if the random function for selecting a block creation node is unfair or predictable [8].

The time-energy borne (TEB) wealth property no longer exists with PoS nor with PoS & BA algorithm. In Ethereum 2.0, ETH may no longer be used as a store of wealth or a base money for the community. The Beacon Chain may not be able to provide a solid foundation for its shard chains.

5.5 The WorldLand Approach

We want to solve the PQ, scale, and environmental concerns while maintaining security, decentralization, and TEB wealth property. We aim to approach it with a new technological means developed. These new tools allow us to crack the dual mandates. Each node does a simple task alone and independently; as a consequence, each node

operates independently; it allows the system to run steadily even with a huge number of participant nodes; nodes are homogenous; and energy spending expenditure can be managed. This protocol is plain simple. Each participating node may easily obey the rule. Each node performs the same simple work because no job is divided, no time is divided, and no communications are required for each to participate in the discussion and reach a consensus; each node simply continues to work independently and repeats the same procedure for each block; consensus is reached when some node announces the next block. The only announcements each need to stay vigil is the announcement of a new valid block. This simplicity lowers the barrier of entry and invites more participating nodes.

This Section 5.5 progresses in the following order: an overview of WorldLand, novel PQ secure primitives, the WorldLand testbed, Safeguarding against profitable double-spending attacks, and how WorldLand may help Ethereum 2.0.

5.5.1. WorldLand Overview

WorldLand protocol aims to build a decentralized, scalable, and secure solution for an extremely large network of nodes, even if the number of participating peer-to-peer nodes reaches more than 1 million.

(The base set of P2P nodes) The base set of p2p nodes is defined as all nodes that participate in transaction validation and block formation. The protocol performs effectively with base-set sizes greater than one million.

(PoS enabled) The option of PoS can be turned on by restricting the base set of nodes to be the set of nodes that have provided an on-chain proof of stake.

(WorldLand consensus with verifiable computation) Like the hash PoW, all of the nodes in the base set collaborate and contribute to the creation of each new block. There will be no separation of jobs for a node to carry out. Each node self-elects herself to do the work. This is accomplished by validating transactions, forming a block, and attaching a PC. Each one repeats this per a new block. The benefit is the simplicity of the algorithm. Finality is determined by the amount of energy stored in the blockchain. If there are two blockchains, a node will select the one with the most energy stored inside it and add the new block to it.

(Verifiable coin-toss) Every node has its own unique (secret key) coin. Each will toss her coin first. It features a single output that may be either Pass or No-Pass. This VCT is a VRF. It has two inputs. It has a single output, either Pass or No-Pass. One input is the secret key of the node; the other is the header of the previous block. As a result, each node cannot but toss this VCT once and only once each block The purpose of VCT is to have a certain portion of the base set of nodes turned OFF; energy is thus saved. If the proportion is set to 90%, energy-saving is 90%.

We aim to design the VCT function so that the odd of Pass can be precisely controlled. The odd of Pass is a critical parameter that the network designer may use to change the amount of energy saved given the size of the base set. For example, when the number

of nodes working in the network is small, it could be set to 100% to maximize the security.

For those nodes who have self-selected themselves to do the computing work, there are two types of computations, VeriComp and SolComp, which every node has to do.

(VeriComp) VeriComp is the process of validating transactions and compiling them into a new block. Upon receiving a new block announcement, each node validates the block and begins work on adding a new block to it.

(SolComp) SolComp is referred to as the computation needed to solve the crypto puzzle. Each round presents a completely fresh and surprising crypto puzzle. The puzzle problem is not predictable in advance, but it is determined if the preceding block header is known. Each node in the self-elected set then starts the race to solve the crypto puzzle as fast as possible. A node with proof of solution inserts the proof into the block header and broadcasts her new block instantly.

(Coin is tossed first before any energy is spent for computing.) With WorldLand consensus, we note that all nodes participate with the same simple rule. Each node takes a random turn to form a new block and attach the proof of computation. Our new VCT function makes it possible to take turns. Each node progresses into the energy spending SolComp process if she gets Pass from her coin-toss function. It can be built in such a way that the odd of Pass may be carefully controlled. For this to work well, the VCT function should be carefully designed.

5.5.2. Novel PQ Secure Primitives

We aim to develop novel postquantum-ready and WorldLand suitable cryptographic primitives. They are new functions for key generation, sign, and verification. They are novel key generation, signing, and verification functions. It also has the new WorldLand VRF, VCT, and VC that we covered in Section 5.5.1.

The quantum computers are known to break well-established cryptographic algorithms such as elliptic-curve cryptography, and digital signature algorithm, and RSA. These methods, in particular, are based on integer factorization problems and discrete logarithms problems, which are not known to be quantum safe. Code-based cryptography issues, on the other hand, are known to be quantum safe.

(Brief history on early code-based cryptography) McEliece firstly presented the code-based cryptosystems using binary Goppa codes in 1978 [9]. In 1986, Niederreiter proposed a knapsack-type public-key cryptosystem based on error-correcting codes using GRS codes [10]. Later, the Niederreiter method is demonstrated to be as secure as the McElice cryptosystem. Sidel'nikov and Shestakov demonstrated in 1992 that Niederreiter's plan to employ GRS codes was insecure [11]. There are various ideas to minimize the public-key size by employing different codes such as Gabidulin codes [12,13], algebraic geometry codes [14,15], and Reed-Muller codes [16]. However, all of these approaches ultimately proved to be unstable [17,18].

First, we explain current advances in PQ secure signature algorithms. Second, we describe how to create a new PQ secure VRF. Third, we discuss a novel VCT function.

Fourth, we discuss the BFT and ECE of the proposed WorldLand.

5.5.2.1. Find recent PQ secure signature primitives

The goal of this part is to research recent advances in PQ cryptography and select a set of suitable PQ secure algorithms. They can be used to meet our goal of developing a PQ secure signatures and a PQ secure VRF for the WorldLand blockchain.

A digital signature (DS) algorithm is composed of three parts. The first component is the KeyGen component, which produces a public key and a private key pair. The second is the Sign part. Given the message and the private key, it generates a signature. The third component is the Verify section, which generates a binary, Pass or Fail, output based on the message and signature.

A VRF is similar to the DS algorithm in that it consists of three functions: a KeyGen function that generates a private and public-key pair; a VRF function that generates a signature (proof) and a random number given the input of a private key and the message; and a Verify function that generates an output of Pass or Fail given the input of the public-key, message, random number, and proof.

We conducted preliminary research and discovered that Dilithium [19], Falcon [20], and Durandal [21] are good candidates for PQ safe signature algorithms suitable for WorldLand blockchain: the key metrics we used to select them are the size of the keys, the size of the signatures, the time it takes to complete a sign, and the time it takes to verify.

Let us compare them here. The unit is msec. Dilithium requires 1.4, 6.2, and 1.5 for key generation, sign, and verification. Falcon, on the other hand, takes 197.8, 38.1, and 0.5. Durandal receives 4, 4, 5 points. Durandal therefore has the quickest signature time when compared to rival methods. The signature time corresponds to the VRF generation time. Durandal could serve as the first candidate for us to build a fast PQ-safe VRF. It offers a code-based DS algorithm with rank metrics. While rendering a quantum-safe signature, it is also sufficiently concise. The signature is 4kB long, while the public key is around 20kB in size. The signature and verification processes take just 4 msec and 5 msec, respectively. It is powerful, quick, and succinct enough to be considered a candidate for a worldwide public monetary grade blockchain, such as WorldLand.

We aim to carefully study these candidate PQ secure algorithms. We aim to select the best one that renders results satisfying the key performance metrics of WorldLand. The best PQ secure algorithm will be selected and developed into the WorldLand protocol suite.

The selected signature algorithm will be implemented with the Go language; we will have it replace the elliptic-curve DS cryptography.

5.5.2.2. Make novel PQ secure VRF and VCT functions

The goal of this section is to discuss how we approach making a novel PQ secure VCT function. To the end, we must first create a good PQ secure VRF function; we will then utilize it to create the VCT function.

A VRF can be defined as a function that generates a random number with a unique signature (proof) attached to it, given a private key and a message. What makes it distinct from an ordinary random number generator is that it also offers a verification procedure. Thus, any verifier can check if or not the random number was properly calculated. The quality of the random number it generates must be great; given the size of the keys, the random number's entropy must be maximized.

A VRF is similar to a DS scheme as mentioned in 5.5.2.1. But there exists a crucial difference. It is the signature. The signature for a DS method is nonunique stochastic by design, since stochastic signatures increase security. However, for a VRF, the signature must be made unique for each fixed input. Recall our goal of using a VRF. We aim to use it as a means to save energy spending in the SolComp stage. To that aim, the VRF should be designed to execute just once and only once every block; otherwise, the node would abuse it by running VRF as many times as possible until she produces a suitable output; no energy savings are realized as a result. Such enforcement is achieved if the VRF by design generates a unique signature for a given fixed input message. We may modify the input message to contain public information that had existed prior to the time the VRF was performed, such as the previous block's block header. The same goes for the public key. The public key should have been already posted somewhere in the blockchain prior to the time of running the VRF. The private key associated with it is therefore fixed. As a result, each node cannot but run it once and only once every block.

(Challenges) We need to investigate the PQ secure algorithms such as Durandal, Falcon, and Dilithium and create a new VRF which generates a unique signature. To that aim, it is critical to comprehend the underlying workings of these algorithms' signature generating primitives.

(Our approach) In general, creating a new routine within a cryptographic algorithm is not an easy task since it will change the method's security output. However, it appears that there are a few options for this goal. Any such modification to make a unique proof is basically to have the degree of freedom (DoF) lowered in the proof part. If the same amount of DoF is increased somewhere else, the system can be made to remain secure. To illustrate, suppose the DoF in the proof is reduced so that the proof be unique for a given fixed input. We can then discuss two possible directions. First, we add the same amount of DoF in the random value; the VCT function may be modified to accommodate this modification, which slightly increases the size of the random value. Second, we would take the approach of increasing the same amount of DoF in the private key; but this would slightly increase the size of the private key. Such a balance is required to ensure that such a change does not compromise security. We will have to try a few different techniques to find the ideal one for WorldLand and PQ security.

(Cryptanalysis for PQ secure VRF) The security of the proposed VRF will be evaluated using (a) uniqueness analysis, (b) collision-resistance analysis, and (c) pseudorandomness analysis. The performance of our proposed VRF candidate will be measured by analyzing the time required in the development of the proposed signature, followed by the hashing time, and the overall time, which includes key generation, signing, proof, verification, and block building [22,23]. The other factors such as sizes of private and public keys, lengths of signature and hash, computational complexity, and energy consumption will also be considered to evaluate the efficiency [24].

(How to make the VCT function from the VRF output) Given a new good VRF function ready, we then aim to utilize it to make two more novel primitive functions. The first step is to create a new coin-toss function that accepts the result of the new VRF function and produces a binary output–Pass or No-Pass. The second step is to create a new control procedure that seeks to alter the odd of Pass based on the network designer's requirements. Such needs are to first enable PoS and to second enable energy efficiency control. The probability of Pass can be weighted based on the stake with an on-chain proof each node has made. The same can be done for energy efficiency. Furthermore, it is critical to establish that these primitives are PQ safe.

5.5.2.3. Error-Correction Codes PoW and how to make it PQ safer?

For the VC part, we aim to use ECCPoW[25,26] for its ASIC resistance, simplistic, time-varying, PQ ready, and *time-energy* properties. ECCPoW is a new VC method our team has developed and published [25,26]. ECCPoW is based on an error-correction code called the low-density parity-check (LDPC) code. Error-correction code works in the same way as error-correction code-based cryptosystems do. The resistance of ECC cryptosystems against quantum Fourier sampling attacks has been demonstrated [27]. Faster and more secure ECC cryptosystems are still being studied [28]. Durandal, for example, is a lightweight and secure rank-metric code-based cryptosystem [21].

How our previous work, ECCPoW [25,26], will be extended in this project?

In the proposed project, we need to extend ECCPoW [25,26] in two aspects. The first is to make it WorldLand suitable (see M1–M6 requirement). The second is to make it PQ safer by using medium-density codes. We want to make sure these extensions are safe from well-known security threats.

(Difficulty Control Algorithm) The tradeoff relation between the amount of verifiable computation and energy spending expenditure can be precisely determined. This tradeoff relation can be utilized to devise a difficulty control (DC) algorithm. The DC algorithm's purpose is to have the network create blocks in a defined regular (in the average sense) interval while reacting to changes in the total number of participating p2p nodes over time and a certain energy spending expenditure level.

In this research, we aim to examine the possibility of making ECCPoW PQ safer. In ECCPoW, LDPC codes were used to generate the time-varying crypto puzzles. We intend to study the potential of replacing it with moderate-density parity-check (MDPC) codes to make ECCPoW PQ safer in this project. LDPC codes do not possess any

algebraic structure but the only simple combinatorial property (sparsity in the parity-check matrix); this makes it postquantum secure. There have been different suggestions for McEliece schemes using LDPC codes [29-32]. However, since their low weight parity-check rows correspond to low weight codewords in the dual codes, they can be easily utilized to attack the cryptosystem. As a result, after raising the density to ten times, MDPC codes have been proposed for cryptosystems. Furthermore, the quasi-cyclic structure has been devised for shorter public/private keys [33]. One famous example of this cryptosystem is BIKE, one of the 3rd round algorithms in NIST Post-Quantum Cryptography (PQC) Standardization.

5.5.2.4. BFT and Energy Consumption Efficiency of WorldLand

Each node runs the VCT, sees the outcome (Pass or Fail), and advances herself to the verifiable computation stage if it was Pass.

WorldLand supports a BFT of 1/2.

Suppose a base set of a certain size for the WorldLand nodes. To launch a 51 percent double-spending attack, the attacker needs to hold 51% seats on the SolComp committee. The usage of VCT just decreases the overall size of the committee but has no effect on the proportion of the committee. This necessitates the adversary to have had 51% presence in the base set. This stays true regardless of the VCT's failure probability.

WorldLand can control energy spent for verifiable computation with the odd of Pass.

The ECE is calculated by comparing a network with the odd of Pass set to none to a baseline network. For the baseline network, the odd of Pass is set to 0%. When the odd of Pass is set to 10%, an ECE (ESE) of 90% is reached.

5.5.3 The WorldLand Testbed

The WorldLand protocol suite will be developed on an existing open-source platform such as Ethereum Istanbul. We will upgrade the opcode table. We will use WorldLand cryptography instead of the elliptic-curve cryptography for Sign/Verification. We will present simulations on a proof-of-concept (PoC) network with a larger number of peer-to-peer computers. Amazon Web Services will be used to reduce resource commitments and costs. Quantum attacks [24] will be used to assess the security of the PoC network.

We will utilize the fork of Ethereum Istanbul (2019) for verification and validation of the WorldLand. Similar to our ECCPoW implementation [25], we will use the Go version 1.10 or higher as the developer language. The configuration of the network will be conducted using the puppeth. We will name the network as WorldLand. A new genesis will be created and WorldLand will be selected as the consensus algorithm. After defining the chain ID and exporting the genesis, the network will be configured using the WorldLand consensus procedure.

In the testing phase, we will use the WorldLand to produce the genesis file

worldland.json inside the bin of Ethereum with full specifications such as chainID, nonce, difficulty, and time stamp. Other json files such as WorldLand-harmony.json will also be verified using standard attributes. We will initialize each VC node with init worldland.json and test the initialization with geth console notes; define the geth data path and the neworkID to run the VC node; use the geth console to check if a node is successfully implemented or not.

Finally, we will connect our network with the MetaMask. We will also examine if standard smart contracts are correctly operating in the WorldLand test network. Implementation of tokens, for example, ERC20, ERC777, ERC721, and ERC1155, will be carried out; stress test of many transaction executions will be performed on the network.

5.5.4. Safeguarding the network against profitable double-spending attacks

Even the most secure hash PoW protocols are still vulnerable, it is now known, to double-spending (DS) attacks [34]. The problem gets exacerbated when the network, the computational power of the network, is small. By borrowing computational resources from a mining rig lending site, an attacker may simply launch a DS assault. As long as there is a profit-taking opportunity, such an attack is possible. A opportunity opens up as long as the profit overwhelms the cost. The key new finding in [34] is that profitable DS attacks can occur even if the honest nodes have well more than 50% of the computational resources of the network. The attacker can attempt to double spend a transaction whose stake exceeds the cost of leasing mining rigs from a lending service. WorldLand aims to safeguard the network from the profitable DS attacks. Such assaults cannot be completely forbidden, but they can be discouraged by lowering the profit the attacker can make and increasing the cost the attacker must bear. Micropayments are not affected by this; big transactions need attention. We intend to develop innovative methods of securing large transactions. Mathematical guidance tools will be developed in the form of APIs. They will be made available to the global population.

5.5.5. How does this project benefit the greater Ethereum ecosystem?

(Ethereum 2.0) Ethereum 2.0 has three phases: Phase 0–Beacon Chain, Phase 1–shards, and Phase 2–execution. Phase 0 is primarily concerned with the engagement of validators, who will serve as the basis for the development of subsequent stages. The Beacon Chain mainly stores data like validator addresses, validator states, and shard links. Furthermore, the Beacon Chain allows validators to collaborate in groups to suggest blocks, vote for blocks, and report the slashable behavior of other validators. The Beacon Chain oversees the validators and manages the staked ETH. Each committee is formed by the Beacon Chain, which includes at least 128 validators. A committee is a group of random validators that performs votes recorded on the Beacon Chain and oversees the behaviors of proposers. To limit the danger of malicious attacks, the blockchain chooses validators at random.

The Beacon Chain also coordinates the network by serving as the consensus layer using RANDAO algorithm. Ethereum 2.0 intends to combine the RANDAO protocol

with verifiable delay functions (VDFs) to pick block proposers at random on the Beacon Chain. However, the current VDFs are complex and are not post quantum secure [36].

As a result, one can use the WorldLand primitives in a consensus layer of Ethereum 2.0 to make it quantum safe. Furthermore, other layer 2 project teams can benefit from our work as well. Summarizing what we have expressed so far, we have the following results the Ethereum communinity can take benefits of:

1. PQ secure primitives: Using coding theoretic principles, this project aims to design and implement postquantum secure primitive functions for consensus and virtual machines. The WorldLand PQ primitives may be used in any global blockchain ecosystem, including Ethereum 2.0 and L2 solutions, to make them PQ safe.
2. Low energy consumption: The WorldLand consensus is simple, concise, and fast; it can be used in any blockchain ecosystem for minimizing energy consumption significantly.
3. Scalable blockchain with security and decentralization: The WorldLand will support a scalable blockchain ecosystem while providing a quantum-safe and decentralized environment.
4. Failure-resistance: When using WorldLand, the blockchain network will stay operational even if a huge percentage of nodes would have gone down or a severe network partition would have occurred.

6 Total budget requested*

USD100,000.

7 Budget breakdown and project roadmap–Please include a brief explanation on the milestones/roadmap in a 3–6 months' timeframe, along with expected deliverables. Outline how the funding will be utilized for the research project and/or team members.

The project consists of three major tasks with a twelve-month timeline. These projects, namely PQ Primitives Development, WorldLand Suite Development, and Realtime WorldLand Testing & Validation, need expenditures of around $50,000, $30,000, and $20,000 respectively. Development work will be accomplished over the first six months of the project. In the second month, the WorldLand Suite Development task will begin and will be completed within the next seven months. In the last five months of this timeline, the Realtime WorldLand Testing & Validation task will be carried out.

The total budget required for this project is $100,000 which is divided into the direct cost (75%) and indirect cost (25%). Direct cost includes salaries & benefits, equipment, materials & supplies, and travel. The salaries & benefits budget (37.5%) includes salaries of faculty worth $18750 and students worth $18750. Blockchain Intelligence Convergence (BIC) center already has all the necessary equipment. Materials & supplies worth $22500 (22.5%) are required to successfully implement the WorldLand suite. A travel fee of

$15000 (15%) is necessary for attending conferences or seminars. GIST overhead is the indirect cost of $25000 (25%).

Members of the Team.

The team has three professors, and several postdoctoral/master/Ph.D. level student researchers.

a. The principal investigator Prof. Heung-No Lee received his B.S., M.S., and Ph.D. degrees from the University of California, Los Angeles, CA, USA, in 1993, 1994, and 1999, respectively, all in electrical engineering. From 1999 to 2002, he worked as a Research Staff Member at HRL Laboratories, LLC in Malibu, California, USA. He worked as an Assistant Professor at the University of Pittsburgh in Pittsburgh, Pennsylvania, from 2002 until 2008. Since 2009, he has been with the School of Electrical Engineering and Computer Science, GIST, South Korea, where he is a tenured full professor. His technical works are in information theory, signal processing theory, communications/networking theory, and their applications. He received numerous prominent national prizes, including the Top 100 National Research and Development Award in 2012, the Top 50 Fundamental Research Achievements Award in 2013, the Science/Engineer of the Month in January 2014, and the Prime Minister's Commendation in April 2022. He also works on national policy and currently is serving as an advisory member of the Presidential Committee on Policy Planning. He is a current associate editor for IEEE Transactions on Cybernetics. He has published more than 100 SCI/SCIE journals. He is the director of the ITRC Blockchain Intelligence Center, which has national funding of up to $6 million for the next eight years to nurture Masters/Ph.D. students. He is also the director of the GIST Institute for Artificial Intelligence.

   He will serve as the WorldLand project's principal investigator, working on VRF and WorldLand consensus designs, and overseeing the whole WorldLand network development and testing process.

b. Prof. Youngsik Kim received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, in 2001, 2003, and 2007, respectively. Until 2010, he worked in Samsung Electronics' Semiconductor Division, researching and developing security hardware IPs for different embedded systems, including modular exponentiation hardware accelerators for RSA and elliptic-curve cryptography in smartcard devices and mobile application processors. He is currently a professor at Chosun University, Gwangju, South Korea. He is also a submitter for two candidate algorithms (McNie and pqsigRM) in the 1st round for the NIST PQC Standardization and three candidate algorithms in the Korean Competition for PQC. He is also a technical adviser for the Korean PQC Research Group (kpqc.or.kr), which organizes the NSRI-organized Korean Competition for PQC. He is selected as one of 2025's 100 Best Technology Leaders (for Cryptosystems) by the National Academy of Engineering of Korea. Postquantum cryptography, completely homomorphic encryption, and privacy-preserving machine learning are among his research interests.

He will take the role of leading VRF design and advise students for programming and documentation.

c. Prof. Dilbag Singh has received a Ph.D. degree in the field of Computer Science and Engineering from the Thapar Institute of Engineering and Technology, India in 2019. He has served as an assistant professor at three prestigious Indian universities: Chandigarh University, Manipal University Jaipur, and Bennett University. Image processing, computer vision, deep learning, metaheuristic approaches, and information security are among his research interests. He has published more than 80 research papers in SCI/SCIE indexed journals. He has also submitted 5 patents and published 3 books and 2 book chapters. His H-index is 32. He has also served as a lead guest editor/member of the editorial board of many SCI/SCIE indexed publications, including the Journal of Healthcare Engineering, Mathematical Problems in Engineering, Journal of Intelligent & Fuzzy Systems, and others. He was in the top 2% list issues by "World Ranking of Top 2% Scientists" in 2021.

   He will take the role of developing WorldLand protocol design and advise students on programming and documentation.

d. Dr. Manjit Kaur received a Master of Engineering degree in information technology from Punjab University, Chandigarh, India, in 2011, and a Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2019. She was an assistant professor at three well-known Indian universities: Chandigarh University in Mohali, India, Manipal University in Jaipur, India, and Bennett University in Greater Noida, India. In 2021, she moved to the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju, South Korea, where she is currently affiliated. PQ cryptography, completely homomorphic encryption, and privacy-preserving machine learning, as well as wireless sensor networks, digital image processing, and metaheuristic approaches, are among her research interests. She was in the top 2% list issues by "World Ranking of Top 2% Scientists," in 2021. She was part of the 14 Web of Science/Scopus indexed conferences.

   She will be in charge of designing the WorldLand protocol, setting up the testbed, and advising students on programming and testing.

8 Challenges* - Have you come across any obstacles thus far? If so, how have you attempted to tackle these issues? Have you been successful in overcoming them?

Challenge 1: Selection of Post-Quantum secure and efficient algorithm.

It has required a significant amount of work to identify and choose Post-Quantum secure and efficient algorithms capable of providing lightweight and secure PQ safe cryptosystems. As our goal was to find such an algorithm than can optimistically tradeoff between Keygen, Sign, and create time suitable for a global scale blockchain.

Solution for Challenge 1: We have reviewed a number of articles and websites and discovered some PQ secure algorithms such as Dilithium, Falcon, and Durandal which meet our objectives. Finally, we chose Durandal among the comparing algorithms since it takes substantially less time to Keygen, Sign, and Verify.

Challenge 2: Implementation of WorldLand and validation.

Solution for Challenge 2: Another major difficulty is the design and development of PoC. We have already implemented and successfully shown ECCPoW Ethereum in 2019 [R8]. The student researchers involved in that research have graduated from GIST. We have a new wave of researchers and professors joined in the center who are currently studying the ECCPoW suite while learning graduate-level mathematics, analysis tools, coding theory, cryptography, cryptocurrencies and blockchain programming. They are in the initial stage of their research catching up.

Nevertheless, we are better staffed now than before; we shall be able to build the WorldLand network for validation and testing purposes.

9 Additional support requests - Aside from funding and financial support, are there other resources that would help you or your team succeed?

Besides funding and financial support, it would be nice if the BIC center makes an MoU with the Ethereum foundation. Cooperative seminars, developer exchange programs, and joint research initiatives might all be avenues of collaboration. It would be great if Vitalik Buterin make a visit to the center at GIST for the MoU ceremony and participate in the WorldLand project kick-off meeting. During the project duration, we would like to host a global event in Seoul, Korea, to which prominent teams in the new consensus and deFi fields such as Algorand, Cardano, Polygon, Uniswap, Compound, and dYdX will be invited. Scholars in the fields of PQ security, such as Falcon, Durandal, and Dilithium, will also be invited.

Relevant publication of Team members

[R1] Y. Kim, R. K. Raman, Y.-S. Kim, L. R. Varshney, and N. R. Shanbhag, “Efficient Local Secret Sharing for Distributed Blockchain Systems,” IEEE Communications Letters, vol. 23, no. 2, pp. 282-285, Feb. 2019. (Corresponding Author) (Selected as 50 Popular Documents of IEEE Communications Letters 13 times since published)

[R2] Y. Kim, C. Guyot, and Y.-S. Kim, “On the Efficient Estimation of Min-Entropy,” IEEE Transactions on Information Forensic and Security, vol. 16, pp. 3013–3025, May 2021. (Corresponding Author) (Top 6.8% in COMPUTER SCIENCE, THEORY & METHODS, JCR 2020)

[R3] E. Lee, J.-W. Lee, J.-S. No, and Y.-S. Kim, “Minimax Approximation of Sign Function by Composite Polynomial for Homomorphic Comparison,” online published, IEEE Transactions on Dependable and Secure Computing, Aug. 2021. (Top 2.3% in COMPUTER SCIENCE, SOFTWARE ENGINEERING, JCR 2020)

[R4] J.-W. Lee, E. Lee, Y. Lee, Y.-S. Kim, and J.-S. No, “High-Precision Bootstrapping of RNS-CKKS Homomorphic Encryption Using Optimal Minimax Polynomial Approximation and Inverse Sine Function,” In: Canteaut A., Standaert FX. (eds) Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Computer Science, vol 12696. Springer, Cham. (Top Crypto Conference)

[R5] Y. Lee, J.-W. Lee, Y.-S. Kim, Y. Kim, J.-S. No, and H. Kang, “High-Precision Bootstrapping for Approximate Homomorphic Encryption by Error Variance Minimization,” accepted to EUROCRYPT 2022, Feb 2022. (Top Crypto Conference)

[R6] Hyoungsung Kim, Jehyuk Jang, Sangjun Park, and Heung-No Lee*, “Error-Correction Code Proof-of-Work on Ethereum”, IEEE Access, Vol. 9, pp. 135942-135952, Sep 2021. doi: https://doi.org/10.1109/ACCESS.2021.3113522. (Impact Factor: 3.367, IITP & Do-Yak project) Paper: (Open Access)

[R7] Jehyuk Jang and Heung-No Lee, “Profitable Double-Spending Attacks,” Applied Sciences, 10, 8477, Nov. 2020. doi: https://doi.org/10.3390/app10238477. (IF: 2.474, Do-Yak and IITP) Paper: (Open access) MATLAB evaluation script: https://codeocean.com/capsule/2308305/tree.

[R8] Hyunjun Jung, Heung-No Lee*, “ECCPoW: Error-Correction Code Based Proof-of-Work for ASIC Resistance”, *Symmetry*, June. 2020, 12(6), 988.

[R9] Sangjun Park, Haeung Choi and Heung-No Lee*, “Time-Variant Proof-of-Work using Error-Correction Codes”, Submitted to IEEE Trans. on Information Forensics and Security. (https://arxiv.org/abs/2006.12306).

References

[1] https://crypto8.com/2021/03/26/lighthouse-confirms-prototype-merge-between-ethereum-and-eth-2-0-with-99-98-less-energy-consumption/.

[2] "Ethereum's energy usage will soon decrease by ~99.95%", https://blog.ethereum.org/2021/05/18/country-power-no-more/.

[3] D'Arco, Paolo, Zahra Ebadi Ansaroudi, and Francesco Mogavero. "Multi-stage Proof-of-Works: Properties and Vulnerabilities." Cryptology ePrint Archive (2020). https://ia.cr/2020/1262

[4] Bob McElrath, "What's wrong with Proof-of-Stake," https://medium.com/@BobMcElrath/whats-wrong-with-proof-of-stake-77d4f370be15. (Accessed on April 13, 2022)

[5] Amy Castor, "Why Ethereum is switching to proof of stake and how it will work," March 4, 2022. https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/. (Accessed on April 13, 2022)

[6] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," Journal of Network and Computer Applications, Volume 182, 2021, https://doi.org/10.1016/j.jnca.2021.103035.

[7] Li, Wenting, Sébastien Andreina, Jens-Matthias Bohli, and Ghassan Karame. "Securing proof-of-stake blockchain protocols." In Data privacy management, cryptocurrencies and blockchain technology, pp. 297-315. Springer, Cham, 2017.

[8] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A Survey on Long-Range Attacks for Proof-of-Stake Protocols," IEEE Access, Vol. 7, 2019.

[9] McEliece, R.: A public key cryptosystem based on algebraic coding theory. DSN progress report, 42-44:114–116 (1978).

[10] Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Probl. Control and Inform. Theory, 15:19–34 (1986).

[11] Sidelnikov, Vladimir Michilovich, and Sergey O. Shestakov. "On insecurity of cryptosystems based on generalized Reed-Solomon codes." (1992): 439-444.

[12] Gabidulin, E., Paramonov, A., and Tretjakov, O.: Ideals over a non-commutative ring and their applications to cryptography. In Proc. Eurocrypt '91, volume 547 of LNCS. Springer Verlag (1991).

[13] Gabidulin, E., Ourivski, A., Honary, B., and Ammar, B.: Reducible rank codes and their applications to cryptography. IEEE Transactions on Information Theory, 49(12):3289–3293 (2003).

[14] Janwa, H. and Moreno, O.: McEliece public key cryptosystems using algebraic geometric codes. Designes, Codes and Cryptography, 8:293–307 (1996).

[15] Gaborit, P.: Shorter keys for code based cryptography. In Proc. of WCC 2005, pages 81–90 (2005)

[16] Sidelnikov, V.: A public-key cryptosystem based on binary Reed-Muller codes. Discrete Mathematics and Applications, 4 No. 3 (1994).

[17] Overbeck, R.: A new structural attack for GPT and variants. In Proc. of Mycrypt 2005, volume 3715 of LNCS, pages 50–63. Springer Verlag (2005).

[18] Lee, P. and Brickell, E.: An observation on the security of McEliece's public key cryptosystem. In Advances in Cryptology-EUROCRYPT'88, volume 330 of LNCS, pages 275–280. Springer Verlag (1989)

[19] Lyubashevsky, Vadim, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. "Crystals-dilithium." Submission to the NIST Post-Quantum Cryptography Standardization [NIS] (2017).

[20] Zhang, Xiangjun, Weiguo Wu, Shiyuan Yang, and Xiong Wang. "Falcon: a blockchain-based edge service migration framework in MEC." Mobile Information Systems 2020 (2020).

[21] Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G. (2019). Durandal: A Rank Metric Based Signature Scheme. In: Ishai, Y., Rijmen, V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science(), vol 11478. Springer, Cham. https://doi.org/10.1007/978-3-030-17659-4_25.

[22] Li, Zengpeng, Teik Guan Tan, Pawel Szalachowski, Vishal Sharma, and Jianying Zhou. "Post-Quantum VRF and its Applications in Future-Proof Blockchain System." arXiv preprint arXiv:2109.02012 (2021).

[23] Esgin, Muhammed F., Veronika Kuchta, Amin Sakzad, Ron Steinfeld, Zhenfei Zhang, Shifeng Sun, and Shumo Chu. "Practical post-quantum few-time verifiable random function with applications to algorand." In International Conference on Financial Cryptography and Data Security, pp. 560-578. Springer, Berlin, Heidelberg, 2021.

[24] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[25] Jung, Hyunjun, and Heung-No Lee. "ECCPoW: Error-Correction Code based Proof-of-Work for ASIC Resistance." *Symmetry* 12, no. 6 (2020): 988.

[26] Kim, Hyoungsung, Jehyuk Jang, Sangjun Park, and Heung-No Lee. "Error-Correction Code Proof-of-Work on Ethereum." *IEEE Access* 9 (2021): 135942-135952.

[27] Hang Dinh, Cristopher Moore, and Alexander Russell. 2011. McEliece and niederreiter cryptosystems that resist quantum fourier sampling attacks. In Proceedings of the 31st annual conference on Advances in cryptology (CRYPTO'11). Springer-Verlag, Berlin, Heidelberg, 761–779.

[28] G. Alagic et. al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," in National Institute of Standards and Technology Interagency or Internal Report 8309 (NISTIR 8309), 2020, doi: https://doi.org/10.6028/NIST.IR.8309.

[29] C. Monico, J. Rosenthal, and A. Shokrollahi, “Using low density parity check codes in the McEliece cryptosystem,” in IEEE International Symposium on Information Theory – ISIT’2000. IEEE, 2000, p. 215.

[30] M. Baldi and F. Chiaraluce, “Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes,” in IEEE Int. Symposium on Information Theory ISIT’07, 2007, pp. 2591 –2595.

[31] M. Baldi, M. Bodrato, and F. Chiaraluce, “A new analysis of the McEliece cryptosystem based on QC-LDPC codes,” in 6th Int. Conf. on Sec. and Cryptography for Networks. Springer, 2008, pp. 246–262.

[32] A. Otmani, J. Tillich, and L. Dallot, “Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes,” Special Issues of Mathematics in Computer Science, vol. 3, no. 2, pp. 129–140, Jan. 2010.

[33] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. L.S.M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In IEEE International Symposium on Information Theory – ISIT’2013, pages 2069–2073, Istambul, Turkey, 2013. IEEE.

[34] Jang, J.; Lee, H.-N. Profitable Double-Spending Attacks. Applied Sciences, 2020, 10, 8477, https://doi.org/10.3390/app10238477.

[35] Dolev, Danny, and H. Raymond Strong. "Authenticated algorithms for Byzantine agreement." *SIAM Journal on Computing* 12.4 (1983): 656-666.

[36] Heung-No Lee, Blockchain and Future Society, 4th Lecture Module: PoW Success Probability and Alone-Impossible-Together-Possible Theory, Massive Open Online Course Lecture Video at https://gist.edwith.org/bitcoin-tech, the lecture note available at https://infonet.gist.ac.kr/?page_id=8954, or https://infonet.gist.ac.kr/?page_id=7619, Oct. 31st, 2019.