Jewelz Whitepaper

I. Introduction

Jewelz is an up-and-coming cryptocurrency designed to revolutionize how the cryptocurrency industry works. Currently, most cryptocurrencies use large amounts of energy or are increasingly centralized. This is because the current systems for securing the blockchain are designed to use scarcity as a basis for security in a way that disproportionately benefits those with money to invest in the cryptocurrency. For Proof of Work the need to "have money to make money" is apparent in the fact that large investors have created massive mining farms to own a reasonable percentage of a network's computational power. In Proof of Stake, the percentage of mining rewards owned is proportional to the amount of coin that you have available to stake.

Jewelz is designed to make mining equal and accessible to all. Using the new Serial Proof of Work system, Jewelz removes the incentives for miners to create massively parallel mining farms. This increases both the eco-friendliness of mining by limiting the total power consumption of the Jewelz network and the equality of mining by placing all participants on even footing.

The Jewelz blockchain is designed to be a backend for the Jewelz platform, a collection of web and mobile applications that allow players to earn in-game rewards that can be transferred across any application on the platform or traded at an exchange for other cryptocurrencies or fiat currencies. The eventual goal of the Jewelz platform is to create an eLearning platform where students are rewarded for completing educational modules by earning Jewelz cryptocurrency.

The remainder of this whitepaper is organized as follows. Section II provides background on the environment that Jewelz is entering, including the basics of blockchain and the limitations of existing cryptocurrencies and how Jewelz plans to address these. Sections III and IV describe the way mining and validation of candidate blocks works on the Jewelz blockchain. Section V addresses potential security concerns about the Jewelz platform. Section VI discusses the cryptoeconomics of Jewelz and Section VII describes the educational component of the Jewelz platform. Sections VIII and IX provide an introduction to the Jewelz roadmap and close with a recap of the potential and innovation of the Jewelz platform.

II. Background

The cryptocurrency space is crowded with well over a thousand different offerings. However many of these options are unsustainable or have veered away from the ideals of blockchain by increasing centralization. The Jewelz cryptocurrency is designed to be a truly sustainable, decentralized cryptocurrency and the foundation for the Jewelz ecosystem of gaming and eLearning applications.

A Brief History of Blockchain

Cryptocurrency is a relatively new method of performing financial transactions in a decentralized and trustless way. The first cryptocurrency, Bitcoin, was launched in January 2009 by Satoshi Nakamoto. Nakamoto created Bitcoin to address issues that he saw with the traditional financial system, where currencies were completely under the control of centralized organizations.

At the time, the world was in the middle of the Great Recession when the world economy was suffering due to the burst of the real estate bubble. The bubble was created by banks making loans to people who were incapable of paying them back, causing banks to fail and need government bailouts when the bubble burst. In the first or *genesis* block of Bitcoin, Satoshi included that day's headline from a British newspaper stating that the British government was on the verge of a second bailout of banks. This served the dual purposes of proving that the genesis block was actually created on that date and critiquing the traditional financial system that Bitcoin was designed to replace.

Bitcoin was designed to be a means of transferring value between two people in a decentralized manner. In order for Bitcoin to be decentralized, Satoshi needed to create a way of storing the ledger of transactions in a distributed yet trustworthy way. To do this, Satoshi invented the blockchain, which uses cryptography to verify that no-one can modify the contents of a *block* of transactions after it is created and that anyone can verify the authenticity of a copy of the blockchain without needing to trust the person who gave it to them. By storing all transactions on the blockchain, cryptocurrency transactions can be verified by the entire network and no-one can control the blockchain because control requires ownership of more resources than the rest of the blockchain put together.

Bitcoin was designed to be solely a means for performing financial transactions on the blockchain. While it does have some support for writing programs that execute on the blockchain, this functionality is intended to be used to define the requirements for transactions to be completed. For example, a transaction may require approval from two or more parties to be completed. Bitcoin scripting was deliberately designed not to be Turing Complete, meaning that it lacks some of the functionality of a full computer. When Vitalik Buterin proposed changing this, his proposal was rejected.

After his proposal was rejected, Buterin began development on the Ethereum cryptocurrency. While other cryptocurrencies were created before Ethereum, Ethereum was the first smart contract platform, meaning that developers could write programs that ran on the blockchain and that the Ethereum Virtual Machine (the "computer" running on the Ethereum blockchain) was Turing Complete.

Bitcoin and Ethereum have been the bases for over a thousand derivative cryptocurrencies. Early cryptocurrencies based off of Bitcoin made minor changes to the Bitcoin protocol to address its limitations but retained its focus on financial transactions. With the creation of Ethereum, cryptocurrencies were built on top of the Ethereum platform, using its smart contract functionality and built-in features to create cryptocurrencies that provided services in exchange for tokens. Today, thousands of cryptocurrencies exist, providing a wide variety of services to their users.

Cryptocurrency Mining

To understand how Jewelz fits into the cryptocurrency landscape, it is necessary to understand how security works on the blockchain. The distributed ledger needs to be protected against modification despite the fact that it is stored on untrusted machines. Several methods of doing this have been proposed and implemented by different cryptocurrencies. The most common two are called Proof of Work and Proof of Stake.

In Proof of Work, the community of miners races to find a possible solution to a “hard” cryptography problem and the winner earns the right to generate the next block and earn the associated reward. This problem can only be solved by guessing a random value and then checking if it produces a valid solution. The security of a Proof of Work blockchain is based on the fact that an attacker needs to do the same amount of work to create a fake block as the entire network did to create a real one. Since this requires as much computational power as the rest of the network put together, this quickly becomes infeasible with a large cryptocurrency network.

In Proof of Stake systems, users “stake” a portion of their cryptocurrency (meaning that they resolve not to spend it) in order to be eligible to mine potential blocks. The probability that a user will be the one selected to mine a block is roughly proportional to the ratio of the size of the user’s stake to the number of all staked coins. To control a Proof of Stake blockchain, an attacker needs to own a high enough percentage of all of the staked coins to have a high probability of being selected to create a given block. Since coin supplies are limited, the Law of Supply and Demand states that buying up enough coins to achieve this will be infeasibly expensive.

Limitations of Existing Cryptocurrencies

Cryptocurrencies can be roughly classified based upon their security algorithms and Proof of Work and Proof of Stake are the most common algorithms. Both of these algorithms have limitations that make them impractical for long-term, scalable usage.

Limitations of Proof of Work

The Proof of Work algorithm is infeasible in the long term both economically and ecologically. When Satoshi Nakamoto created Bitcoin, anyone could mine Bitcoin since the population was small (sometimes only three people were mining at any given time). As Bitcoin has grown in popularity and value, cryptocurrency mining has evolved from a hobby to a business and large-scale mining rigs and mining pools have been created. These larger-scale operations and coalitions have made independent mining economically infeasible, forcing miners to join existing coalitions.

This has caused a centralization of power within the Bitcoin network to the point where one mining pool had to voluntarily divide in 2014 due to fears that it would control over half of the Bitcoin network's mining power, which would destroy the security of the Bitcoin blockchain. Bitcoin was designed to be a decentralized alternative to traditional currencies and the growing power of Bitcoin mining pools runs directly against its founding principles.

The Proof of Work algorithm also has dramatic ecological impacts. The complexity of the cryptographic problem that miners race to solve is designed to scale with the size and computational power of the network. This means that the amount of power used to fuel the Bitcoin network is only governed by economic pressures, i.e. as long as mining is profitable people will continue to mine. As a result, the Bitcoin Network consumes a massive amount of energy to perform calculations that serve no purpose other than securing the blockchain. At the end of December 2017, the energy consumption of the Bitcoin network was higher than Qatar (ranked 58th in the world in terms of energy consumption). As Bitcoin and other Proof of Work cryptocurrencies increase in usage and popularity, the energy consumption of cryptocurrency mining will continue to grow.

Limitations of Proof of Stake

Proof of Stake is an alternative to Proof of Work that does not share its high energy requirements. In fact, Ethereum was designed from the start to originally use Proof of Work with a forced transition to Proof of Stake built into the development plan. However, Proof of Stake also has issues that limit its ability to be decentralized and operate in the long term.

Proof of Stake is based on the principle that the rich get richer. The percentage of the time that a miner is selected to mine a block and earn the associated reward is roughly proportional to the percentage of staked coins that the miner owns. This means that only those who have the money to stake coins earn any new coins (outside of being the recipient of transactions) and everyone who participates in the network by making transactions loses coins over time to transaction fees (which go to the rest). Over time, the percentage of the network's coins controlled by the rich will increase if they choose not to use them, causing the cryptocurrency to become increasingly centralized. This limits the lifetime of a Proof of Stake network since eventually the richest user on the network could control enough of the cryptocurrency to break the security of the blockchain.

How Jewelz Intends to Revolutionize Cryptocurrency

Jewelz intends to return to the ideals of cryptocurrency by becoming a truly decentralized cryptocurrency. The Proof of Work and Proof of Stake algorithms are both based upon the principles that the rich get richer, causing control of the blockchain to become increasingly centralized. The energy consumption of Proof of Work and the design of Proof of Stake make both of them unsustainable as active currencies in the long term.

In Proof of Work, each miner's ability to mine is limited only by the amount of parallel processing power under their control. The creates a system with high energy consumption and that favors those with the ability to invest heavily in dedicated mining systems.

Jewelz intends to move away from this power-hungry, centralized model by removing the parallel processing component of Proof of Work calculations. Jewelz's Serial Proof of Work algorithm uses cryptographic principles to ensure that miners can create a valid block only by trying options in sequence rather than in parallel. This reduces the energy consumption of Jewelz and prevents the centralization of mining power through the creation of large-scale mining systems, making Jewelz a fairer, more sustainable option than most existing cryptocurrencies.

III. Mining Jewelz

Unlike other cryptocurrencies, Jewelz is based on a Serial Proof of Work algorithm for block mining. This protocol allows Jewelz to avoid the high energy consumption and unbalanced mining reward distribution faced by other cryptocurrencies. The first part of this section describes the miner registration process required by Jewelz. This protects Jewelz mining against unfair parallelization. The remainder of the section provides a brief description of the Serial Proof of Work algorithm that allows Jewelz to remain low-energy and equal opportunity for miners.

Miner registration

Unlike many cryptocurrencies, Jewelz requires miners to perform registration before being allowed to mine. This is intended to prevent users from creating multiple accounts and performing mining in parallel.

The Jewelz blockchain is intended to be accessed via applications like games and eLearning systems. Miner registration is performed via an in-app purchase shared across all applications in the Jewelz ecosystem. By performing this one-time purchase, miners gain the ability to contribute to the blockchain and earn rewards through mining and block validation.

Serial Proof of Work Algorithm

Jewelz's Serial Proof of Work algorithm requires that block miners perform Proof of Work calculations sequentially, enforced by cryptographic principles. This is accomplished by requiring miners to create and publish a hash chain as part of the mining operation. A hash chain is a series of Proof of Work calculations such that the nonce used in one attempt is the output of the previous Proof of Work attempt. As these outputs cannot be determined in advance, miners must test each potential nonce in sequence rather than in parallel.

To avoid the chance of unfair parallelization, the Jewelz blockchain requires miners to start their hash chains using a certain, public value. If a miner is mining independently, this value is the SHA512 hash of their public key. Miners mining as part of a pool must use the concatenation of their own public key and that of the pool's leader. Since Jewelz's miner registration process limits each user to a single mining account, this restricts a miner's ability to gain an unfair advantage by performing parallelized mining operations.

In order to prevent miners from performing Serial Proof of Work calculations in parallel using permutations of the transaction list, Jewelz includes strict guidelines for what should be included within a block. Each transaction in Jewelz must be timestamped and signed with the sender's public key. When a node receives a transaction, they should also record the timestamp of the time of receipt.

A block must contain all transactions beginning with the first transaction not included in the previous block and going up to a pre-determined cutoff time. The purpose of the cutoff is to remove the potential for network latency issues causing nodes to operate with differing transaction lists.

To prove that a candidate for the blockchain was produced using a valid Serial Proof of Work hash chain, miners must include information about the computed hash chain as part of their block. Since inclusion of the entire chain is infeasible due to memory requirements, miners will break the hash chain into chunks of a pre-determined size and include the output value of the final Proof of Work attempt of each chunk within the block. This allows anyone to easily validate the entire hash chain or any chunk of it by starting at the output of the previous chunk and verifying that the output of the current chunk was reached in the reported number of steps.

IV. Jewelz Block Validation

The Jewelz cryptocurrency uses Serial Proof of Work to ensure that no users can gain an unfair advantage in mining through the use of specialized mining hardware or heavy investment in the cryptocurrency. A consequence of this is that validation of a Jewelz block candidate is more complicated that validation of a block in Proof of Work.

The only necessary requirement for a Proof of Work block is that its Proof of Work calculation meets the established difficulty target, a requirement that can be trivially verified by anyone with access to the blockchain. In addition to this, Serial Proof of Work mandates how a miner reaches the target result, which requires more effort to validate.

Jewelz includes a formal validation stage to ensure that a block candidate is correct before it can be added to the blockchain. This section first describes the method by which consensus on the transaction list is reached, followed by how users are determined to be eligible to participate in validation of a given block, and finally a description of the Jewelz validation protocol.

Transaction List Consensus

Jewelz's Serial Proof of Work algorithm requires that all miners use the same transaction list for mining. Otherwise, a user could mine in parallel using various permutations of the transaction list. Since requiring consensus on the transaction list before performing mining is undesirable, miners reach an implied consensus by selecting and ordering transactions based upon public criteria. This means that a candidate block's transaction list must be checked to reveal the possibility of cheating.

When a block candidate is released, nodes should compare their transaction list with the one reported in the block. If they differ, a challenge should be issued by the node. Each node should record both the reported timestamp and time of receipt for a given transaction. This allows nodes to resolve challenges by consensus by voting whether or not the propagation delay of a transaction across the network is plausible. Once a set minimum number or percentage of users are in agreement, the block candidate's transaction list is accepted or rejected. If no challenges are made, no consensus vote is required.

Validation Eligibility

One of the primary goals of Jewelz is to create a blockchain where all users have the ability to earn mining rewards. However, Jewelz block validation requires speed and parallelization, which gives an advantage to users with access to dedicated hardware. To avoid the possibility of all validation rewards being controlled by a subset of users and to decrease the energy requirements of block validation, Jewelz has implemented a system to determine which users are eligible to participate in validation for a given block.

Eligibility to validate a block is determined by comparing the SHA512 hash of the previous block on the blockchain to the miner's public key. If the value of the user's public key modulo a given value is less than the hash of the block modulo the same value, then the user is eligible to participate in block validation. The value of the modulus will be updated over the life of the Jewelz blockchain to ensure that enough Jewelz users are eligible to validate a given block without opening validation up to the entire Jewelz network.

Jewelz Block Validation

Block validation in Jewelz is structured as a race where a set number of finalists will be rewarded for its participation. Each eligible validator is free to participate and is encouraged to use parallel processing to validate the entirety of the candidate block's hash chain as quickly as possible. This is intended to perform validation quickly so that publishing of valid blocks is delayed by the minimum amount of time possible.

Validators can use the reported chunk waypoints included within the candidate block to parallelize their work. Each chunk can be validated independently by testing if a hash chain beginning with the output of the previous block produces the reported output after the set number of steps. A block's hash chain is validated if every chunk has been checked.

A validator reports completion of block validation by reporting the number of an invalid chunk if one is found or that all chunks are valid. If no validator claims a chunk is invalid after a set interval, the candidate is added to the blockchain and the first K validators are rewarded for their efforts.

If a validator reports a chunk as invalid, all Jewelz users are invited to check the validity of the reported chunk and report if they find it correct. After a consensus of a set number or percentage of Jewelz users is reached, rewards and penalties are issued. If a validator reported an incorrect result (valid if it is invalid or vice versa), they are fined twice the expected validation reward. A miner producing a block with an invalid chunk is fined twice the expected mining reward. These penalties are divided among the validators who correctly verified the chunk's validity (up to the number of validators needed for consensus). These penalties disincentivize cheating in mining or validation and incentive swift verification of invalid chunks.

V. Jewelz Security Considerations

By using the Serial Proof of Work algorithm for mining, Jewelz has increased the target surface for potential malicious miners. The security of the blockchain against cheating in Proof of Work and Proof of Stake cryptocurrencies has been thoroughly explored. By adding requirements for serialization of mining, Jewelz opens the door for miners to gain advantages in other ways.

The three main threats to the principles of the Jewelz cryptocurrency are unfair parallelization of mining, generation of invalid blocks, and cheating during the validation procedure. Here, each threat will be briefly discussed as well as the steps taken to mitigate it in the Jewelz cryptocurrency. <For a more detailed analysis, please review the Jewelz redpaper.>

Unfair Parallelization

Jewelz aims to make mining accessible to the average user by enforcing serialization during mining. This removes the advantages gained by investment in large mining rigs and provides ecological and economic benefits to the cryptocurrency. However, this creates the possibility that miners can gain unfair advantages by finding methods to parallelize their mining operations. Jewelz's solutions to potential parallelization schemes are described in the Mining and Validation sections of this document. Parallelization by registering multiple mining accounts is restricted via Jewelz's registration process. Permuting the transaction list is prevented by Jewelz's requirements for inclusion in the transaction list and checked during block validation. The entirety of a block candidate's hash chain is checked during validation, preventing miners from inserting a fake Serial Proof of Work attempt to move from an unsuccessful hash chain to a successful one discovered via parallel processing.

Fake block generation

The validity of blocks generated by Serial Proof of Work is more difficult to check than Proof of Work blocks. A miner could create a candidate block where only a single hash is reported incorrectly, allowing them to create a hash chain via parallelization. To guarantee that every link in the hash chain is checked, Jewelz has a formal validation procedure that incentivizes users to check the entire hash chain.

Cheating in Validation

Since block validation allows users to earn rewards using parallel processing and is structured as a race, users may be incentivized to cheat in validation to earn rewards. One method of doing so would be to report that a block is correct without checking the entire block. To disincentivize cheating, incorrectly reporting the validity of a chunk carries a heavy penalty.

VII. Jewelz Cryptoeconomics

Jewelz is a cryptocurrency designed to be the backend for an application platform and using the revolutionary Serial Proof of Work algorithm for security. Both of these factors affect how values moves through the platform as described here.

Game Integration

The Jewelz cryptocurrency is completely integrated with the games, eLearning platforms, and other applications that make up the Jewelz ecosystem. This has the dual benefit of providing a method to incentivize gaming and learning through interaction with the Jewelz environment and incentivizing the use rather than storage of the Jewelz cryptocurrency.

By using Jewelz as an in-game cryptocurrency, users are incentivized to spend Jewelz in order to earn rewards and unlock new content. This should help increase the circulation of Jewelz and stabilize the price of the cryptocurrency. By tying the value of Jewelz to in-game purchases with certain expected values, the value of Jewelz will be further stabilized as users will be disinclined to sell Jewelz at less than their worth or purchase them for greater than their worth.

Effects of Serial Proof of Work

One of the main purposes of the Serial Proof of Work algorithm used in Jewelz is to reduce the centralization of power present in many existing cryptocurrencies. In Proof of Work and Proof of Stake systems, it “takes money to make money” since the ability to earn block rewards is dependent on investments either in large-scale mining equipment (for Proof of Work) or large amounts of cryptocurrency to stake (for Proof of Stake). This squeezes small-scale miners out since the majority of block rewards go to large organizations.

Serial Proof of Work removes the advantage that large-scale mining rigs give to miners. By enforcing serialization of mining, Jewelz significantly levels the playing field, allowing any Jewelz user to have a meaningful chance to mine Jewelz. This spreads mining rewards more evenly throughout the Jewelz community, increasing the stability of the coin’s value and removing the threat of value loss due to sell-offs by a small number of powerful investors.

VIII. Jewelz and Education

User education is one of the central goals of the Jewelz cryptocurrency. The Jewelz cryptocurrency is designed to integrate with the Jewelz Platform, a collection of games and eLearning applications that use Jewelz as an in-game currency.

The educational mission of Jewelz begins with the first game on the Jewelz platform, AllMine. As part of the AllMine game, users will have the opportunity to learn and answer questions about the basic principles of cryptocurrency. As a reward for correct answers, players will be rewarded with Jewelz cryptocurrency which can be used to purchase in-game rewards or be traded.

Once the Jewelz platform has been launched, development of Jewelz University will begin. The purpose of Jewelz University is to enable users to be incentivized to pursue their educational interests. Users will be encouraged to develop educational modules in their areas of expertise to be approved and added to the offerings at Jewelz University. Upon completion of a module, students will be earn an opportunity to mine Jewelz, giving them the chance to earn a reward for their educational efforts. Course developers will receive a set number of mining opportunities upon approval of their course offering and have the opportunity to earn additional rewards based upon their course's popularity and user reviews. This ensures that Jewelz University contains high-quality content of value to its users.

The goals of the Jewelz cryptocurrency are to make cryptocurrency accessible to all users and to create a platform for incentivized learning. The Jewelz platform is designed to create a cryptocurrency with real value through integration with mobile games. This source of value makes it possible to provide real incentives for pursuing educational interests and creates a beneficial flow of value where users can earn Jewelz through pursuing education and then apply it to improving their entertainment experience on the Jewelz platform.

IX. Jewelz Roadmap

The AllMine puzzle game is the first game on the Jewelz platform and is scheduled for release in Summer 2018. The game lets players collect Adoraboos and build Utopias for them to live in. Ingame questions about cryptocurrency topics help to introduce players to the basics of blockchain and cryptocurrency while earning Jewelz cryptocurrency stored on a traditional Proof of Work blockchain (named Jewelz Red).

The release of the Serial Proof of Work Jewelz blockchain (named Jewelz Diamond) is currently scheduled for early-to-mid 2020. This blockchain will bring all of the benefits of Serial Proof of Work to the Jewelz platform and create a sustainable foundation for the Jewelz platform. From there, the ability to develop for and interact with the Jewelz blockchain will be opened up via an API.

Finally, the Jewelz platform will be used as the core of an incentivized eLearning system. Developers can create eLearning modules to be included in the Jewelz environment and will be rewarded with Jewelz upon integration of their module into the platform with bonuses based on usage and community reviews. Players can learn about topics that interest them and be rewarded with Jewelz cryptocurrency upon completion of modules. This cryptocurrency will be tradable for other cryptocurrencies or fiat currency on exchanges or usable for upgrades within any game on the Jewelz platform.

X. Conclusions

Jewelz is a cryptocurrency that uses Serial Proof of Work to create a sustainable, decentralized cryptocurrency. By removing the ability for value to be centralized in the hands of those capable of investing heavily into the platform, Jewelz can create a mining “middle-class” and become more stable in value. By supporting a platform with a variety of games and other applications, the Jewelz cryptocurrency further stabilizes its value by tying it directly to real-world sources of value.

This stability of value is important to Jewelz’s long-term goal of being an incentivized eLearning platform. By incentivizing both students and educational module creators, the Jewelz platform can become a self-sustaining eLearning platform where students are rewarded for following their interests.