**WHITE PAPER**

****

**0x35131617a66472F9f0D384F41BbCCa7c999A149e**

**Disclosure**: The information described in this paper is preliminary and subject to change at any time. Furthermore, this paper may contain forward-looking statements. Forward-looking statements generally relate to future events or our future performance. This includes, but is not limited to, Bitcon1’s projected performance; the expected development of its business and projects; execution of its vision and growth strategy; and completion of projects that are currently underway, in development or otherwise under consideration. Forward-looking statements repre-sent our management's beliefs and assumptions only as of the date of this presentation. These statements are not guarantees of future performance and undue reliance should not be placed on them. Such forward-looking statements necessarily involve known and unknown risks, which may cause actual performance and results in future periods to differ materially from any projections expressed or implied herein. Avalanche undertakes no obligation to update forward-looking statements. Although forward-looking statements are our best prediction at the time they are made, there can be no assurance that they will prove to be accurate, as actual results and future events could differ materially. The reader is cautioned not to place undue reliance on forward-looking statements.

www.bitcon1.com | www.bitcon1.co | www.bitcon1.io

Email: info@bitcon1.com

Powered & Partner with NovusZilla Ltd. UK UAE

**Abstract**. This paper discusses the key implementation details, in particular the token economics (tokenomics), of the native token of the Novuszilla platform, called $Bitcon1. This paper provides an architectural overview of the first release of the Novuszilla platform, codenamed Novuszilla aurora . For details on the economics of the native token, labeled $Bitcon1, we guide the reader to the token dynamics paper. The native token secures the network, pays for fees, and provides the basic unit of account between the multiple blockchains deployed on the larger Novuszilla network. For additional details on Novuszilla, which serves as a versatile and universal platform, allowing anyone to launch new blockchains with their own rules, 10 virtual machines, and validator sets, we guide the reader to either the accompanying architectural paper [1] or the Novuszilla docs [2].

Bitcon1 is a project that began in 2022 as an effort to change the way cryptocurrencies are designed and developed. The overall focus beyond a particular set of innovations is to provide a more balanced and sustainable ecosystem that better accounts for the needs of its users as well as other systems seeking integration. The BitCon1 aims to build a community interested in virtual assets integrated with Web 3.0 and Metaverse. BitCon1 team builds an all in one crypto platform, comprising of a virtual world which introduces you with the Metaverse. Where users can explore, build, and create monetized assets like NFT’s which further includes Metaverse avtar, Crypto corgis, Trading cards etc. on Novuszilla Multicurrency Exchange.In addition, Novuszilla introduces the most reliable and economical crypto trading experience for users by coming up with Novuszilla's crypto exchange, integrated with a safe and secure crypto wallet. Novuszilla is build for a community interested in getting into a space like metaverse and virtual world, with a fully automated smart contract that increases its efficiency and staking rewards. In the spirit of many open source projects, it embraces a collection of design principles, engineering best practices and avenues for exploration. These include the following:

● Separation of accounting and computation into different layers

● Implementation of core components in highly modular functional code

● Small groups of academics and developers competing with peer reviewed research

● Heavy use of interdisciplinary teams including early use of InfoSec experts

● Fast iteration between white papers, implementation and new research required to correct issues discovered during review

● Building in the ability to upgrade post-deployed systems without destroying the network

● Development of a decentralized funding mechanism for future work

Bitcon1 is being used as a hope for a lot of the population, by being the ultimate mode of fundraising for the rising talents. Bitcon1 is used to trade in an exclusive NFT marketplace platform, which can trade users NFT’s to a large database; connected to multiple nodes - NFT Marketplaces from all over the world. Bitcon1 is mainly used to trade four categories of NFTs- Celebrity NFTs, Talent NFTs, Players NFTs and user minted NFTs. This is an exclusive opportunity for all the fans to have a hold over their favorite artist NFT’s, by collecting their memorable moments. The world needs ideas and Innovation to make progress against the many problems we face. Creative and talented people that can contribute to this important work are everywhere, but the opportunity to develop is limited to only a small number of well-off children. As a consequence of this, we all – the entire world population – are missing out on the creativity and innovations that would enrich our world and help us move forward. NFTs available on the NFT marketplace fall into these four categories and give opportunities to every talent to showcase their artwork. With the use of Bitcon1 it becomes an effortless experience for the users to trade NFTs.

The economic model of any new digital currency/asset is one of the most critical components of the platform that the asset resides on. This is especially true for the native token of a self-sovereign, permission-less platform, like Bitcon1. In this paper, we discuss the economic design of the native token, called $Bitcon1. The discussion is broken down into the governance properties of the token, its supply, minting (rewards) function of stakers, and other pertinent economics details, such as the transactional economy.

**These are the key takeaway properties of the design of the $Bitcon1 economics model:**

-The resources spent by a validator for staking are proportional to that validator’s total  stake.

- The rewards accumulated by a validator for validating are proportional to that validator’s total stake.

- Since Bitcon1 is leaderless, there are no “rich-get-richer” compounding effects.

- Validators that lock their stake for longer are rewarded more.

- Validators are incentivized to stay online and operate correctly as their rewards are based on proof-of-uptime and proof-of-correctness.

-$Bitcon1 is a capped-supply token, with a maximum cap of 250 million tokens.

-While capped, $Bitcon1 is still governable. The rate at which the maximum cap is reached is subject to governance.

**INTRODUCTION**

Bitcon1 is the Native cryptocurrency of Novuszilla platform, It is a high-performance, scalable, customizable, and secure blockchain platform. It targets three 15 broad use cases:

– Building application-specific blockchains, spanning permissioned (private) and permissionless (public) deployments.

– Building and launching highly scalable and decentralized applications (Dapps).

– Building arbitrarily complex digital assets with custom rules, covenants, and riders (smart assets).

The overarching aim of bitcon1 is to provide a unifying platform for the creation, transfer, and trade of digital assets.

By construction, Bitcon1 possesses the following properties:

Scalable Bitcon1 is designed to be massively scalable, robust, and efficient. The core consensus engine is able to support a global network of potentially hundreds of millions of internet-connected, low and high powered devices that operate seamlessly, with low latencies and very high transactions per second.

Secure Bitcon1 is designed to be robust and achieve high security. Classical consensus protocols are designed to withstand up to f attackers, and fail completely when faced with an attacker of size f + 1 or larger, and Nakamoto consensus provides no security when 51% of the miners are Byzantine. In contrast, Bitcon1 provides a very strong guarantee of safety when the attacker is below a certain threshold, which can be parametrized by the system designer, and it provides graceful degradation when the attacker exceeds this threshold. It can uphold safety (but not liveness) guarantees even when the attacker exceeds 51%. It is the first permissionless system to provide such strong security guarantees.

Decentralized Bitcon1 is designed to provide unprecedented decentralization. This implies a commitment to multiple client implementations and no centralized control of any kind. The ecosystem is designed to avoid divisions between classes of users with different interests. Crucially, there is no distinction between miners,

developers, and users. Governable and Democratic $ Bitcon1 is a highly inclusive platform, which enables anyone to connect to its

network and participate in validation and first-hand in governance. Any token holder can have a vote in selecting key financial parameters and in choosing how the system evolves.

Interoperable and Flexible Bitcon1 is designed to be a universal and flexible infrastructure for a multitude of blockchains/assets, where the base $ Bitcon1 is used for security and as a unit of account for exchange. The

system is intended to support, in a value-neutral fashion, many blockchains to be built on top. The platform is designed from the ground up to make it easy to port existing blockchains onto it, to import balances, to support multiple scripting languages and virtual machines, and to meaningfully support multiple deployment scenarios. Outline The rest of this paper is broken down into four major sections. Section 2 outlines the details of the

engine that powers the platform. Section 3 discusses the architectural model behind the platform, including subnetworks, virtual machines, bootstrapping, membership, and staking. Section 4 explains the governance model that enables dynamic changes to key economic parameters. Finally, in Section 5 explores various peripheral topics of interest, including potential optimizations, post-quantum cryptography, and realistic adversaries. Novuszilla is a complete one stop marketplace for virtual assets which includes crypto exchange, OTC system, crypto wallet, Metaverse betting applications, Staking, immortal virtual avatar, Native crypto currency of The novuszilla- BitCon1 coin and NFT marketplace, majorly connecting the userbase with the entertainment, sports and other industries. The NFT marketplace where you can create, sell and buy NFT’s. Our NFT marketplace comes up with exclusive celebrity NFTs, which can be traded with Bnb or Novus coins. The Novuszilla NFT marketplace also benefits unrecognised creators to potray their talent through the means of NFTs. We come up with a Decentralized peer to peer crypto exchange which charges no transaction fees, trading experience with zero brokerage. The Crypto market has been growing gradually over the last few years. As more and more young investors are excited to explore newer investment options, Novuszilla's team has made sure to bring the best experience and service whether its for crypto or NFT’s. We have made sure to help bring our entertainment industry onto the blockchain, stepping together into the new era of technology via BitCon1 Coin. Let’s dive deep into the concept of BitCon1 coin being integrated with a decentralized finance based system.

**Governance**

We initiate our survey of the Bitcon1 economic design by first discussing governance, as it plays a critical role within future components. To enable the system to adapt to changing economic conditions, the Bitcon1 platform enables key system parameters to be modified dynamically based on user input. A workable process for finding globally acceptable values for system parameters is critical for decentralized systems without custodians. Bitcon1 can use its consensus mechanism to build a system that allows anyone to propose special

transactions that are, in essence, system-wide polls. Any participating node may issue such proposals. Reward rate is an important parameter that affects any currency, whether digital or fiat. Unfortunately, cryptocurrencies that fix this parameter might face various issues, including deflation or hyper-inflation. To that end, the reward rate will be subject to governance,within pre-established boundaries. This will allow token holders to choose the rate at which$Bitcon1 reaches its capped supply.Transaction fees, denoted by the set F, will also eventually be governed. F is effectively a tuple which describes the fees associated with the various instructions and transactions supported in future releases. Finally, staking times and amounts will also be governable.

Ultimately, we note that governance in $Bitcon1 has hysteresis, meaning that changes to parameters are highly dependent on their recent changes. There are two limits associated with each governable parameter: time and range. Once a parameter is changed using a governance transaction, it becomes very difficult to change it immediately and by a large amount.

$Bitcon1 has a capped-supply of 250,000,000 (250M) tokens. The genesis block will have 125M(bep-20) $Bitcon1 tokens. The rest of the 125M tokens will be minted on Novuszilla Blockchain. The principle of the emissions function chosen for Bitcon1 is simple: reach a capped supply, in a fashion similar to Bitcoin’s emissions curve, and yet maintain the ability to

govern the rate at which the system reaches this limit.

**Proof of Stake**

Using proof of stake for a cryptocurrency is a hotly debated design choice, however because it adds a mechanism to introduce secure voting, has more capacity to scale, and permits moreexotic incentive schemes, we decided to embrace it.  Our proof of stake protocol is called Ouroboros and it has been designed by an extremely talented team of cryptographers from five academic institutions led by Professor Stefan of the University of Bath. The core innovation it brings beyond being proven secure using a rigorous cryptographic model is a modular and flexible design that allows for the composition of many protocols to enhance functionality. This modularity allows for features such as delegation, sidechains, subscribable checkpoints, better data structures for light clients, different forms of random number generation and even different synchronization assumptions. As a network develops from having thousands to millions and even billions of users, the requirements of its consensus algorithm will also change. Thus, it is vital to have enough flexibility to accommodate these changes and thereby future-proof the heart of a cryptocurrency.

**Social Elements of Money**

Cryptocurrencies are a prime example of the social component of money. When restricting analysis solely to technology, there is little difference between Bitcoin and Litecoin and even less so between Ethereum and Ethereum Classic. Yet, both Litecoin and Ethereum Classic maintain large market capitalizations and robust, dynamic communities as well as their own social mandates. It can be argued that a large part of the value of a cryptocurrency is derived from its community, the way it uses the currency, and its level of engagement in the currency’s evolution. Furthering the thought, currencies such as Dash have even integrated systems directly into the protocol to engage their community in deciding what should be a priority to develop and fund.

The vast diversity of cryptocurrencies also provides evidence for their social elements. Disagreements about philosophy, monetary policy, or even just between the core developers lead to fragmentation and forks. Yet unlike their cryptocurrency counterparts, fiat currencies of superpowers tend to survive political shifts and local disagreements without a currency crisis or

mass exodus. Therefore, it seems that there are elements of legacy systems that are missing from the cryptocurrency industry. We argue — and have inculcated into the Bitcon1’s roadmap – that users of a protocol need incentives to understand the social contract behind their protocol and have the freedom to propose changes in a productive way. This freedom extends to every aspect of a value exchange system, from deciding how markets should be regulated to which projects should be funded. Yet it cannot be brokered through centralized actors nor require

some special credential that could be co-opted by a well funded minority.

Bitcon1 will implement a system of overlay protocols built on top of CSL to accommodate the needs of its users.

First, regardless of the success of a crowdsale to bootstrap development, funds will eventually dissipate. Hence, Bitcon1 will include a decentralized trust funded from monotonically decreasing inflation and transaction fees. Any user should be eligible to request funds from the trust by a ballot system and the stakeholders of CSL vote on who becomes a beneficiary. The process creates a productive feedback loop seen in other cryptocurrencies with treasury/trust systems, such  as Dash, by   starting a conversation about who should and should not be funded.  Funding discussions force a relation of long and short term goals, the cryptocurrency social contract, priorities and the belief in value creation with particular proposals. This conversation means that the community is constantly evaluating and debating its beliefs against possible roadmaps.

Second, our hope is that Bitcon1 will eventually include a formal, blockchain based system to propose and vote on both soft and hard forks. Bitcoin with its block size debate, Ethereum with the DAO fork, and many other cryptocurrencies besides have endured long standing and, in frequent cases, unresolved arguments over the technical and moral direction of the codebase. It can and should be argued that many of these disagreements, and the fracturing of the community that results when action is taken, are a direct result of a lack of formal processes debating change.

**Signatures**

In order to securely move value from Alice to Bob, Alice needs to prove she has the right to move the funds. The most direct and reliable way of accomplishing this task is to use a public key signature scheme where funds are connected to a public key and Alice controls an associated private key.

There are hundreds of possible schemes with different security parameters and assumptions. Some rely upon mathematical problems connected to elliptic curves, whereas others are connected to exotic concepts using lattices The abstract goal is always the same. There exists a hard problem that cannot be solved unless  someone has a secret piece of knowledge. The holder of this piece of knowledge is said to be the owner of the keypair and should be the only entity that has the ability to use it. There are two groups of concerns a cryptocurrency faces with choosing a signature scheme. First, there is the long-term security durability of the scheme itself. Some cryptographic

schemes used in the 1970s and 1980s such as DES have been broken. The period over which the scheme should be expected to survive must be decided upon. Second, there are many enterprises, governments and other institutions that have preferred, or in some cases, mandated the use of a particular scheme. For example, the NSA maintains the Suite B protocol set. There are standards from ISO and even W3C workgroups on cryptography.  If a cryptocurrency chooses a single signature scheme, it is forced to accept that the scheme

could be broken at some point in the future and at least one entity cannot use the cryptocurrency due to legal or industry restrictions. Yet a cryptocurrency cannot support every signature scheme as this would require every client to understand and validate each scheme.

**The Engine**

Discussion of the Bitcon1platform begins with the core component which powers the platform: the consensus engine.

Background Distributed payments and – more generally – computation, require agreement between a set of machines. Therefore, consensus protocols, which enable a group of nodes to achieve agreement, lie at the heart of blockchains, as well as almost every deployed large-scale industrial distributed system. The topic has received extensive scrutiny for almost five decades, and that effort, to date, has yielded just two families of protocols: classical consensus protocols, which rely on all-to-all communication, and Nakamoto consensus,

which relies on proof-of-work mining coupled with the longest-chain-rule. While classical consensus protocols can have low latency and high throughput, they do not scale to large numbers of participants, nor are they robust in the presence of membership changes, which has relegated them mostly to permissioned, mostly static deployments. Nakamoto consensus protocols [5, 7, 4], on the other hand, are robust, but suffer from high confirmation latencies, low throughput, and require constant energy expenditure for their security.

Bitcon1 of protocols, introduced by Novuszilla, combine the best properties of classical consensus protocols with the best of Nakamoto consensus. Based on a lightweight network sampling mechanism, they achieve low latency and high throughput without needing to agree on the precise membership of the

system. They scale well from thousands to millions of participants with direct participation in the consensus protocol. Further, the protocols do not make use of PoW mining, and therefore avoid its exorbitant energy expenditure and subsequent leak of value in the ecosystem, yielding lightweight, green, and quiescent protocols. Mechanism and Properties Bitcon1 protocols operate by repeated sampling of the network. Each node polls a small, constant-sized, randomly chosen set of neighbors, and switches its proposal if a supermajority

supports a different value. Samples are repeated until convergence is reached, which happens rapidly in normal operations.

We elucidate the mechanism of operation via a concrete example. First, a transaction is created by a user and sent to a validating node, which is a node participating in the consensus procedure. It is then propagated out to other nodes in the network via gossiping. What happens if that user also issues a conflicting transaction, that is, a doublespend? To choose amongst the conflicting transactions and prevent the doublespend, every node randomly selects a small subset of nodes and queries which of the conflicting transactions

the queried nodes think is the valid one. If the querying node receives a supermajority response in favor of one transaction, then the node changes its own response to that transaction. Every node in the network repeats this procedure until the entire network comes to consensus on one of the conflicting transactions. Surprisingly, while the core mechanism of operation is quite simple, these protocols lead to highly desirable system dynamics that make them suitable for large-scale deployment.

– Permissionless, Open to Churn, and Robust. The latest slew of blockchain projects employ classical consensus protocols and therefore require full membership knowledge. Knowing the entire set of participants is sufficiently simple in closed, permissioned systems, but becomes increasingly hard in open,

decentralized networks. This limitation imposes high security risks to existing incumbents employing such protocols. In contrast, transaction, that is, a doublespend? To choose amongst the conflicting transactions and prevent the double spend, every node randomly selects a small subset of nodes and queries which of the conflicting transactions the queried nodes think is the valid one. If the querying node receives a supermajority response in favor of one transaction, then the node changes its own response to that transaction. Every node in the network repeats this procedure until the entire network comes to consensus on one of the conflicting transactions. Surprisingly, while the core mechanism of operation is quite simple, these protocols lead to highly desirable system dynamics that make them suitable for large-scale deployment.

– Scalable and Decentralized A core feature of the Bitcon1family is its ability to scale without incurring fundamental tradeoffs. Bitcon1 protocols can scale to tens of thousands or millions of nodes, without delegation to subsets of validators. These protocols enjoy the best-in-class system decentralization, allowing every node to fully validate. First-hand continuous participation has deep implications for the security of the system. In almost every proof-of-stake protocol that attempts to scale to a large participant set, the typical mode of operation is to enable scaling by delegating validation to a subcommittee. Naturally, this implies that the security of the system is now precisely as high as the corruption cost of the subcommittee. Subcommittees are furthermore subject to cartel formation.

In Bitcon1-type protocols, such delegation is not necessary, allowing every node operator to have a first-hand say in the system, at all times. Another design, typically referred to as state sharding, attempts to provide scalability by parallelizing transaction serialization to independent networks of validators.

Unfortunately, the security of the system in such a design becomes only as high as the easiest corruptible independent shard. Therefore, neither subcommittee election nor sharding are suitable scaling strategies for crypto platforms.

– Adaptive. Unlike other voting-based systems, Bitcon1 protocols achieve higher performance when the adversary is small, and yet highly resilient under large attacks.

– Asynchronously Safe. Bitcon1 protocols, unlike longest-chain protocols, do not require synchronicity to operate safely, and therefore prevent double-spends even in the face of network partitions. In Bitcoin, for example, if synchronicity assumption is violated, it is possible to operate to independent forks of the

Bitcoin network for prolonged periods of time, which would invalidate any transactions once the forks heal.

– Low Latency. Most blockchains today are unable to support business applications, such as trading or daily retail payments. It is simply unworkable to wait minutes, or even hours, for confirmation of transactions.

Therefore, one of the most important, and yet highly overlooked, properties of consensus protocols is the time to finality. Bitcon1 protocols reach finality typically in ≤ 1 second, which is significantly lower than both longest-chain protocols and sharded blockchains, both of which typically span finality to matter of minutes.

1. Architecture

Subnetworks A subnetwork, or subnet, is a dynamic set of validators working together to achieve consensus on the state of a set of blockchains. Each blockchain is validated by one subnet, and a subnet can validate arbitrarily many blockchains. A validator may be a member of arbitrarily many subnets. A subnet decides who may enter it, and may require that its constituent validators have certain properties. The Bitcon1 platform supports the creation and operation of arbitrarily many subnets. In order to create a new subnet

or to join a subnet, one must pay a fee denominated in $Bitcon1.

The subnet model offers a number of advantages:

– If a validator doesn’t care about the blockchains in a given subnet, it will simply not join that subnet. This reduces network traffic, as well as the computational resources required of validators. This is in contrast to other blockchain projects, in which every validator must validate every transaction, even those they don’t care about.

– Since subnets decide who may enter them, one can create private subnets. That is, each blockchain in the subnet is validated only by a set of trusted validators.

– One can create a subnet where each validator has certain properties. For example, one could create a 160 subnet where each validator is located in a certain jurisdiction, or where each validator is bound by some

real-world contract. This may be benificial for compliance reasons.

There is one special subnet called the Default Subnet. It is validated by all validators. (That is, in order to validate any subnet, one must also validate the Default Subnet.) The Default Subnet validates a set of pre-defined blockchains, including the blockchain where $Bitcon1 lives and is traded.

Virtual Machines Each blockchain is an instance of a Virtual Machine (VM.) A VM is a blueprint for a blockchain, much like a class is a blueprint for an object in an object-oriented programming language. The

interface, state and behavior of a blockchain is defined by the VM that the blockchain runs. The following properties of a blockchain, and other, are defined by a VM:

– The contents of a block

– The state transition that occurs when a block is accepted

– The APIs exposed by the blockchain and their endpoints

– The data that is persisted to disk We say that a blockchain “uses” or “runs” a given VM. When creating a blockchain, one specifies the VM

it runs, as well as the genesis state of the blockchain. A new blockchain can be created using a pre-existing VM, or a developer can code a new one. There can be arbitrarily many blockchains that run the same VM. Each blockchain, even those running the same VM, is logically independent from others and maintains its own state.

2 Bootstrapping

The first step in participating in Bitcon1 is bootstrapping. The process occurs in three stages: connection to seed anchors, network and state discovery, and becoming a validator. Seed Anchors Any networked system of peers that operates without a permissioned (i.e. hard-coded) set of identities requires some mechanism for peer discovery. In peer-to-peer file sharing networks, a set of

trackers are used. In crypto networks, a typical mechanism is the use of DNS seed nodes (which we refer to as seed anchors), which comprise a set of well-defined seed-IP addresses from which other members of the network can be discovered. The role of DNS seed nodes is to provide useful information about the set of active participants in the system. The same mechanism is employed in Bitcoin Core [1], wherein the src/chainparams.cpp file of the source code holds a list of hard-coded seed nodes. The difference between BTC and Bitcon1 is that BTC requires just one correct DNS seed node, while Avalanche requires a simple majority of the anchors to be correct. As an example, a new user may choose to bootstrap the network view through a set of well established and reputable exchanges, any one of which individually are not trusted.

We note, however, that the set of bootstrap nodes does not need to be hard-coded or static, and can be provided by the user, though for ease of use, clients may provide a default setting that includes economically important actors, such as exchanges, with which clients wish to share a world view. There is no barrier to become a seed anchor, therefore a set of seed anchors can not dictate whether a node may or may not enter the network, since nodes can discover the latest network of Avalanche peers by attaching to any set of seed

anchors. Network and State Discovery Once connected to the seed anchors, a node queries for the latest set of state transitions. We call this set of state transitions the accepted frontier. For a chain, the accepted frontier

is the last accepted block. For a DAG, the accepted frontier is the set of vertices that are accepted, yet have no accepted children. After collecting the accepted frontiers from the seed anchors, the state transitions that are accepted by a majority of the seed anchors is defined to be accepted. The correct state is then extracted by synchronizing with the sampled nodes. As long as there is a majority of correct nodes in the seed anchor set, then the accepted state transitions must have been marked as accepted by at least one correct node.

This state discovery process is also used for network discovery. The membership set of the network is defined on the validator chain. Therefore, synchronizing with the validator chain allows the node to discover the current set of validators. The validator chain will be discussed further in the next section.

3. Sybil Control and Membership

Consensus protocols provide their security guarantees under the assumption that up to a threshold number of members in the system could be adversarial. A Sybil attack, wherein a node cheaply floods the network with malicious identities, can trivially invalidate these guarantees. Fundamentally, such an attack can only be deterred by trading off presence with proof of a hard-to-forge resource [3]. Past systems have explored the use of Sybil deterrence mechanisms that span proof-of-work (PoW), proof-of-stake (PoS), proof-of-elapsed-time (POET), proof-of-space-and-time (PoST), and proof-of-authority (PoA). At their core, all of these mechanisms serve an identical function: they require that each participant have some “skin in the game” in the form of some economic commitment, which in turn provides an economic barrier against misbehavior by that participant. All of them involve a form of stake, whether it is in the form of mining rigs and hash power (PoW), disk space (PoST), trusted hardware (POET), or an approved identity (PoA). This stake forms the basis of an economic cost that participants must bear to acquire a voice. For

instance, in Bitcoin, the ability to contribute valid blocks is directly proportional to the hash-power of the proposing participant. Unfortunately, there has also been substantial confusion between consensus protocols versus Sybil control mechanisms. We note that the choice of consensus protocols is, for the most part, orthogonal to the choice of the Sybil control mechanism. This is not to say that Sybil control mechanisms are drop-in-replacements for each other, since a particular choice might have implications about the underlying

guarantees of the consensus protocol. However, the bitcon1 family can be coupled with many of these known mechanisms, without significant modification. Ultimately, for security and to ensure that the incentives of participants are aligned for the benefit of

the network, $Bitcon1 choose PoS to the core Sybil control mechanism. Some forms of stake are inherently centralized: mining rig manufacturing (PoW), for instance, is inherently centralized in the hands of a few people with the appropriate know-how and access to the dozens of patents required for competitive VLSI manufacturing. Furthermore, PoW mining leaks value due to the large yearly miner subsidies. Similarly, disk space is most abundantly owned by large datacenter operators.Further, all sybil control mechanisms

that accrue ongoing costs, e.g. electricity costs for hashing, leak value out of the ecosystem, not to mention destroy the environment. This, in turn, reduces the feasibility envelope for the token, wherein an adverse price move over a small time frame can render the system inoperable. Proof-of-work inherently selects for miners who have the connections to procure cheap electricity, which has little to do with the miners’ ability to serialize transactions or their contributions to the overall ecosystem. Among these options, we choose proof-of-stake, because it is green, accessible, and open to all. We note, however, that while the $AVAX uses PoS, the Avalanche network enables subnets to be launched with PoW and PoS. Staking is a natural mechanism for participation in an open network because it enables a direct economic argument: the probability of success of an attack is directly proportional to a well-defined monetary cost

function. In other words, the nodes that stake are economically motivated to not engage in behavior that might hurt the value of their stake. Additionally, this stake does not incur any additional upkeep costs (other then the opportunity cost of investing in another asset), and has the property that, unlike mining equipment, is fully consumed if used in a catastrophic attack. For PoW operations, mining equipment can be simply reused or – if the owner decides to – entirely sold back to the market. A node wishing to enter the network can freely do so by first putting up a stake that is immobilized during the duration of participation in the network. The user determines the amount duration of the stake. Once accepted, a stake cannot be reverted. The main goal is to ensure that nodes substantially share the same mostly stable view of the network. We anticipate setting the minimum staking time on the order of a

250 week.

Unlike other systems that also propose a PoS mechanism, $Bitcon1 does not make usage of slashing, and therefore all stake is returned when the staking period expires. This prevents unwanted scenarios such as a client software or hardware failure leading to a loss of coins. This dovetails with our design philosophy of building predictable technology: the staked tokens are not at risk, even in the presence of software or hardware flaws.

In Bitcon1, a node that wants to participate issues a special stake transaction to the validator chain. Staking transactions name an amount to stake, the staking key of the participant that is staking, the duration, and the time that validation will start. Once the transaction is accepted, the funds will be locked until the

end of the staking period. The minimal allowed amount is decided and enforced by the system. The stake amount placed by a participant has implications for both the amount of influence the participant has in the consensus process, as well as the reward, as discussed later. The specified staking duration, must be between δmin and δmax, the minimum and maximum timeframes for which any stake can be locked. As with the staking amount, the staking period also has implications for the reward in the system. Loss or theft of the

staking key cannot lead to asset loss, as the staking key is used only in the consensus process, not for asset transfer.

4. Smart Contracts in $Bitcon1

At launch Bitcon1 supports standard Solidity-based smart contracts through the Ethereum virtual machine (EVM). We envision that the platform will support a richer and more powerful set of smart contract tools, including:

– Smart contracts with off-chain execution and on-chain verification.

– Smart contracts with parallel execution. Any smart contracts that do not operate on the same state in any subnet in Bitcon1 will be able to execute in parallel.

– An improved Solidity, called Solidity++. This new language will support versioning, safe mathematics and fixed point arithmetic, an improved type system, compilation to LLVM, and just-in-time execution.

If a developer requires EVM support but wants to deploy smart contracts in a private subnet, they can spin-up a new subnet directly. This is how Bitcon1 enables functionality-specific sharding through the subnets. Furthermore, if a developer requires interactions with the currently deployed Ethereum smart

contracts, they can interact with the Athereum subnet, which is a spoon of Ethereum. Finally, if a developer requires a different execution environment from the Ethereum virtual machine, they may choose to deploy their smart contract through a subnet that implements a different execution environment, such as DAML or WASM. Subnets can support additional features beyond VM behavior. For example, subnets can enforce performance requirements for bigger validator nodes that hold smart contracts for longer periods of time, or

validators that hold contract state privately.

4 Governance and The $Bitcon1 Token

285 4.1 The $Bitcon1 Native Token

Monetary Policy The native token, $Bitcon1, is capped-supply, where the cap is set at 250, 000, 000 tokens, with 120, 000, 000 tokens available on mainnet launch. However, unlike other capped-supply tokens which

bake the rate of minting perpetually, $Bitcon1 is designed to react to changing economic conditions. In particular, the objective of $Bitcon1’s monetary policy is to balance the incentives of users to stake the token versus using it to interact with the variety of services available on the platform. Participants in the platform collectively act as a decentralized reserve bank. The levers available on Bitcon1 are staking rewards, fees, and airdrops, all of which are influenced by governable parameters. Staking rewards are set by on-chain governance, and are ruled by a function designed to never surpass the capped supply. Staking can be induced by increasing fees or increasing staking rewards. On the other hand, we can induce increased engagement with the Novuszilla platform services by lowering fees, and decreasing the staking reward.

Uses

Payments True decentralized peer-to-peer payments are largely an unrealized dream for the industry due to the current lack of performance from incumbents. $Bitcon1 is as powerful and easy to use as payments using Visa, allowing thousands of transactions globally every second, in a fully trustless, decentralized manner. Furthermore, for merchants worldwide, $Bitcon1 provides a direct value proposition over Visa, namely lower

fees.

Staking: Securing the System On the Bitcon1 platform, sybil control is achieved via staking. In order to validate, a participant must lock up coins, or stake. Validators, sometimes referred to as stakers, are compensated for their validation services based on staking amount and staking duration, amongst other properties. The chosen compensation function should minimize variance, ensuring that large stakers do not disproportionately receive more compensation. Participants are also not subject to any “luck” factors, as in

PoW mining. Such a reward scheme also discourages the formation of mining or staking pools enabling truly decentralized, trustless participation in the network. Atomic swaps Besides providing the core security of the system, the $Bitcon1 token serves as the universal unit of exchange. From there, the novuszilla platform will be able to support trustless atomic swaps natively on

the platform enabling native, truly decentralized exchanges of any type of asset directly on Avalanche.

Governance

Governance is critical to the development and adoption of any platform because – as with all other type of systems – Bitcon1 will also face natural evolution and updates. $Bitcon1 provides on-chain governance for critical parameters of the network where participants are able to vote on changes to the network and

settle network upgrade decisions democratically. This includes factors such as the minimum staking amount, minting rate, as well as other economic parameters. This enables the platform to effectively perform dynamic parameter optimization through a crowd oracle. However, unlike some other governance platforms out there, Bitcon1 does not allow unlimited changes to arbitrary aspects of the system. Instead, only a pre-determined number of parameters can be modified via governance, rendering the system more predictable and increasing safety. Further, all governable parameters are subject to limits within specific time bounds, introducing hysteresis, and ensuring that the system remains predictable over short time ranges. A workable process for finding globally acceptable values for system parameters is critical for decentralized systems without custodians. Avalanche can use its consensus mechanism to build a system that allows anyone to propose special transactions that are, in essence, system-wide polls. Any participating node may

issue such proposals. Nominal reward rate is an important parameter that affects any currency, whether digital or fiat. Unfortunately, cryptocurrencies that fix this parameter might face various issues, including deflation or inflation. To that end, the nominal reward rate is subject to governance, within pre-established boundaries. This will allow token holders to choose on whether $Bitcon1 is eventually capped, uncapped, or even deflationary.

Discussion

1 Optimizations

Pruning Many blockchain platforms, especially those implementing Nakamoto consensus such as Bitcoin, suffer from perpetual state growth. This is because – by protocol – they have to store the entire history oftransactions. However, in order for a blockchain to grow sustainably, it must be able to prune old history.

This is especially important for blockchains that support high performance, such as Bitcon1. Pruning is simple in the Bitcon1 family. Unlike in Bitcoin (and similar protocols), where pruning is not possible per the algorithmic requirements, in $Bitcon1 nodes do not need to maintain parts of the DAG that

are deep and highly committed. These nodes do not need to prove any past history to new bootstrapping nodes, and therefore simply have to store active state, i.e. the current balances, as well as uncommitted transactions.

Client Types Avalanche can support three different types of clients: archival, full, and light. Archival nodes store the entire history of the $Bitcon1 subnet, the staking subnet, and the smart contract subnet, all the way to genesis, meaning that these nodes serve as bootstrapping nodes for new incoming nodes. Additionally these nodes may store the full history of other subnets for which they choose to be validators. Archival nodes are typically machines with high storage capabilities that are paid by other nodes when downloadingold state. Full nodes, on the other hand, participate in validation, but instead of storing all history, they simply store the active state (e.g. current UTXO set). Finally, for those that simply need to interact securely with the network using the most minimal amount of resources, Bitcon1 supports light clients which can

prove that some transaction has been committed without needing to download or synchronize history. Light clients engage in the repeated sampling phase of the protocol to ensure safe commitment and network wide consensus. Therefore, light clients in Avalanche provide the same security guarantees as full nodes.

Sharding is the process of partitioning various system resources in order to increase performance and reduce load. There are various types of sharding mechanisms. In network sharding, the set of participants is divided into separate subnetworks as to reduce algorithmic load; in state sharding, participants agree on storing and maintaining only specific subparts of the entire global state; lastly, in transaction sharding, participants agree to separate the processing of incoming transactions.

In Novuszilla aurora, the first form of sharding exists through the subnetworks functionality. For example, one may launch a gold subnet and another real-estate subnet. These two subnets can exist entirely in parallel. The subnets interact only when a user wishes to buy real-estate contracts using their gold holdings, at which point Bitcon1 will enable an atomic swap between the two subnets.

2 Concerns

Post Quantum Cryptography Post-quantum cryptography has recently gained widespread attention due to the advances in the development of quantum computers and algorithms. The concern with quantum computers is that they can break some of the currently deployed cryptographic protocols, specifically digital signatures. The Avalanche network model enables any number of VMs, so it supports a quantum-resistant virtual machine with a suitable digital signature mechanism. We anticipate several types of digital signature schemes to be deployed, including quantum resistant RLWE-based signatures. The consensus mechanism does not assume any kind of heavy crypto for its core operation. Given this design, it is straightforward to extend the system with a new virtual machine that provides quantum secure cryptographic primitives.

Realistic Adversaries The Avalanche paper [6] provides very strong guarantees in the presence of a powerful and hostile adversary, known as a round-adaptive adversary in the full point-to-point model. In other terms, the adversary has full access to the state of every single correct node at all times, knows the random choices of all correct nodes, as well as can update its own state at any time, before and after the correct node has the chance to update its own state. Effectively, this adversary is all powerful, except for the ability to directly update the state of a correct node or modify the communication between correct

nodes. Nonetheless, in reality, such an adversary is purely theoretical since practical implementations of the strongest possible adversary are limited at statistical approximations of the network state. Therefore, in

practice, we expect worst-case-scenario attacks to be difficult to deploy

Inclusion and Equality A common problem in permissionless currencies is that of the “rich getting richer”. This is a valid concern, since a PoS system that is improperly implemented may in fact allow wealth generation to be disproportionately attributed to the already large holders of stake in the system. A simple example is that of leader-based consensus protocols, wherein a subcommittee or a designated leader collects all the rewards during its operation, and where the probability of being chosen to collect rewards is

395 proportional to the stake, accruing strong reward compounding effects. Further, in systems such as Bitcoin, there is a “big get bigger” phenomenon where the big miners enjoy a premium over smaller ones in terms

of fewer orphans and less lost work. In contrast, Bitcon1 employs an egalitarian distribution of minting: every single participant in the staking protocol is rewarded equitably and proportionally based on stake. By enabling very large numbers of people to participate first-hand in staking, Bitcon1 can accommodate millions of people to participate equally in staking. The minimum amount required to participate in the protocol will be up for governance, but it will be initialized to a low value to encourage wide participation.

This also implies that delegation is not required to participate with a small allocation.

Conclusion

In this paper, we discussed the architecture of the Avalanche platform. Compared to other platforms today, which either run classical-style consensus protocols and therefore are inherently non-scalable, or make usage of Nakamoto-style consensus that is inefficient and imposes high operating costs, the Bitcon1 is lightweight, fast, scalable, secure, and efficient. The native token, which serves for securing the network and paying for various infrastructural costs is simple and backwards compatible. $Bitcon1 has capacity beyond other proposals to achieve higher levels of decentralization, resist attacks, and scale to millions of nodes without any quorum or committee election, and hence without imposing any limits to participation. Besides the consensus engine, Bitcon1 innovates up the stack, and introduces simple but important ideas in transaction management, governance, and a slew of other components not available in other platforms. Each participant in the protocol will have a voice in influencing how the protocol evolves at all times, made possible by a powerful governance mechanism. Avalanche supports high customizability, allowing nearly instant plug-and-play with existing blockchains.

Related Work

One of the first stablecoin taxonomies classified stablecoin projects by collateral type and discussed pros and cons of each category [56]. Several papers and reports have followed a similar taxonomy, adding more detail on individual projects [57] [58] [48]. A paper by Pernice et. al takes a different approach,

categorizing stablecoins by monetary and exchange rate regimes [54]. Our contribution is extending the existing taxonomies with a discussion of other important stablecoin design aspects, namely price stabilizing mechanisms and price measurement methods. We also categorize many of the existing stablecoin projects according to our extended taxonomy.

Peg and Collateral

1 Peg

The most salient choice for stablecoin design is the peg, which oftentimes is

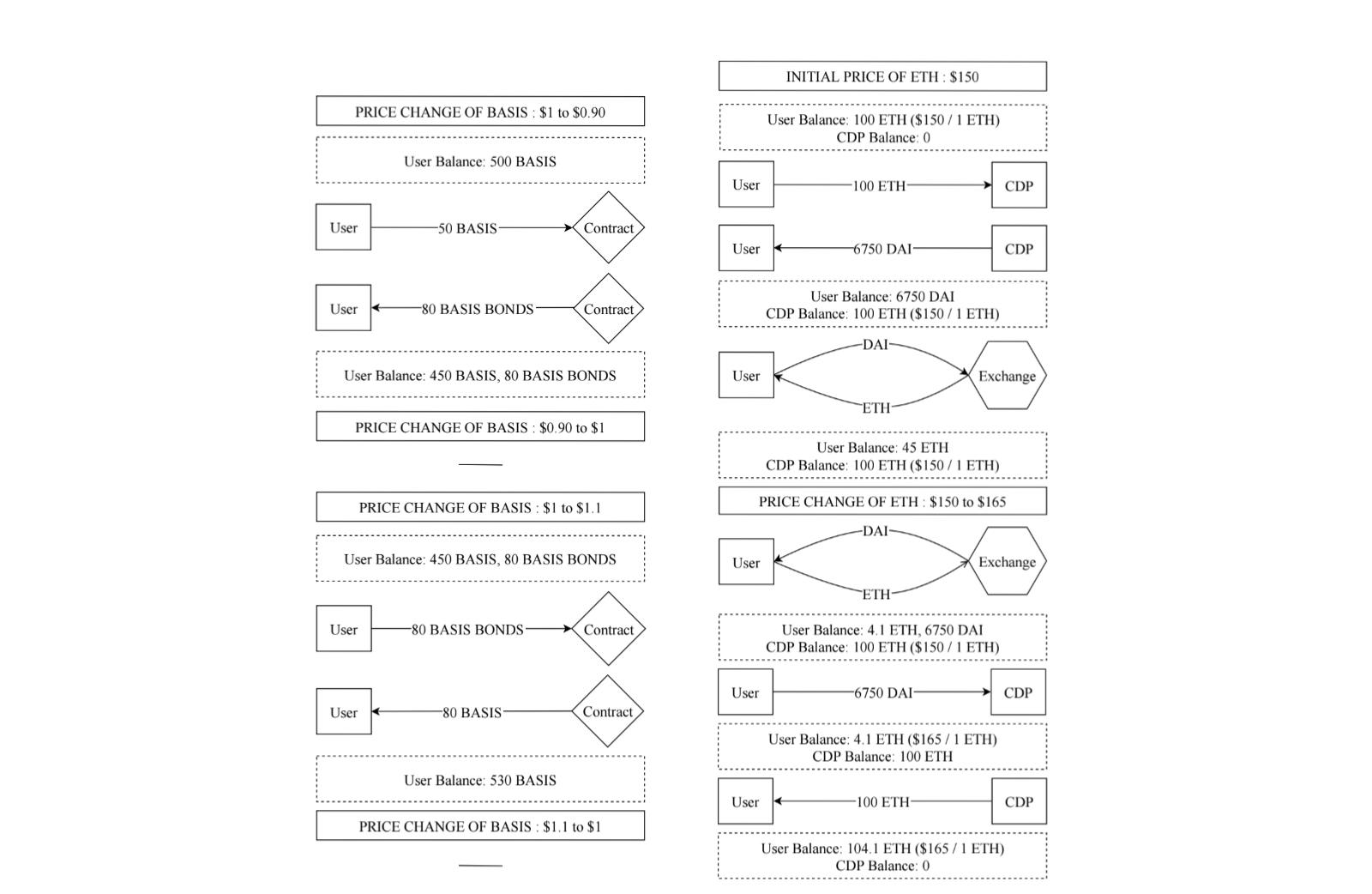
included in the name of the stablecoin.1 USD is a popular choice, likely due

to USD being typically considered a stable store of value around the world. In

fact, it is not uncommon for foreign citizens, especially those in emerging and

developing economies, to store their wealth in USD rather than their national

currency. The other benefit of using USD is that price comparison is easy. A



singular fiat currency peg allows one to check whether the peg holds by simply

comparing the dollar price of an object to the pegged coin price of the same

object. Other stable fiat currencies, such as the Euro, the Japanese Yen, and the

Swiss Franc, are also popular choices for similar reasons. Besides fiat, there are also stablecoins pegged to commodities, most commonly gold. Some examples include Digix [27] and HelloGold [31]. It is interesting to note that, in general, there are fewer commodity-pegged coins than fiat-pegged coins. A possible explanation is that commodity prices fluctuate in value more than fiat currencies, although typically less severely than most digital

currencies. Other stablecoins may choose to peg to a bundle of currencies and/or commodities. This has the benefit of insulating the stablecoin against shocks to any one country, currency, or commodity. However, pegging to a



Bundle can also have the opposite effect and introduce noise if some of the assets included in the bundle are very volatile. Saga [60], for example, is pegged to the IMF’s special drawing rights (SDR), a basket of world currencies curated by the IMF. Currencies are selected into the SDR if the issuing country is one of the world’s top exporters, the currency is widely used in international transactions, and the currency is widely traded in foreign exchange markets. However, the SDR is seldom used in any context other than the IMF’s store of value and unit of account, making it a less practical choice than the dollar. Facebook’s upcoming Libra also plans to peg its currency to an as of yet undetermined basket of currencies and assets. Saga plans to later peg their currency to the consumer price index (CPI) if they outgrow the SDR, i.e. if they become a dominant world currency. The CPI is a unitless index which tracks the inflation of the price of a basket of consumer goods. No stablecoin is currently pegged to the CPI, so it is unclear how this would be executed. It is possible, for example, that the stablecoin supply would be adjusted so the nominal price level remains constant. Pegging to a fiat currency or commodity with finite supply can eventually lead to problems

of scale, and pegging to an index can circumvent this problem. However, the

choice of CPI as a peg is not ideal for a variety of reasons. It is typically measured

monthly or even less frequently, due to logistical challenges in determining what

should be in the basket and how much each component should be weighted. There

are also regional differences in consumption, so it is unclear how to construct a

basket that reflects global spending patterns.

Collateral

Emergent currencies often make use of collateral to ensure that the circulating

currency has redemption value. This provides a lower bound on the price, thereby

mitigating some of the risk of holding, using, and denominating debts in the

currency. Since the goal of collateralizing is to bound the redemption value, it is

easiest and most effective, but not necessary, to use whatever the stablecoin is

pegged to. If users can always redeem one unit of the stablecoin for one dollar,

arbitrageurs should ensure that it never trades at any other price.

Unfortunately, collateralizing a coin creates the problem of securely storing

large quantities of the collateral.Traditionally, the best place to store large quantities of cash is in a bank, because it is secure, relatively easy to audit, and often comes with deposit insurance. However, this is also centralized, thus making it prone to deceptive practices. For example, Tether [66] recently admitted it was only 74% collateralized [65], despite initially claiming full collateralization [66]. Moreover, there are often limits to how much deposit insurance covers, potentially leaving the majority of the reserve uninsured. Some stablecoins avoid this problem by storing their collateral as physical cash in a vault instead of a bank.

For example, Rockz [59] stores 90% of its collateral in the form of physical fiat

currency in an underground vault in the Swiss Alps.

Commodity backed stablecoins also suffer from the problem of where to store

their collateral, since there are fewer institutions which accept and insure deposits in the form of commodities than ones that accept cash. This, in turn,

leads to a high degree of centralization. One way to avoid having to store large amounts of fiat is to collateralize with another cryptocurrency. This has the advantage of potentially decentralized operation, and allows for easier diversification across backing assets. The problem with this approach is that digital collateral can itself be very volatile, making it hard to use as a guarantee of value. Any stablecoin backed by cryptocurrencies must have some mechanism built in to safely handle large swings in the value of the underlying collateral. We discuss these mechanisms in section 4. Other stablecoins do away with the problem of volatile collateral by simply not collateralizing the currency at all. This has many advantages. First, not having any collateral to store or unlock simplifies many logistical challenges. Second, it is also cheap to operate, since it does not require the issuer to keep real or crypto assets on hand. Unfortunately, this ease of operation comes with drawbacks. Algorithms are usually gameable.

The value of the currency in this case stems purely from the reliability of the issuing mechanism and/or people’s beliefs. Once users’ expectations of the coin’s stability change, whether due to a law in design or idiosyncratic changes in sentiment, there may be little to keep the price afloat because there is no inherent redemption value.

Consequently, when these stablecoins fail, they tend to do so swiftly and catastrophically. One example is NuBits [45], which dropped from its pegged price of $1 to less than $0.30 over the course of 2 weeks in early 2018. It never recovered its peg, and has been trading below $0.10 for the past six months.4

Collateral amount

Hand in hand with the decision of collateral type comes the decision of collateral amount. Since collateral serves to support the price by creating a reliable

redemption value, the best choice seems to be a fully collateralized stablecoin.

If every unit of currency can be redeemed for the underlying asset, there is virtually no rational reason they should ever trade at different prices, thus making

price fluctuations minimal. However, one to one collateralization is sometimes

excessive, and sometimes insufficient. Having a full reserve, where the value of the collateral is exactly the value of the circulating currency, makes it hard for a currency to scale. As the stablecoin becomes more widely used, the issuers have to keep buying more collateral in

order to keep up with demand. Nevertheless, this stablecoin design has been

successfully utilized by Hong Kong’s currency board; the Hong Kong Dollar is

fully collateralized by USD and has maintained a roughly 7.8 to 1 peg to the US

dollar since the early 1980s. It is currently the 13th most traded currency in the

world.

Instead of staying fully collateralized, some currencies, like Saga, try to mimic

the historical trajectory taken by the US Dollar. Such currencies initially fully

collateralize their stablecoin, then slowly reduce their collateral ratio and ease off

the peg once the money supply has exceeded some threshold. Although Tether

eventually admitted they were not fully collateralized as they initially claimed,

there was no ostensible detriment to the price. A reason for the continued stability despite only partial collateralization is that full collateral is not necessary

as long as people do not believe that more than the entire reserve amount will

ever be cashed out at once. It is also worth noting that almost any supposedly

fully collateralized fiat backed stablecoin whose collateral is being held in a bank,

such as USDC, is functionally a partial reserve currency. All commercial banks

keep only some of their deposits on hand and use the rest for investments or to

issue loans. This does not cause any problems as long as they keep enough on

hand to satisfy demand for withdrawals. Other coins, especially algorithmic ones such as Basis, do not keep any collateral at all. Instead, value is preserved purely by expanding supply when the price is too high and contracting it when the price is too low. On the other end of the spectrum, many currencies collateralized by crypto-currencies keep more than the value of the circulating currency in reserve to guard against price swings in the collateral. This way, even if the collateral asset depreciates, there is still enough for each unit of the stablecoin to be redeemed for an equivalent amount of the underlying asset.

4 Mechanics

All stablecoins require some mechanism to adjust the price when it deviates

from the peg. Usually, this is done by expanding supply when the price is too

high and contracting it when the price is too low. This means that there usually

needs to be some way of measuring the price (covered further in the next section)

and knowing how much to expand or contract the supply. Most stablecoins are

designed such that rational, self interested users will act to restore the peg when

the price deviates. For example, this could be achieved by allowing users to

redeem stablecoins for collateral when the price of the stablecoin is too low.

Other stablecoins issue a secondary token designed to absorb the volatility of

the first, resulting in a stablecoin/volatilecoin pair. Still others depend on an

algorithmic market making mechanism or central-bank contract to manage the

supply Reserve of Pegged Asset Many stablecoins will build a mechanism where

users will be incentivized to expand or contract the supply until the price returns to the peg. The simplest way to achieve this is in a fully collateralized

system backed by the pegged asset, and allow users to expand supply when

the price is too high and redeem when the price is too low. Arbitrageurs earn

money while helping maintain the peg. For example, if a stablecoin pegged to

USD is trading at less than $1, stablecoin holders should redeem the coin for

the underlying collateral, thereby buying a dollar for less than a dollar. This

will contract the supply until the price returns to the peg and the arbitrage

opportunity disappears, or until the reserve runs out.

On the other hand, if the market price of the stablecoin is above $1, many systems will allow users to expand the supply by wiring funds to the account where

the rest of the collateral is being held. This allows the user to buy something

worth more than $1 by paying only $1 for it. The simplicity and autonomy of

this system makes it extremely appealing, which is why a majority of stablecoins

in circulation today use this method, or a very similar one. However, it is not

foolproof. On October 15, 2018, the price of Tether briefly dropped below $0.93

due to a large selloff. The price recovered to above $0.98 within the day and

appears to have suffered no lasting effects [22]. Other notable examples of this

design include USDC, TrueUSD, Carbon [18], Paxos [19], Gemini Dollars [23],

and many others. As stated previously, the main problem with allowing users to always redeem for collateral is storing large amounts of collateral at some physical location.

Since it is expensive to provide the security needed to protect large sums of

money, most stablecoins rely on one central location, like a bank. This introduces

two issues: centralization and dependency on legacy financial institutions. USDC

gets around one of these problems by storing collateral at a network of banks

rather than a single one. However, it still relies heavily on existing banks. The

other problem with this type of system is the ability to scale. As previously

discussed, this makes it difficult, though not impossible, to become a global

currency due to the inconvenience of storing assets of such high value in a large

number of locations. This inconvenience, is one of the reasons USD outgrew the

gold standard.

A common variation on this design requires a central authority to mint the

coins, but allows people to redeem the stablecoin for the underlying collateral.

This creates a lower bound on the price of the stablecoin but not an upper

bound, since users can redeem when the stablecoin price is too low but cannot

mint when the price is too high. This is common in cases where the collateral is

not necessarily dollars, such as Digix. Since it would be inconvenient to accept

and verify gold deposits from individual users, users are not allowed to mint

Digix by contributing capital to the collateral pool. They can, however, still

redeem their Digix for physical gold, thereby creating a lower bound on the

value of Digix. In addition to allowing people to mint coins, Tether was released in waves, allegedly at strategic times to prop up the price of Bitcoin [34]. Users can redeem Tether for USD, but since Tether is no longer fully collateralized, they also reserve the right to deny people the right to redeem.

Another variation being employed by Facebook’s Libra [46] is to allow only

the set of validators to mint or redeem coins, instead of all users. This reduces

overhead since presumably larger amounts would be transacted each time, and

at a lower frequency. This may come at the cost of a lower speed of adjustment,

since the set of potential arbitrageurs who can correct the price is restricted.

Dual coin Another way to maintain stability is to pair the pegged coin with

a secondary coin which absorbs the volatility of the first. The most well known

example of this is the seigniorage shares model employed by the original formulation of Carbon. When the price of the stablecoin dips below the peg, a secondary coin is auctioned in exchange for the stablecoin. The proceeds from the auctionare then burned to contract the supply. When the price of the stablecoin is above the peg, additional coins are minted to holders of the secondary token. Holders of the secondary token help prop up the price when the currency inflates and are rewarded during deflationary periods. There are two big concerns with this type of system. One is that the secondary coin often meets the SEC’s definition of a security. Regulatory complications stemming from this designation were enough to keep Basis from launching [1]. Carbon also changed from a dual coin system to a fiat backed system, for undisclosed reasons, possibly due to regulatory hurdles. The second concern is that if holders of the primary token do not believe that the stablecoin will appreciate in the future, there is no incentive to buy or hold the secondary token.

In other words, one needs a strong contingent of users who, even during a downturn, believe that the stablecoin will eventually appreciate in value. Additionally, since cryptocurrency markets are often subject to long downturns, people may be reluctant to wait for extended, indeterminate amounts of time for their investment to pay off. Since there is no collateral backing this system, if people are not willing to buy the secondary coin, there will be no force propping up the value of the stablecoin.

Variations on this design include USDX and Celo [39], which use concepts

from dual coin systems and redemption based systems to peg their tokens. USDX

is a stablecoin collateralized with Lighthouse (LHT), a digital currency. USDX is pegged to USD but backed over 200% by LHT, which is stored in two centralized funds.

People are free to exchange LHT to USDX and vice versa at a valuation

of $1/USDX. As such, when USDX is trading at a price of less than $1, people

are incentivized to redeem it for $1 worth of LHT, contracting the supply and

raising the price. LHT ends up absorbing the volatility of USDX because the

supply of USDX is contracted by expanding the circulating supply of LHT. The

main issue in this design stems from USDX being 200% collateralized by LHT.

The largest possible market cap for USDX is half the market cap of LHT, and

if the market value of LHT declines, so does the potential market cap of USDX.

It is unclear what LHT derives its value from, so the potential market cap of

USDX might be small and/or unstable.

Celo works similarly to USDX, but with a few additions. Celo is backed by

CeloGold,5 Bitcoin, and Ethereum. In addition to allowing people to redeem

Celo for CeloGold and vice versa, there is an algorithmic central bank which

buys and sells Celo and CeloGold to stabilize the price.

StatiCoin/RiskCoin [62] is another variation of the dual coin system which

allows creation and redemption of coins to maintain a peg. Users who want

to mint StatiCoin send ETH to the contract and receive a dollar equivalent

amount of StatiCoin in return. When they want to redeem, they send StatiCoin

to the contract and receive an equivalent dollar amount of ETH. Users who want

to mint RiskCoin also send ETH to the contract and receive a corresponding

amount of RiskCoin in return, depending on what the current RiskCoin price

is. StatiCoin can always be redeemed for $1 worth of ETH, provided there is

enough collateral, while RiskCoin holders are the residual claimant to the ETH

held by the contract. If there is $100 worth of ETH held by the contract, 90

StatiCoins in circulation, and 2 RiskCoins in circulation, the value of all of the

outstanding Riskcoin is $10 and each RiskCoin is worth $5. If the next day the

value of the ETH held in the contract drops to $90, RiskCoin will be worth

$0 and users will not be allowed to mint additional RiskCoin until the dollar

value of collateral exceeds the number of StatiCoin issued. StatiCoin is unique

because it is crypto-collateralized but does not require overcollateralization, an

inefficient mechanism for absorbing volatility. If the value of the collateral falls

below the market cap of StatiCoin, StatiCoin may become unpegged because

not all holders of StatiCoin will be able to redeem for the underlying collateral.

If the price of ETH drops enough to reduce the price of RiskCoin to 0, then

StatiCoin will become an unreliable store of value precisely when Ethereum is

losing value and a stable valued asset is most needed.

Terra [40] is yet another dual coin stablecoin, with its volatility absorbed by

the secondary token Luna. Luna serves two purposes in this system. It absorbs

volatility because it is auctioned to contract the supply when the stablecoin

price is too low and purchased with Terra when the stablecoin price is too high.

It is also the staking token of the system. Fees and mining rewards, paid in

Terra, are increased when Terra decreases in value to incentivize holding Luna

and smooth the pro-cyclicality of the value of Luna. Unlike previously discussed

designs, such as Staticoin/Riskcoin, the secondary token Luna can retain value

and creates payoffs from fees and mining rewards even in an extended contraction. However, it does this by raising fees when the value of Terra is decreasing,which discourages Terra use when the value of Terra is already low. Terra also increases the staking pool in times when the market cap of Terra is small and there is less need for stakers, and decreases it when the market cap is large and more security is needed.

Yet another variation on the dual coin system is the triple coin system proposed by Basis. Instead of having a singular volatility absorbing coin, Basis has

bond tokens and share tokens. Bond tokens are auctioned off when the price of

Basis decreases below $1, and each one is redeemable for 1 Basis when the price

of Basis is above $1. If all of the Bond tokens have been redeemed and the price

of Basis is still above $1, additional Basis is minted pro rata to holders of share

tokens until the price of Basis returns to $1. Holders of Basis bonds absorb the

downside and are the first to benefit from increases in the market cap of Basis,

while holders of Basis shares benefit only when there are large expansions in the

value of Basis. There are infinite ways to tranche the volatility absorbing coin;

in theory there could be systems with four or more coins splitting the stablecoin

volatility across several parties.

Algorithmic Other currencies use a fully algorithmic approach to adjust the

supply of the stablecoin in response to price fluctuations. One such example

is Ampleforth, previously named Fragments [42]. Whenever the value of Ampleforth changes, token holders have their balances adjusted proportionally to preserve the value of a single token. For example, if Ampleforth is originally

worth $1, then, after an increase of 10% to $1.10, all balances will automatically

be inflated by 10%. Likewise, if the value of Ampleforth declines, each Ampleforth holder’s balance will be decreased accordingly. This makes Ampleforth a stable unit of account, since by design, the ratio of Ampleforth’s market cap to the number of Ampleforth tokens is periodically adjusted to be $1. Unfortunately, this is not a good store of value. Holding Ampleforth is no different than holding a non-pegged coin: if the market cap of Ampleforth declines, users’ balances and outstanding payments will decline proportionally.

A different algorithmic approach is employed by Saga. Although Saga does

not peg the value of its coin, it uses an algorithmic path-independent market

maker inspired by Bancor [35] to provide liquidity and to dampen sudden price

fluctuations. The market maker sets the price and bid ask spread for Saga based

on how much collateral it has in its reserve. For example, when Saga is just

starting out and its reserve is small, the price will be set at 1 SDR, and the

market maker will sell a Saga for 1.0015 SDR and buy for 0.9985 SDR. This

makes it so that users should not sell Saga on secondary markets for less than

0.9985 or buy for more than 1.0015 SDR, which limits how suddenly the price

can change. As the reserve grows and shrinks, the price and spread are gradually

adjusted in response. Like Ampleforth, Saga does not guarantee that the value

of Saga holdings will be stable over time. However, the market maker does guard

against sudden price movements, and thus provides short-term stability.

Leveraged loans Leveraged loans are a system of stablecoins which utilize

components from all the above classes. Dai [47] is the most successful example of such a system. Users lock up collateral, such as Ethereum and other cryptoassets, in collateralized debt positions (CDPs). They can then mint Dai, a stablecoinpegged to $1, up to 2/3 the value of the collateral in the CDP. Users can then unlock their collateral by paying back the borrowed Dai, plus a stability fee that accrues over time. Dai is destroyed once it is paid back.

If the value of the collateral in a CDP drops below 1.5x the Dai borrowed, the

debt position is automatically liquidated, and the collateral is used to purchase

the amount of Dai borrowed against it. Any remaining collateral, minus a liquidation fee, is returned to the original CDP owner. If the value of the collateral depreciates quickly and drops below the value of the Dai borrowed, a secondary

coin is minted to cover the difference. Currently, the secondary coin is PETH,

but eventually it will be transitioned to MKR. Since MKR is the governance

token, and MKR holders are diluted when CDPs are underwater, there is an

incentive for the holders of the governance token to set parameters such that

users are not defaulting on their loans. However, we note that the probability of

the value of the collateral declining to less than the Dai borrowed is low since

the price of the collateral would have to suddenly drop by over 33%.

Users are incentivized to buy Dai and unlock their collateral when the price

of Dai decreases, because a decrease in the price of Dai makes it cheaper for

them to unlock their collateral. This contracts the supply and restores the peg.

If Dai continues to trade at a price lower than its intended peg, MKR holders

can vote to raise the stability fee charged to CDP holders. This serves as further

incentive for CDP holders to liquidate their positions and contract supply.

Dai received a lot of attention in March 2019 for consistently trading around

$0.98 instead of $1 as it was supposed to. Since then, it underwent a series

of stability fee increases, some of which quixotically lowered the price of Dai

instead of raising it as intended. Despite this issue and Ethereum’s price decrease

by ∼ 90% since Dai launched, Dai has managed to remain within ∼ 2% of its

pegged value.

Price information

A crucial step in making supply adjustments at the appropriate times is accurately measuring the price. Most stablecoins make use of an external oracle, an

independent price feed(s) deemed trustworthy by the issuers of the stablecoin.

This leaves a crucial component of the system completely out of the hands of

the stablecoin issuer. The entities publishing the price feed might deviate from

their standard practice in how they calculate prices and trigger disastrous downturns or upturns for the stablecoin. This is not unheard of, since, for example, CoinMarketCap suddenly and abruptly decided to stop including prices from exchanges in South Korea, resulting in a sudden drop in reported prices.

If a stablecoin was formerly using this price feed and desired no change in how

prices are calculated, the system would be left with few options other than to

accept the new price feed, find a different oracle, or adjust oracle prices to correct for the new calculation method. Short term pricing errors can arise from

using an oracle too, as was the case with Synthetix. In June 2019, a commercial

API used by Synthetix suffered a glitch and began to report incorrect exchange

rates, resulting in a bot making over $1B during this period [9]. Although the

bot owner chose to reverse the trades during this episode, there is no guarantee

that the next profiteer will be as generous. Note that these are examples which

arose even with no malicious adversaries in the system.

On the other hand, if there is a malicious actor intent on sabotaging the

stability, a price oracle can serve as a potential target. Increasing the number

of price feeds might be a potential solution to this issue. However using the

median makes price updating slow, since the system must wait for sufficient

majority of price feed reports. As a result, even some of the most active and

popular stablecoins, including MakerDao, use only a few price oracles, making

them a potential source of attack vectors [49]. There are only 14 price oracles for

MakerDao, so hijacking of any 8 would corrupt the median-price rule. Moreover,

these oracles may not be fully independent, as they might have overlap in where

they obtain their price information or in their deployment platform.

Nonetheless, the use of external oracles persists because the alternatives are

generally worse. Prices for most assets are generated based on the prices at

which the assets are transacted on exchanges. However, many crypto exchanges,

both centralized and decentralized, have stale prices and/or inflation of trade

volumes [7]. If trades are being inflated by the exchange, it is possible that

exchanges might just be taking prices from some external feed and adding noise.

Unless the initial exchanges are chosen wisely and with near perfect foresight, a

non-noisy price feed is just as good or better.

Alternately, Schelling point mechanisms [16], a.k.a. crowd oracles, can also

be used to set the price. The justification for this method is that it is hard for

voters to coordinate on a deceptive answer. However, with a pegged coin, there

exists a natural alternate coordination point: the pegged price. If this is a more

advantageous equilibrium for voters, then information obtained in this manner

is not going to be trustworthy. Many of these schemes use rewards for being close

to the median and slashing for voters far from the median to incentivize truth

telling. However, this may incentivize people to answer how they think others

will answer, commonly known in economics as the beauty pageant problem.

Take for example Basis, a variant of the dual coin example discussed earlier,

whose original design mentioned the possibility of using a crowd oracle. If users

correctly express that the stablecoin has appreciated and is trading above its peg,

more of the stablecoin will be minted, and users who only hold the stablecoin

and not the secondary coin will be diluted. This makes it such that the payoff

for holders of the stablecoin is higher if they lie and claim that the stablecoin

is trading at its intended price rather than its true price. Even if a user wants

to tell the truth, when enough people are incentivized to divert, the rest of the

honest users will have to lie, abstain from voting, or be penalized.

Terra tries to get around the problem of dishonest voting by sampling only

a subset of voters to make collusion difficult. However, if there is a non truthful

equilibrium that is beneficial for a majority of voters, then the subsampling may

not help. Celo also uses a crowd oracle and acknowledges that there is potential

for price manipulation. The designers of Celo trust that holders of the voting

token will prioritize long term growth over short term profit, which may be an

incorrect assumption. Some stablecoins are designed so that no external oracle is needed for the stablecoin to remain stable. In systems where users can always trade in for theunderlying collateral, such as Tether or Saga, there is no need for a price feed.

Instead, prices are measured using users’ trades. Individual users decide how

to value the token and then cash in or out accordingly. However, as previously

discussed, the convenience of not having to measure the price usually comes at

the cost of having to store collateral.

MARKET BACKGROUND

The metaverse is an online virtual world incorporating augmented reality, virtual reality and 3D holographic avatars. The term 'metaverse' was first coined in 1992 by sci-fi author Neal Stephenson in his book "Snow Crash", which envisioned a world where life like avatars interacted in 3D buildings and other virtual environments. Corporations such as Meta and Microsoft are aiming to make this world a reality. Using their already established footholds in both technology and social networking. both are taking enormous strides in making Stephenson's metaverse a reality, with projections that the metaverse market will be worth $US824 billion by 2028. Contemporary depictions of the metaverse also have strong parallels to Game-Fi, and what Game-Fi has tried to establish. Although most Game-Fi's environments aren't the same as what Meta or Microsoft are aiming for, they do represent what it is the metaverse is trying to achieve. A virtual world, where users can participate in activities for enjoyment or financial reward, essentially replicating the real world.

**3.**

DeFi SYSTEM

Decentralized Finance based system refers to the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed network. Decentralized networks strive to reduce the level of trust that participants must place in one another, and deter their ability to exert authority or control over one another in ways that degrade the functionality of the network. In a decentralized blockchain network, no one has to know or trust anyone else. Each member in the network has a copy of the exact same data in the form of a distributed ledger. If a member’s ledger is altered or corrupted in any way, it will be rejected by the majority of the members in the network.

Non-fungible tokens (NFTs)

Non-fungible tokens (NFTs) are digital assets that represent objects such as art, collectables, and in-game items. NFTs are stored on a digital ledger known as a blockchain that certifies the integrity of each asset and ensures that they're unique. As a result, the NFT market has experienced exponential growth, having increased by 2100% to US$2 billion in the first quarter of 2021. As of the third quarter in 2021 NFTs market is estimated to be worth an excess of US$10.5 billion.

CRYPTO EXCHANGE

Cryptocurrency exchanges are platforms that facilitate the trading of cryptocurrencies for other assets, including digital and fiat currencies. In effect, cryptocurrency exchanges act as an intermediary between a buyer and a seller.

OTC PLATFORM

An over-the-counter (OTC) market is a decentralized market in which market participants trade stocks, commodities, currencies, or other instruments directly between two parties and without a central exchange or broker. Over-the-counter markets do not have physical locations; instead, trading is conducted electronically. This is very different from an auction market system. In an OTC market, dealers act as market-makers by quoting prices at which they will buy and sell a security, currency, or other financial products.

**4.**

PROOF OF STAKE

Since cryptocurrencies are decentralized and not under the control of financial institutions, they need a way to verify transactions. One method many crypto use is proof of stake (PoS). Proof of stake is a type of consensus mechanism used to validate cryptocurrency transactions. With this system, owners of the cryptocurrency can stake their coins, which gives them the right to check new blocks of transactions and add them to the blockchain. This method is an alternative to proof of work, the first consensus mechanism developed for cryptocurrencies. Since proof of stake is much more energy-efficient, it has gotten more popular as attention has turned to how crypto mining affects the planet. Understanding proof of stake is important for those investing in cryptocurrency. The proof-of-stake model allows owners of a cryptocurrency to stake coins and create their own validator nodes. Staking is when you pledge your coins to be used for verifying transactions. Your coins are locked up while you stake them, but you can un-stake them if you want to trade them. When a block of transactions is ready to be processed, the cryptocurrency's proof-of-stake protocol will choose a validator node to review the block. The validator checks if the transactions in the block are accurate. If so, they add the block to the blockchain and receive crypto rewards for their contribution. However, if a validator proposes adding a block with inaccurate information, they lose some The proof-of-stake model allows owners of a cryptocurrency to stake coins and create their own validator nodes. Staking is when you pledge your coins to be used for verifying transactions. Your coins are locked up while you stake them, but you can un-stake them if you want to trade them. When a block of transactions is ready to be processed, the cryptocurrency's proof-of-stake protocol will choose a validator node to review the block. The validator checks if the transactions in the block are accurate. If so, they add the block to the blockchain and receive crypto rewards for their contribution. However, if a validator proposes adding a block with inaccurate information, they lose some The proof-of-stake model allows owners of a cryptocurrency to stake coins and create their own validator nodes. Staking is when you pledge your coins to be used for verifying transactions.

**5.**

Your coins are locked up while you stake them, but you can un-stake them if you want to trade them. When a block of transactions is ready to be processed, the cryptocurrency's proof-of-stake protocol will choose a validator node to review the block. The validator checks if the transactions in the block are accurate. If so, they add the block to the blockchain and receive crypto rewards for their contribution. However, if a validator proposes adding a block with inaccurate information, they lose some The proof-of-stake model allows owners of a cryptocurrency to stake coins and create their own validator nodes. Staking is when you pledge your coins to be used for verifying transactions. Your coins are locked up while you stake them, but you can un-stake them if you want to trade them. When a block of transactions is ready to be processed, the cryptocurrency's proof-of-stake protocol will choose a validator node to review the block. The validator checks if the transactions in the block are accurate. If so, they add the block to the blockchain and receive crypto rewards for their contribution. However, if a validator proposes adding a block with inaccurate information, they lose some of their staked holdings as a penalty. Mining power in proof of stake depends on the amount of coins a validator is staking. Participants who stake more coins are more likely to be chosen to add new blocks. Each proof-of-stake protocol works differently in how it chooses validators. There's usually an element of randomization involved, and the selection process can also depend on other factors such as how long validators have been staking their coins. Although anyone staking crypto could be chosen as a validator, the odds are very low if you're staking a comparatively small amount. If your coins make up 0.001% of the total amount that has been staked, then your likelihood of being chosen as a validator would be about 0.001%.That's why most participants join staking pools. The staking pool's owner sets up the validator node, and a group of people pool their coins together for a better chance of winning new blocks. Rewards are split among the pool's participants. The pool owner may also take a small fee.

WEB 3.0

Imagine a new type of internet that not only accurately interprets what you input, but actually understands everything you convey, whether through text, voice or other media, one where all content you consume is more tailored to you than ever before. We are at the tipping point of a new phase in the web’s evolution. Some early pioneers call it Web 3.0.

Arguably, there are a few early-stage Web 3.0 applications that already exist today, but until the new internet becomes fully embedded in the web infrastructure, their true potential cannot be observed. Web 3.0 is the upcoming third generation of the internet where websites and apps will be able to process information in a smart human-like way through technologies like machine learning (ML), Big Data, decentralized ledger technology (DLT), etc. Web 3.0 was originally called the Semantic Web by World Wide Web inventor Tim Berners-Lee, and was aimed at being a more autonomous, intelligent, and open internet.

**6.**

The Web 3.0 definition can be expanded as follows: data will be interconnected in a decentralized way, which would be a huge leap forward to our current generation of the internet (Web 2.0), where data is mostly stored in centralized repositories. Furthermore, users and machines will be able to interact with data. But for this to happen, programs need to understand information both conceptually and contextually. With this in mind, the two cornerstones of Web 3.0 are semantic web and artificial intelligence (AI).

Web 3.0 Technologies: There are a few details that we need to keep in mind when looking into Web 3.0 tech. First of all, the concept isn’t new. Jeffrey Zeldman, one of the early developers of Web 1.0 and 2.0 applications, had written a blog post putting his support behind Web 3.0 back in 2006. But talks around this topic had begun as early as 2001.

Evolution of the Web 3.0 Technologies: Web 3.0 will be born out of a natural evolution of older-generation web tools combined with cutting-edge technologies like AI and blockchain, as well the interconnection between users and increasing internet usage. Apparently, Internet 3.0 is an upgrade to its precursors: web 1.0 and 2.0.

Key Features of Web 3.0**:** To really understand the next stage of the internet, we need to take a look at the four key features of Web 3.0: Ubiquity Semantic Web Artificial Intelligence 3D Graphics Ubiquity, Ubiquity means being or having the capacity to be everywhere, especially at the same time. In other words, omnipresent. In that sense, Web 2.0 is already ubiquitous since, for instance, a Facebook user can instantly capture an image and share it, which then becomes ubiquitous since it's available to anyone no matter where they are, as long as they have access to the social media platform. Web 3.0 simply takes this a step further by making the internet accessible to everyone anywhere, at any time. At some point, internet-connected devices will no longer be concentrated on computers and smartphones like in Web 2.0 since IoT (Internet of Things) technology will bring forth a plethora of new types of smart devices.

**THE BITCON1: VISION & MISSION**

Like the protocol, it is set in stone. Such a vision will not change in the next year, decade, or century. The only thing that will change here is that the numbers will get more favourable to the consumer. After Bitcon1 scales to billions of transactions, it will scale further.

The community has a vision of a system that scales to billions of transactions a second, a system open to anyone globally, a system that costs no more than a thousandth of a cent for a standard transaction of 250 byte, no matter where you are in the world and no matter what you are doing. A system that is completely traceable and works within the existing legal structures.

We aim to create such a framework which makes it feasible for every sector to build a trustable and reliable data ledger system. An open-source toolkit which will streamline the deployment of blockchain throughout a broad and diverse sector.

The purpose of Bitcon1 is not to take down banks or governments. Bitcon1 is a tool. The aim of Bitcon1 is to make a secure, robust electronic cash system that can provide micropayments and the ability to conduct transactions globally, for values as low as or lower than a thousandth of a US cent. Bitcon1 is a competitive system, one that helps deliver value to the consumer. The purpose of the system is to exchange value quickly, easily, and for very low fees.

There is no such thing as too large a volume. There is no such thing as spam. There is no such thing as a system that cannot be seized or frozen using a legally issued court order. And there is no such thing as a transaction within the law that should not be sent. Very simply, Bitcon1 is a system designed to grow with transactions and allow the transfer of value globally, within milliseconds, without all the existing cost infrastructures that an expensive system like the Visa network or the MasterCard network brings with it.

Finally, Bitcon1 is set in stone. The protocol is fixed. In other words, any transaction made today will work in a year and a decade or a century from today. If you write a transaction and sign it and hold it off-chain, the same transaction will remain valid and be processed by a miner without any need for resigning or alterations as long as the system is functioning. For instance, if Bitcon1 is working 200 years from now, somebody writing a transaction today can expect and have a contractual right to have the transaction sent to the network and processed by a miner in two centuries from today. The protocol doesn’t change.

Bitcon1 aims to open up opportunities for those who work in global markets where the remittance industry takes a large percentage of their money. Bitcon1 will open up opportunities for those in poverty-stricken countries without access to banking services. Bitcoin will remove many of the problems associated with no longer having access to bank accounts and relying on payday lenders and check-cashing services that can take up to 30% of their already meagre income.

Bitcon1 has the potential to revolutionize a range of sectors where trust is needed among parties with misaligned interests.

The coin is widely spreading its network to play a vital role in the entertainment industry by trading non fungible tokens (NFT’s) of most appreciated movie dialogues and celebrities giving a new way to the investors and fans to connect with the entertainment industry. The coin would be primarily used to trade talent NFT’s providing a new scope of investments for rising talents.

Globally, the supply chain industry is fragmented – with many parties operating in silos. Bitcon1 aims to play a vital Role in supply chain and partners with Novuszilla, presenting a technology that would have far-reaching implications for global trade and supply chains – bringing standardization, alignment and transparency.

Bitcon1 will be completely traceable while protecting privacy. Such technology will aid in reducing corruption. If large-scale money transfers are linked to organised crime or other forms of corruption, the ability to trace, freeze, and seize bitcon1 will enable the imposition of controls to mitigate money laundering and ensure that it is not designed to promote anarchy. On the contrary, it is designed to ensure that anarchy fails.

NOVUSZILLA CRYPTO EXCHANGE

Novuszilla crypto exchange provides you with the most trusted crypto trading experience as it comes up with a complete decentralized finance based system where everything works in front of you, this peer to peer transactions system do not ask you to transfer your assets to a third party. We charge no trading fees, no brokerage which allows our user base to do more and more trades everyday. This is a decentralized exchange where you do not transfer your funds to a third party and we do not ask for user identity as all the payments are blockchain based. Novuszilla’s team aims to get our user base stable crypto returns with finest trading experience, for this purpose novuszilla crypto exchange provides our user base with 100x leverage to frees up your capital since you only have to commit a fraction of the value of the assets you are trading. Providing you with 100x leverage, gives you an opportunity to take much larger positions than would be possible with trading the actual underlying asset. It means you can make the most out of your capital and invest in a range of different assets, instead of restricting yourself to one or two.

NOVUSZILLA NFT MARKETPLACE

Novuszilla NFT marketplace is an exclusive platform which can trade users NFT’s to a large database as we are connected to multiple nodes - NFT Marketplaces from all over the world. We mainly come up with four categories of NFTs- Celebrity NFTs, Talent NFTs, Players NFTs and user minted NFTs. This is an exclusive opportunity for all the fans to have a hold over their favorite artist NFT’s, by collecting their memorable moments. The world needs ideas and innovation to make progress against the many problems we face. Creative and talented people that can contribute to this important work are everywhere, but the opportunity to develop is limited to only a small number of well-off children. As a consequence of this, we all – the entire world population – are missing out on the creativity and innovations that would enrich our world and help us move forward. For this purpose Novuszilla segregates the NFTs available on our NFT marketplace into these four categories and give opportunities to every talent to showcase their artwork. By bringing in multiple blockchain technology we let you choose your comfort of gas fees or no gas fees at all. Small and unrecognized artists cannot afford to pay huge gas fees which is why we tend to work on Binance smart chain- dealing with the minimal gas fees. Hence, we tend to come up with the most convenient trading experience for NFT’s. Not just NFT trading but our exclusive NFT portal also provides you with the data analysis of all the NFT’s globally being traded. This includes the data of high demand NFT fluctuations in the market and on which platform that NFT is being traded. With the R & D of these data users can easily decide which NFT’s they want to invest in and till what time period. These facilitation will increase the credibility of BitCon1 in huge crypto market.

**8.**

NOVUSZILLA OTC PLATFORM

We bring in the most exclusive and convenient way of trading, for which novuszilla provides you with over the counter service. Over the counter helps you know our team, by getting the chance to sit and trade with us. We make sure to make you understand everything on the table to get the most tremendous returns. We hope to host you in the best ways possible.

NOVUSZILLA METAVERSE BETTING AND GAMING APPLICATIONS

In a world full of gaming, we aim to bring you an unbelievable gaming experience where you feel every bit of the surrounding of your virtual game just sitting at your place. You can simply earn by spending your time on our application. You build your own immortal virtual avatar which lives in that virtual world and can only be controlled by you. The value of that avatar depends on the credibility of your performance in our virtual world. The avatar will be tokenized through blockchain and the value would be based depending upon the performance of avatar in the virtual world. This avatar would be your immortal virtual self which would always operate according to your instructions in that virtual world. The betting would take place through the avatars which would be AI and web 3.0 based. In this day and age, practically everyone wants to do betting just through the phone for which we provide you with a full-featured version of the betting application that will work on Android or iOS.

BITCON1 COIN

**9.**

BitCon1 Coin is the Native Cryptocurrency of the Novuszilla Platform. This is an utility coin which is integrated with metaverse, made to generate stable profits and provide higher returns to our stake holders. BitCon1 coin is also a talent driven coin which aims to bring the entertainment, Sports and other industries onto the blockchain. BitCon1 coin is associated with this all in one crypto platform giving it more value than ever. The phases in which the coin would come in the market is mentioned in this whitepaper. Every asset moves on the protocol of demand and supply theory whether it is cryptocurrency, NFTs or Fiat currency. For which we have listed all the utilities of BitCon1 cryptocurrency in the given document.

BITCON1 UTILIZATION

BitCon1 coin is a multifunctional utility token designed and powered by Novuszilla; a virtual world where you can add any amount of credibility to your immortal avatar and earn through it. Trading in the marketplace, crafting NFTs, Metaverse Betting applications, iGaming, Supply Chain, Health Care, Crypto exchange , Crypto wallet and automated staking programs, every function works with BitCon1 coin. To better understand the utilities of BitCon1, users are advised to start from the basic function – work as the medium of trading NFTs and services in the BitCon1 and Novuszilla.

(a) Bitcon1 in NFT MARKETPLACE

Bitcon1 is being used as a hope for a lot of the population, by being the ultimate mode of fundraising for the rising talents. Bitcon1 is used to trade in an exclusive NFT marketplace platform, which can trade users NFT’s to a large database; connected to multiple nodes - NFT Marketplaces from all over the world. Bitcon1 is mainly used to trade four categories of NFTs- Celebrity NFTs, Talent NFTs, Players NFTs and user minted NFTs. This is an exclusive opportunity for all the fans to have a hold over their favorite artist NFT’s, by collecting their memorable moments. The world needs ideas and Innovation to make progress against the many problems we face. Creative and talented people that can contribute to this important work are everywhere, but the opportunity to develop is limited to only a small number of well-off children. As a consequence of this, we all – the entire world population – are missing out on the creativity and innovations that would enrich our world and help us move forward. NFTs available on the NFT marketplace fall into these four categories and give opportunities to every talent to showcase their artwork. With the use of Bitcon1 it becomes an effortless experience for the users to trade NFTs.

(b) Bitcon1 in SUPPLY CHAIN

As blockchain technology is so new, supply chain decision-makers need clear guidelines, tools and frameworks to help them maximize the benefits and minimize the risks of this technology, this is where Bitcon1 comes in. This toolkit will be built by the industry and piloted, so we can see what works and what does not. We are going to piece together the puzzle, so others don’t have to start from scratch. Bitcon1 will make it an efficient process for the users and large MNCs to work on this idea.

Our multi-stakeholder community, representing large shippers, supply chain providers and governments, will design governance frameworks to accelerate the most impactful uses of blockchain in port systems – in a way that is strategic, forward-thinking, and globally interoperable; and by which countries across the economic spectrum will be able to benefit.

Our team will release white papers regularly focusing on the findings from the project community. The recommendations will include guidelines on data privacy, security, creation and use of data, public versus private platforms, interoperability, digital identity and signatures. Supporting an approach that considers the entire ecosystem promises to ensure an inclusive perspective and result that will benefit all stakeholders.

Working together to develop digital solutions and services to create efficient, accountable and transparent supply chains. Building solutions to ease the burden of compliance requirements and to eliminate counterfeit or substandard products.

Bitcon1 brings together governments, leading companies, civil society and experts from around the world to co-design and pilot innovative approaches to the policy and governance of technology. Bitcon1 Join hands to streamline new and complex logistic problems, helping to revolutionize sectors and ecosystems and build trust globally.

(c) Bitcon1 in HEALTH CARE

Bitcon1 has the potential to transform health care, placing the patient at the center of the healthcare ecosystem and increasing the security, privacy, and interoperability of health data. Bitcon1 aims to provide a new model for health information exchanges (HIE) by making electronic medical records more efficient, disintermediated, and secure.

A blockchain powered health information exchange could unlock the true value of interoperability. Blockchain-based systems have the potential to reduce or eliminate the friction and costs of current intermediaries.

The promise of blockchain has widespread implications for stakeholders in the healthcare ecosystem. Capitalizing on this technology has the potential to connect fragmented systems to generate insights and to better assess the value of care. In the long term, a nationwide blockchain network for electronic medical records may improve efficiencies and support better health outcomes for patients.

(d) Bitcon1 in iGAMING

The use of Bitcon1 will revolutionize the general way players make and receive payments on online gaming sites. Bitcon1 will make it easier, faster, and more secure for users to carry out online transactions. Some of the top online casinos are partnering with Bitcon1 to deposit and even withdraw. You

Due to the decentralized nature of Bitcon1, users can be guaranteed their data security with minimal chances of hackers intercepting the transaction. Users can receive their winnings faster than ever before as the prizes are directly deposited into their wallets. It does not rely on bank approvals which can take some time.

Bitcon1 have provided a more convenient payment method for users from all over the world. Transactions can be quickly deposited and withdrawn. Bitcon1 is efficient and transparent, and payments are processed faster than traditional currencies.

Players using Bitcon1 at online casinos can benefit from improved bonuses and promotional offers. Since the Bitcon1 system eliminate intermediaries in their transactions, the returns and benefits tend to favor the players more than when using traditional forms of currency. Experienced players can walk away with huge winnings from their initial investments.

The use of bitcon1 has made it easier to guarantee the fairness and reliability of online casinos from all over the world.There are smart contracts in place that ensures players will receive their winnings from playing online games. Casinos are bound by agreements and cannot break them. Players can be assured of the general fairness of the games too. The games utilize state-of-the-art software such as random number generators to keep the games balanced and fair for all the players. As the iGaming sector grows, the number of online casinos integrating Bitcon1 in their operations will also increase.

TECHNOLOGY

BitCon1 is made on Binance smart chain with a Proof-of-Stake consensus algorithm. Specifically, it uses something called Proof of Staked Authority (or PoSA), where participants stake BNB to become validators. This is based on a fully automated, Peer to Peer and decentralized finance based system replacing legacy and centralized institutions.

TOKENIZED ITEMS

Every artwork you see in The Novuszilla, from a movie clips to customized avatars of celebrities, and even whole planets, are all tokenized in BitCon1 Coin as tradable NFTs. There are four different types of NFTs in The Novuszilla as follows;

Celebrity NFT’s

This celebrity driven NFT platform launches Exclusive NFT’s which belongs to the celebrities. Celebrities create, mint and sell their NFT’s on The Novuszilla’s NFT Marketplace allowing the buyers bid as per their covenient prices of BitCon1. The celebrity would list their NFT from their own portal. Being fond of collectibles this is a great opportunity to get hands on these NFT’s before it gets traded to a level where we have no reach.

Crafted NFT’s

**10.**

In BitCon1 & Novuszilla, everyone can unleash their creativity to customize anything, such as clothes, transportation and houses. Users are allowed to mint their own NFT items, and the crafted items can be traded by BitCon1 on the marketplace.

Players NFT's

The global sports market reached a value of nearly $388.3 billion in 2020, having increased at a compound annual growth rate (CAGR) of 3.4% since 2015. We take immense proud to be having such great players integrated with us. Players NFT's would consist of tokenized artwork captured while playing their respected sports. These NFT's would be launched by the players by themselves. The investors can bid them in the given time period.

Talent NFT's

This is a social cause program initiated for all the young and unknown talents. We aim to bring these talents to the limelight by portraying their art in the form of NFT's. We would tend to have investors as stakeholders for their NFT's. This fund would further be used by the talent to enhance their artwork. As the talent is recognized in the real world, the NFT prices would increase accordingly, providing the stakeholders their deserved returns in BitCon1.

BITCON1 TOKEN SALE

All projects have initial token distributions in the beginning, whereby they decide how many tokens they will give, grant or sell, and to whom. These decisions also determine how ‘fair’ the project’s launch is. A well-organized token launch is one that anyone can attend, with only a small portion of tokens distributed to inside investors. It is also important to note that the centralization of token ownership goes against the key principle of blockchains, i.e., decentralization.

In the initial token distribution of BITCON1, We distribute tokens to four main groups: the public, their communities, insiders, and their own foundations. The public refers to anyone keen on investing in the project, while the community consist of users who are passionate about the project and find scope in the business model. Insiders are essentially the advisors and VCs, and the foundation is usually a non-profit that manages the project in one way or another.

Because crypto communities emphasize open-source principles, they expect the blockchain to permit funding from the public, who should receive ownership in return. Participating in Novus ICO leads to an ownership in the project as users buy the coins at the minimum value offered and get lifetime earning opportunity in correspondence to the growth of the company.

**11.**

Therefore we bring in the opportunity to buy the novus tokens initially at a lower cost getting a bonus everyday on the outstanding novus tokens in your wallet. The early you buy the higher bonus percentages you get.

You can sell the coins any-time after listing. In case of Referral incentives you can swap it with USDT any time after incentives received.

The following information in the whitepaper mentions about the coin supply and Referrals.

**7. ROADMAP**

|  |  |
| --- | --- |
| **PERIOD** | **ACTION** |
| 15th Nov. 2022 to 31st March 2023 | Pre-Token Booking of BitCon1  (Referral Program) |
| 19th Dec. 2022 | Novuszilla Wallet and Swapping  of BitCon1 |
| 1st Apr. 2023 to 30th Sept. 2022 | ICO at Respective Price |
| 15th Oct. 2023 | BitCon1 Coin Allotment |
| 20th Oct. 2023 | BitCon1 Coin Listing on Various Centralized Exchanges. |
| Q4 - 2023 | Novuszilla Blockchain Network,Data Storage Solutions for Supply Chain |
| Q1 - 2024 | Launch of Healthcare Blockchain Application |

**8. ICO PRICE ISOLATION**

|  |  |
| --- | --- |
| **SCHEDULE** | **PRICE** |
| 1st Apr. 2023 to 30th Apr. 2023 | $ 7.0 |
| 1st May 2023 to 31st May 2023 | $ 7.5 |
| 1st June 2023 to 30th June 2023 | $ 8.0 |
| 1st July 2023 to 31st July 2023 | $ 8.5 |
| 1st Aug. 2023 to 31st Aug. 2023 | $ 9.0 |
| 1st Sept. 2023 to 30th Sept. 2023 | $ 9.5 |

|  |  |
| --- | --- |
| **Listing Price Band, 20th Oct. 2023** | **$ 10 - $ 18** |

Note: All rights are reserved to change Price Band and Road Map Schedule (can be change as per the market response and coin booking volume) partially or fully are reserved with Novuszilla Ltd. & BitCon1 Management Board.

**9. CONTRIBUTE TO EARN**

*Refer to the Business Proposal.*

**12.**

**10. BITCON1 COIN DISTRIBUTION**

BitCon1 Token distribution is an integral part of NOVUSZILLA Crypto Chain. It describes the proportions in which different groups of users and investors own Novuszilla blockchain tokens. You can find token distribution in following chart where each piece represents a specific group’s ownership of the project.

|  |  |  |
| --- | --- | --- |
| **CATEGORY** | **Composition of Coins (In Cr.)** | **PERCENTAGE** |
| Talent Ownership | 5.00 | 20% |
| Development Fund | 0.75 | 3% |
| Marketing | 2.50 | 10% |
| Public Sale | 11.25 | 45% |
| Coin for Mining | 5.00 | 20% |
| Charity | 0.50 | 2% |

**BITCON1 STAKING PROGRAM**

Like a lot of things in crypto, staking can be a complicated idea or a simple one depending on how many levels of understanding you want to unlock. For a lot of traders and investors, knowing that staking is a way of earning rewards for holding certain cryptocurrencies is the key takeaway. But even if you’re just looking to earn some staking rewards, it’s useful to understand at least a little bit about how and why it works the way it does. We have come up with this very simple staking system valid only till the listing of coin. The staking returns are sent into the Novus wallet every day depending upon the amount of coins staked in token booked wallet .i.e daily percentage returns is directly proportional to the number of coins purchased in the ICO period. Following is the return values consecutive to the coins purchased. Note: This percentage is applicable according to ongoing phase coin price. As the coin price increases i.e. the ICO phases pass, the percentage return will decrease accordingly. Investor return percentage depends on the phase they participate in, the percentage return change with every phase. This Auto-Staking Bonus is available to anyone who booked their BitCon1 during this period

**13.**

**(15th Nov. 2022 to 31st March, 2023)**

|  |  |  |
| --- | --- | --- |
| **BITCON1 TOKEN SET** | **DAILY BONUS (300 days)** | **TOTAL BITCON1 BONUS** |
| 10 BitCon1 | 0.05 BitCon1 | 15 BitCon1 |
| 50 BitCon1 | 0.30 BitCon1 | 90 BitCon1 |
| 100 BitCon1 | 0.70 BitCon1 | 210 BitCon1 |
| 500 BitCon1 | 4.00 BitCon1 | 1200 BitCon1 |
| 1000 BitCon1 | 9.00 BitCon1 | 2700 BitCon1 |
| 5000 BitCon1 | 50.00 BitCon1 | 15000 BitCon1 |

**12. BITCON1 COIN FEATURING PLATFORMS**

* Pancake swap
* Binance
* BUY U COIN
* Coin DCX
* Novuszilla Crypto Exchange



**13. SUMMARY**

BitCon1 is a decentralized crypto currency at Novuszilla platform satisfying social and financial needs for all people around the globe. People have the opportunity to live an exciting life, where they can develop, trade and create digital assets in a futuristic virtual world. Furthermore, users have the chance to grow their real-world wealth by exploring and mastering the art of investments in BitCon1.Decentralized applications (dApps) are digital applications or programs that exist and run on a blockchain or peer-to-peer (P2P) network of computers instead of a single computer. DApps (also called "dapps") are outside the purview and control of a single authority. DApps—which are often built on the Ethereum platform—can be developed for a variety of purposes including gaming, finance, and social media.

**14.**

REFERENCES

1. Bitcoin: bitcoin/bitcoin (Oct 2018), https://github.com/bitcoin/bitcoin

2. Buttolph, S., Moin, A., Sekniqi, K., Sirer, E.G.: Avalanche token paper - token dynamics (2019),

https://files.avalabs.org/papers/token.pdf

420 3. Douceur, J.R.: The sybil attack. In: International Workshop on Peer-to-Peer Systems. pp. 251–260. Springer (2002)

4. Eyal, I., Gencer, A.E., Sirer, E.G., van Renesse, R.: Bitcoin-ng: A scalable blockchain protocol. In: 13th USENIX

Symposium on Networked Systems Design and Implementation, NSDI 2016, Santa Clara, CA, USA, March 16-18,

2016. pp. 45–59 (2016), https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal

5. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

425 6. Rocket, T.: Snowflake to Avalanche: A novel metastable consensus protocol family for cryptocurrencies. IPFS

(2018),

<https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV>

7. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger (2014)

8. Barghuthi, Y., Mezrin, V.: Jibrel network (2018), https://github.com/

jibrelnetwork/

9. Biggs, J.: https://tinyurl.com/y5bxzn6q

10. Bitbay: Bitbay: Decentralized peg (David Zimbeck), https://bitbay.market/

downloads/whitepapers/bitbay-dynamic-peg.pdf?utm\_source=medium&utm\_

medium=blog&utm\_campaign=dynamic-peg-whitepaper

11. Bitcoin.com: Mongolian central bank authorizes a digital coin (2018), https://

tinyurl.com/y8gsynkb

12. Price-stable cryptocurrencies, https://bitshares.org/technology/

price-stable-cryptocurrencies/

13. Brent, T., Colson, D., Elder, M., Fisher, H., Freeman, N., Ostman, J., Nostrand,

E.V.: Reserve stabilization protocol (2019), https://reserve.org/whitepaper.

pdf

14. Brooks, S., Jurisevic, A., Spain, M., Warwick, K.: Havven: A decentralised

payment network and stablecoin (2018), https://www.synthetix.io/uploads/

havvenwhitepaper.pdf

15. Brooks, S., Jurisevic, A., Spain, M., Warwick, K.: Havven: A decentralised

payment network and stablecoin (2018), https://www.synthetix.io/uploads/

havven\_whitepaper.pdf

16. Buterin, V.: Schellingcoin: A minimal-trust universal data feed, https://blog.ethereum.org/2014/03/28/

schellingcoin-a-minimal-trust-universal-data-feed/

17. Carats.io: Whitepaper (2018), https://www.carats.io/whitepaper.pdf

18. Carbon money, https://www.carbon.money/

19. Cascarilla, C.: Paxos standard (2018), https://account.paxos.com/whitepaper.

pdf

20. Centre: Centre whitepaper (2018), https://www.centre.io/pdfs/

centre-whitepaper.pdf

21. https://tinyurl.com/y7bb64r5

22. https://coinmarketcap.com/

23. Company, G.T.: The gemini dollar: A regulated stable value coin, https://bit.

ly/2oVLfkI

24. Eisele, S.: The white company launches white standard $usd-backed stablecoin,

bringing long-awaited liquidity, transparency, and stability to cryptocurrency holders (2018), https://tinyurl.com/y3ngachk

25. English, J.: Bridging the gap to a stable token (2018), https://blog.sweetbridge.

com/bridging-the-gap-to-a-stable-token-c4fdbd70e9c3

26. EOSDT: Technical specification (2019), https://eosdt.com/specification

27. Eufemio, A., Chng, K., Djie, S.: Digix’s whitepaper (2016), https://digix.

global/whitepaper.pdf

28. Epay usd: A compliant, stable value currency (2019), https://www.epay.com/en/

eusd\_white\_paper\_en.pdf

29. Findlay, S.W.: Q&a introduction to aaa reserve currency (2017), https://medium.com/arc-blog/

q-a-introduction-to-arc-reserve-currency-in-1-000-words-49bea91c22eb

30. Finlay, D.: Phi: Decentralized lending and stable currency might not actually be

stable (2016), https://tinyurl.com/julelge

31. Foundation, H.: Technical whitepaper (2017), https://static.coinpaprika.com/

storage/cdn/whitepapers/763.pdf

32. Georgen, C.: Topl: Empowering growth by enabling investment (2017), https:

//tinyurl.com/y4suph2r

33. Globcoin: https://globcoin.io/howitworks.html

34. Griffin, J.M., Shams, A.: Is bitcoin really un-tethered? (2018), https://ssrn.com/

abstract=3195066orhttp://dx.doi.org/10.2139/ssrn.3195066

35. Hertzog, E., Benartzi, G., Benartzi, G.: Bancor protocol (2018), https:

//storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor\_

protocol\_whitepaper\_en.pdf

36. Triennial central bank survey: Foreign exchange turnover in april 2016, https:

//www.bis.org/publ/rpfx16fx.pdf

37. Hoang, K., Zhang, D., Diwan, A., Guy, B.: Stably: Transparent reserve-backed

stablecoins for multiple blockchain protocols (2018), https://www.stably.io/

static/whitepaper.pdf

38. J.p. morgan creates digital coin for payments (2019), https://www.jpmorgan.com/

global/news/digital-coin-payments

39. Kamvar, S., Olszewski, M., Reinsberg, R.: Celo: A multi-asset cryptographic protocol for decentralized social payments, https://bit.ly/2HyGvLK

40. Kereiakes, E., Kwon, D., Maggio, M.D., Platias, N.: Terra money: Stability and adoption (2019), https://s3.ap-northeast-2.amazonaws.com/terra.

money.home/static/Terra\_White\_paper.pdf?201904

41. Kim, R., Choi, B.: Xank: A treasury-backed stability-guaranteed cryptocurrency

(2018), http://paper.xank.io

42. Kuo, E., Iles, B., Cruz, M.R.: Ampleforth - a new synthetic commodity (2019),

https://www.ampleforth.org/paper/

43. Labs, A.: Aurora: A decentralized financial institution utilizing distributed computing and the ethereum network (2019), https://auroradao.com/whitepaper/

Aurora-Labs-Whitepaper-V0.9.7.pdf

44. Lebed, A.: Stableunit: A low-volatility p2p electronic cash system (2018), https:

//stableunit.org/StableUnit-whitepaper.pdf

45. Lee, J.: Nu (2014), https://nubits.com/NuWhitepaper.pdf

46. Libra white paper (2019), https://libra.org/en-US/white-paper/

#introducing-libra

47. Maker: The dai stablecoin system (2017), https://bit.ly/2DwX21S

48. Mita, M., Ito, K., Ohsawa, S., Tanaka, H.: What is stablecoin?: A survey on price

stabilization mechanisms for decentralized payment systems, https://arxiv.org/

abs/1906.06037

49. https://mkr.tools/system/feeds

50. https://finance.yahoo.com/news/makerdao-governance-risk-call-march-191947369.

html

51. Neetzel, D., Konopka, R., Jeger, F., Trobe, B.L., Heyden, H.: Instant, feeless and

green p2p value transfer with fiat stablecoins (2018), https://docsend.com/view/

k9hyw3f

52. Neutral: Faq (2019), https://blog.neutralproject.com/posts/2019/05/14/

what-is-neutral.html

53. OneGram: Whitepaper (2018), https://onegram.org/whitepaper

**THANK YOU FOR YOUR VALUABLE TIME**

**For further queries, please write us at: info@bitcon1.com**

**15.**