Privacy, Community, Power

Verus consensus non emitur

“True consensus cannot be bought” - anonymous

Michael J. Toutonghi Michael F. Toutonghi Alex R. English

June 12, 2018

June 12, 2018

Abstract

The Verus Project aims to establish a secure, privacy-centric, fairly-distributed cryptocurrency. But – beyond this currency – Verus seeks to become much more than a zero-knowledge privacy coin, one with two completely new highly-decentralizing proof of work and proof of stake algorithms.

In addition to payments, decentralization, and privacy features, Verus Project plans include its direct use as a currency for provisioning scalable and secure public blockchains as a service (PBaaS), for Verus applications built upon these parallel chains to scale. What this will do is simple: It will enable all people – as well as all nodes on the Verus network to participate in and benefit from a decentralized, blockchain service economy.

This paper details the Verus vision and describes the function of Verus as its own platform, and also as a member of the Komodo platform ecosystem, in the context of its first applications. Verus core applications will provide a foundation to build additional applications and services, which will leverage Verus' automatically created blockchains, called autochains. Autochains – or PBaaS – will be provisioned and notarized by the Verus blockchain miners and stakers, in exchange for Verus currency.

Autochains will be validated through proof-of-stake by their user populations. In addition to extremely scalable, dynamic, publicly-secured autochain applications, this will add a dynamic isolation and security component to applications that can also create, manage, and verify transactions on the main Verus chain or any other Komodo-compatible, Crypto-Conditions [17], Interledger Protocol [25] enabled blockchains.

The ways we apply this technology to our world – to our biggest contemporary challenges – has the potential to completely remake the fabric of our society.

Preface

Human progress leapt forward with the invention of money. Money enabled worldwide, trade-based economies to move from a primitive, barter-based system to a consensus-based valuation and accounting of verifiable, storable, divisible, and scarce commodities as early currencies of exchange.

Even in recent times, actual or perceived scarcity and authenticity of source, whether genuine gold, an original giant coin of Micronesia [27] – or government backed notes with trusted fiscal management and the ability to exchange for oil – provide the foundation of value upon which, ultimately, human resources are bought and sold.

What blockchain does is straightforward. It enables the creation of cryptographic tools and applications that do nothing less than provide us with a new future of programmable money. This programmable money integrates directly with existent accounting functions and, eventually, with all automated services. Blockchain technologies provide humans with a new, verifiable solution to ensure scarcity, authenticity of source, inbuilt transferability, fungibility through privacy, and programmable rules. More than that, fully peer to peer, public blockchains disintermediate and provide tools that offer the opportunity to revitalize our economic systems and societies, potentially creating a more equitable and honest economic framework for all.

About This Document

This vision paper is not intended as a technical reference, but as a vehicle to communicate our vision, our plans, and our thinking – as we work on realizing the true potential of Verus.

All technologies described are based on a clear understanding of methods intended to implement each solution but – as with any project – the specific implementation details will be refined as we actually realize their functionality. To supplement this vision paper, we will follow soon after its initial release with a white paper, describing the new technologies developed for Verus Coin's initial launch, what benefits they provide, and provide details of their implementation. We will continue to supplement this vision paper with white papers, as appropriate, for each completed phase of Verus Coin's development, in the future.

As of this point, we have completed Phase 1, having released Verus Coin with zero knowledge privacy, two brand new algorithms combined for simultaneous CPU-mineable proof of work (POW) and fair proof of stake (POS) consensus, in-wallet mining and staking on PCs, leverage of and support for advanced Komodo platform technologies, and wallets and miners for every major PC operating system.

1 Introduction

Information vies for our attention in today's digital world, trying to convince us of what product to use or which politician to believe. We are watched and measured as we react to that information, in order to convince us what to buy or to believe. This is an active process that exploits our lack of online privacy – combined with weaknesses in human psychology – in order to make profit; extracting value from, even affecting our behavior, learning about and influencing each of us individually to open our wallets or add our voices to another's agenda.

No single person can digest and fully understand – let alone verify – a fraction of the information thrust at us in daily life. We are told to give up on the notion of privacy and to trust networks of companies with our most private data, our identity, our credit histories, our location, our habits. We are also told that our voices are lost in the digital sea of information. Yet how is this the same sea through which we are laser-targeted based on correlating our behaviors to learn so much about us, individually? What if these technologies could be turned towards the benefit of society, first – and then allowed to support businesses, in that context?

We on the Verus team believe it **is** possible to support businesses and governments requirements with digital systems that: 1) respect your privacy, 2) give you control over your data, and 3) enable you to speak your mind with the anonymous authority of an authorized voter or member of a community, in a way that can directly be heard and affect actual change.

Before we explain how, it would help to understand the shared beliefs behind our vision for Verus. These beliefs underpin everything we build into the Verus network:

1. We believe that every human has ideas, knowledge, and value to contribute to our society. By using technology to reward people for their contributions, we can enable each of our verifiable, yet anonymous voices to be heard as a collective truth.

2. We believe that those who contribute positively over time to the system should be rewarded for that contribution and provided with ongoing incentive.

3. We believe that a world-scale, peer-to-peer system that can enable humans to be queried directly, confidentially, verifiably – and in a transparent manner – can directly provide populations of people and the world with valuable, transformative tools.

With Verus, we will introduce digital tools to enable us all to build a better world together. We will monetarily incentivize – with our technologies – behavior that strengthens communities and institutions. This is the thing that's missing in the online world today: Fiscal incentive for communal behavior built into the very fabric of its function.

The Verus Project's tools will make it easy to create an identity – or multiple identities – on the Verus multi-blockchain system, which can accumulate value and even have multiple personas, each to represent a facet of your identity as a whole. This reflects how we might express identity in our personal or professional lives, where some situations call for provable credibility, yet others require no more information than what you might reveal when encountering a casual stranger.

Each identity will have its own, unique address. Unless its owner reveals information to link two or more identities, it is cryptographically hard – meaning virtually impossible – to correlate one identity to another. At the same time, the owner of an identity can still cryptographically verify statements made about identities under their control, attesting to identity properties (such as passport, age, height, citizenship, photo, etc.) as strongly as is possible with today's digital technology. As part of the Verus vision, to be described in more detail in later phases, we intend to support fully decentralized verification of identities that can provide as strong verification as today's centralized systems. At the same time, we believe it is important for practical reasons to enable compatibility with centralized forms of identity and to enable people to optionally support KYC in identities. To enable a smooth bridge between centralized and decentralized identity systems, today's ID systems, including biometric and government issued IDs, will be supported via centralized or decentralized verification to enable use of Verus identity in situations that require conformance to know-your-customer (KYC) regulations. Theseforms of ID, however, are not required to establish or use even strong, decentralized identities on the Verus network.

Verus autochains, will operate parallel to the main Verus chain and enable large-scale applications – such as polls or elections – to run simultaneously without concern for congestion or excessive fees. Autochains will enable poll application users to provision their own secure blockchains just by using the application – spawning dynamic parallel chains that can process thousands (or potentially millions) of transactions per second when needed. Autochains will operate by proof of stake, enabling each chain to have security isolated to its direct user population. Autochains will also be backed by Verus notarization and block time synchronization – providing the full weight of its PoW/PoS security layer as well as the Komodo platform's delayed proof of work (dPoW), to provide notarization all the way back to the full power of the actual Bitcoin blockchain.

For **Phase II**, what we expect to be an extended development phase, we will work to implement autochains and their first application in the world. We will eventually use them to create, secure, scale, and perform polls for everything from classifying online content, to identifying real public opinion, to actual, real-time elections for an organization or – conceivably – a government.

Our goal is to make these polls easy to use from a PC or mobile device, yet industrial strength and suitable for serious, secure elections. They will leverage the latest cryptographic technologies for privacy – known as zero-knowledge proofs – to preserve confidentiality.

They will be:

- **Confidential** — No one but the voter knows who or what they voted for – unless the voter discloses. Results of the vote can be withheld until the vote is complete, at which time they can be released to everyone, simultaneously.

- **Verifiable** — Only voters that are authorized to vote can vote. Each voter can vote only once. Each voter can look at the released results and see that their vote was counted.

- **Transparent** — Anyone can validate the number of votes counted, and the number of votes,each person or selection received.

- **Secure** — Our novel autochains – dynamic, security isolated, proof-of-stake (PoS) blockchains – are layered over proof-of-work (PoW) and delayed proof-of-work (dPoW) security, all the way back to the real Bitcoin blockchain through Komodo.

  By default, the first layer of security is run by the actual voters, themselves. Together, this provides unprecedented layered security both in the autochain and in delayed proof-of-work, leveraging the network with the most hash power in the world.

  We like to think that – on a Verus autochain – a 51% attack is called winning a poll.

- **Scalable** — Each poll is conducted on its own, automatically-created-and-validated blockchain, operating under its own visible validation rules.

2 Our Vision for Verus Foundational Applications

Throughout history, understanding what a population truly thinks or feels has been an invaluable capability. The manipulation of that understanding can, and has, repeatedly changed the course of history.

The Verus Project plans to use highly decentralized blockchain technology to enable all people to safely, anonymously, and confidently express their opinions – on any issue. Verus users will be able to share their knowledge in a public forum, query a population of humans (or eventually both AIs and humans), quickly and effectively, and – importantly – earn cryptocurrency in exchange for these contributions to collective knowledge.

A primary goal of the Verus Project is to enable societies and organizations to make decisions based on a more honest understanding of the public's actual beliefs. To achieve this goal, we consider the need for both confidentiality and transparency, to ensure that – first and foremost – the system can be trusted. It is also critical to prioritize decentralization and develop a core platform that can leverage fully transparent blockchain technologies, while running many applications that respect privacy. With Verus, these applications can leverage zero-knowledge succinct non-interactive arguments of knowledge – or zk-SNARKs – the most reliable and tested iteration of proven, zero-knowledge privacy technology available today.

Our novel approach ensures that this technology can be used at scale, across any population size, throughout the world. Using the tested-at-scale infrastructure and tools of the Komodo platform, and Verus planned development of PBaaS – the Verus developers will build human organizational tools, including voting and fully self-sovereign identity with a reputation system that respects privacy. The goal, here, is a significant one, and these tools are planned in a way to allow entire human populations to transparently and directly share their knowledge and opinions – without the risk of privacy violation, spin or censorship.

Verus tools will also leverage human (and eventually non-human) intelligence at scale to solve previously challenging problems in a decentralized manner – financially rewarding those who contribute to their proper function.

To serve all people in the world simultaneously with these public, peer-to-peer tools, Verus introduces autochains. Autochains are a novel scaling model for blockchain systems. Autochains will enable full node miners to provide public blockchain provisioning services. These services will occur in transient, parallel chains, chains that are isolated from congestion, disruption, or interference from the main Verus blockchain. As an autochain operates, it is

almost completely parallel and isolated from the main Verus chain, except for the capability of posting transactions and proofs to Verus, for results and coordination across applications or people.

By combining privacy, polls at scale, and identity, Verus can be used to post polls and ask almost any question of a population or subpopulation of people, receive an honest – and, importantly – verifiable answer, and still respect the privacy of the respondents. When even the first support for polling is active on the Verus network, the Verus community will be able to vote on the long term direction of the Verus Project, itself.

Over time, Verus polls – used for purposes such as determining the accuracy of news online, for research, or even for political polling, will be combined with machine learning to enable all of us, as a society, to benefit directly from our collective intelligence without today's risks to our individual privacy. Verus will combine auditability and verifiability of transactions with the option of verified, confidential participation – meaning societies and organizations can directly understand what people think, feel, and believe, as populations – without taking control of their personal data or targeting some individuals, based on their answers or beliefs.

Ultimately, our vision for the Verus Project is to enable us all to directly participate in our own worldwide economy. Verus applications will enable any individual to speak up with the power of an authorized participant – and with the confidence of anonymity – to produce a verifiable, transparent, and honest flow of information throughout the globe. It will transform the way that anonymity functions in our current technological environment – prioritizing cooperation and providing the financial incentive for that cooperation to occur.

3 Important Verus Concepts

The longer term Verus Project vision of a better society through public blockchain services relies upon three fundamental pillars –where the correct operation of each strengthens the others in the form of a virtuous circle.

These pillars are:

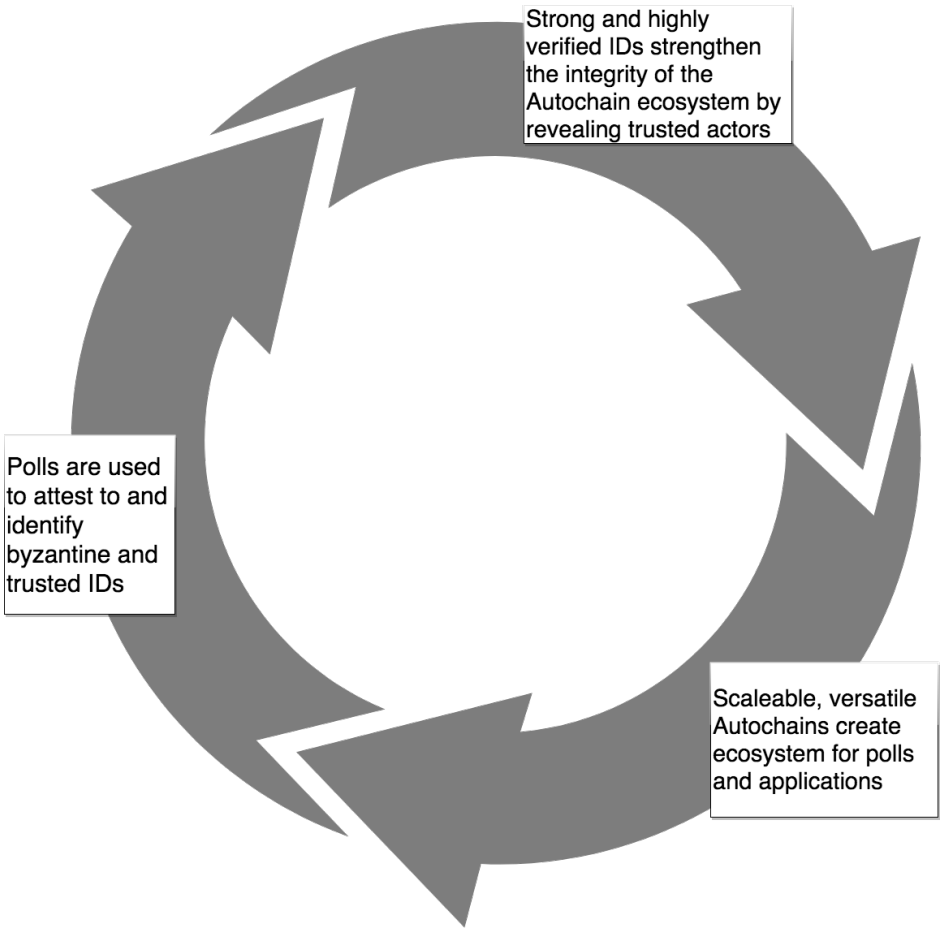
1. Extreme transaction throughput and scalable decentralized applications with autochains, which provide public blockchains as a service (PBaaS)

2. Selectively strong, private identity, and

3. Open application support with a foundation of polls, voting, and lottery selection services.

Each of these pillars will help us process human knowledge, understanding, and/or opinion on any content or topic. Together, they will enable direct querying – with confidential and truthful – answers across an entire population. It will create a secure, public platform that respects privacy, and can potentially serve as the foundation of a more respectful society.

It is also important to know about the the concept of **Verus Virtue** when reading further in this document. The best way to think about Virtue for the purposes of this document is as a separate currency that can be earned, but not purchased or sold, and is part of the



evolution of the Verus proof-of-stake algorithm, slated for later phases of the Verus project. Proof of Virtue is a technology that will be described in much greater detail and implemented in later phases of the Verus project.

3.1 Autochains

With Verus, we plan to create a platform upon which we will build voting and even election systems that support our vision of enabling a better society through blockchain.

To run simultaneous polls across disparate populations on one blockchain-based system, we need another dimension of information – one that retains privacy, and is anchored to a primary store of value, Verus.

One approach to creating another dimension of meaning would be a system of "coloring." The Ethereum blockchain system and some layers over Bitcoin or Bitcoin compatible coins use a version of a coloring system. [5][6][7][8]. While, at first glance, this seems like a reasonable approach, it is actually a suboptimal solution, at best.

With Ethereum and the ICO experiences of 2017 [9][10], we now know what happens when you create one blockchain and overload it with transactions: Congestion and unnecessarily high fees. Developers have proposed many solutions to this problem of scaling – including a move to proof-of-stake systems and sharding (effectively trying to separate the various

functions on a blockchain), or even a move to large systems of parallel chains with a common design.

Yet instead of implementing a "solution" with colored coins sharing one blockchain, we have decided to take a completely new approach to this problem. Our approach will not only provide an extra dimension of information and an unlimited number of token types, or "colors", but it will do so with highly scalable PBaaS autochains, which also reward Verus miners and node operators as provisioning agents. This is a novel method of scaling, one which provides significant scale and security benefits through isolation of transaction processing for each application instance on its own blockchain.

Rather than thinking of Verus as a single blockchain, it is more appropriate to think of it as a blockchain-based system, one that is rooted in a primary value chain.

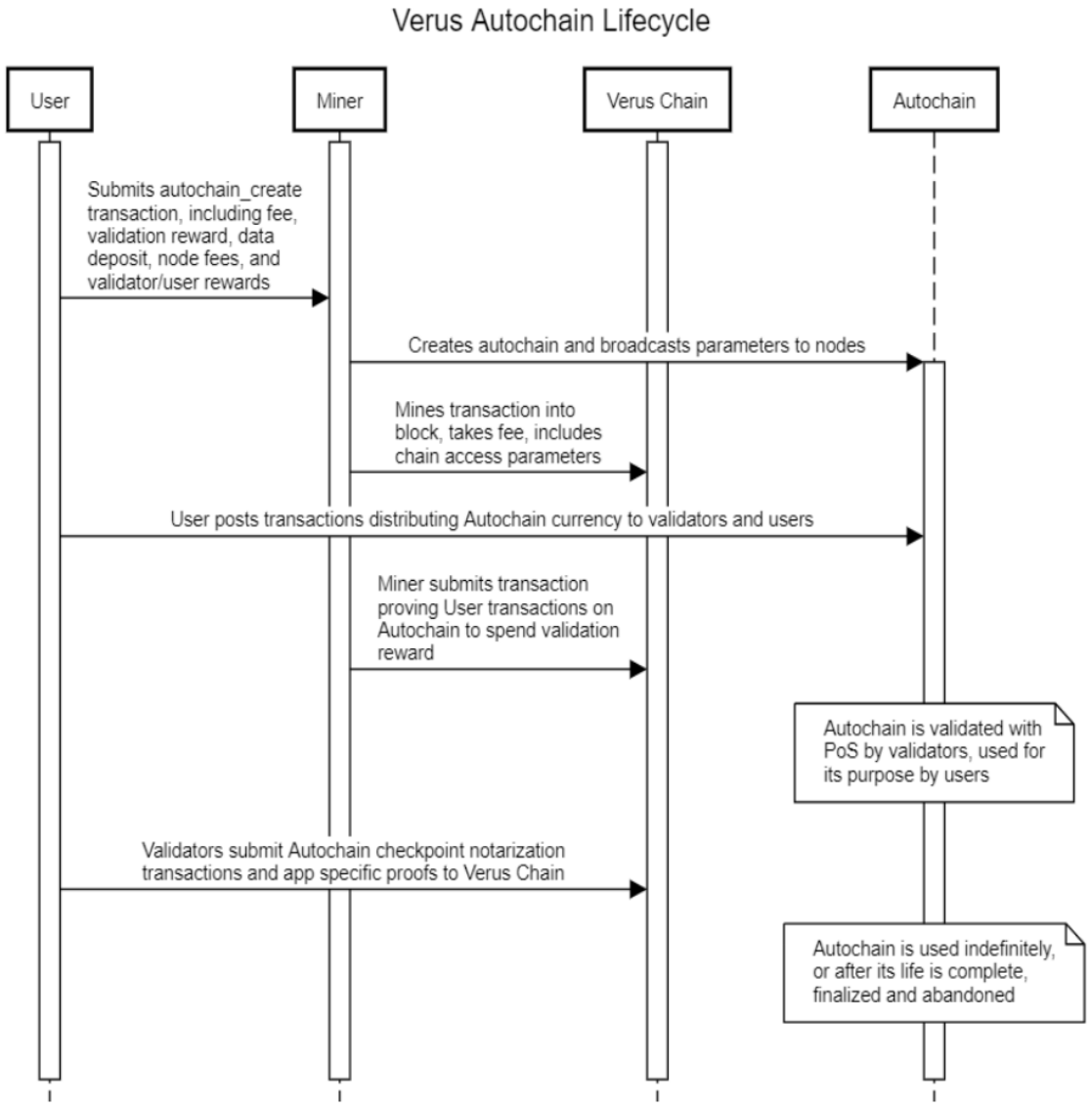
Autochains are exactly what they sound like – automatically instantiated blockchains that are validated initially – and when notarizing – by Verus miners, and otherwise, only by their users, often a disjoin set from the whole of Verus users. Autochains, once instantiated, can be used indefinitely or can have a finite lifetime to be used for a specific purpose. In this document, we will often discuss autochains in the context of a few concrete applications that we intend to implement on the Verus network. It is important to keep in mind that their versatility is **basically unlimited**. Due to their security being inherited from the main Verus chain, autochains eliminate perhaps the biggest disadvantage that creating consensus-based distributed ledger applications suffers from: Weak defense against attacks in their earliest stages.

In **Phase II**, Verus will define an autochain provisioning protocol, and specific voting protocols, based on blockchain transactions. These protocols will include zero knowledge proofs, Crypto Conditions [17], and Interledger Protocol [25] technologies to provide proper incentive for all participants to engage in the automatic creation and use of on-demand, isolated or public blockchains, ones that rest on a secure, public foundation.

The autochain protocol will also provide the ability to place a value on the data generated by the autochain's operation. This value will then either be released to the public or paid out, through rewards, to the participants in the creation of that data. This creates a model that incentivizes release of learning and information to the public – also making applications which do so much less expensive to run.

For Verus poll applications, validation will default to a form of proof-of-stake (PoS), where all members of the chain are stakers. This is because that security model matches exactly the interests of the majority of voters in having an accurate record. Because PoS does not involve powerful mining equipment or competition to solve a cryptographic puzzle, it can operate on much less powerful hardware– even on mobile devices. Since voters, themselves, secure the chain simply by running the voting software, poll chains are generally not affected by activity on the main Verus chain (except when posting interledger transactions). In addition, an autochain's operation, independent of scale, adds no overhead or congestion to the main Verus chain's transaction load – besides the transactions to provision the poll chain and post results back to the main chain itself.

Since we want to be able to create autochains from clients that may not be running full nodes or even own stable IP addresses, full nodes will be incentivized to provide reliable static node support for autochains. Once they provide this support, they will be recognized



by validators on the autochain. They will then be able to use this recognition to boost their reputation for selection in future lotteries.

By advertising autochain node support on the main blockchain – along with a stable payment address via a transaction – the node IP can be selected in a random lottery. The Eigentrust ratings of all nodes can then be recorded by all other nodes that serve the chain at regular intervals. Nodes which consistently offer better QoS will get better ratings. Nodes that get poorly rated will still share in the node rewards for the current blockchain – but will be less likely to be selected in the next node lottery.

3.2 The Virtue Autochain

3.2.1 Roots of Trust in Distributed Consensus

The Bitcoin [14] proof of work implementation introduced the world to systems that establish trust, not due to belief in any individual human's behavior, but based on the tendency of humans to act in their own self-interest.

The Bitcoin protocol rewards winners of a contest, referred to as "miners", in statistical proportion to the computing power they employ to "mine" for Bitcoin, as compared to the total computing power of all miners. For every block of validated transactions added to the Bitcoin blockchain, someone wins a competition to earn the right to define that block while adhering to specific, verifiable rules. The competition involves verifiably solving a statistical mathematical puzzle that is specific to exactly that block, meaning the same work cannot be reused on any other block. The winner of each competition earns the right to accurately process the next block of pending Bitcoin transactions and to claim a specific measure of Bitcoin, called the "block reward" (plus fees of all transactions in the block that was processed).

Mining competition serves to determine the amount of computing power a would-be attacker would have to control in order to mine of blocks that were not earned according to the intended rules, execute transactions that might otherwise be rejected, and prevent certain transactions from executing altogether. Based on the way that miners achieve consensus on what is the correct chain, forging a false Bitcoin chain to achieve this would require an attacker to control more than 50% of the total power of all miners – both honest and byzantine.

Since, right now, it is likely infeasible for any single actor to mount such an attack against Bitcoin, the largest network of hash power today, this type of competition, called proof-of-work (PoW), currently manages hundreds of billions of dollars of value, sends transactions of that value to anyone, anywhere, at any time, and does this all without any company, bank, or trusted third party, of any kind.

In addition to enabling secure management of large sums of money, PoW has also sparked a mining arms race and significant investment in computing power to claim Bitcoins and other cryptocurrencies, creating the equivalent of the world's largest distributed supercomputer doing nothing but the same calculations, albeit on different data, over and over again. As a result, one side effect of the public blockchains' PoW security system is massive power consumption and significant ecological cost.

Due to this, a great deal of research and development has gone into alternative consensus mechanisms [11][12][13]. Most serious PoW alternatives center around the concept of proof-of-stake (PoS) – the idea, that by putting something at stake commensurate with the value being transacted in the transaction flow, a rational staking person, known as a "validator," will choose good behavior within the ecosystem, so as not to lose their "stake."

Even though large systems are being built that depend on 100% PoS, there remains controversy over its robustness when users have incompatible interests, or when an attacker's stake is not valued as highly as the perceived value to be gained by corrupting the system.

Most modern PoS and PoW systems make a **fundamental assumption** about all miners; that they are either 'byzantine', and intend to compromise the system as a whole, or

'rational', in statistically the same proportions for all participants equally. One need only consider that if there was a way to learn a more accurate statistical function for each participant's probability of being **either** byzantine or rational, using such a function to determine who participates in the system's validation would improve its resistance to attack.

In fact, any accurate method of recognizing those who were attempting to strengthen the system – and thus who could statistically be more trusted than a byzantine or even average participant – could both decrease the power consumption and ecological cost of blockchain security and further strengthen resistance to attack. This then brings up the question: **"How do we recognize trustworthy participants?"**

Some methods studied and proven effective are the Eigentrust reputation management algorithm [20], and its improved derivative the Eigentrust++ mechanism implemented in the NEM blockchain [22]. Originally designed by Sep Kamvar, Mario Glosser and Hector Garcia-Molina in 2003, the Eigentrust algorithm is built to function on peer-to-peer networks. It aims to isolate byzantine actors in said networks by assigning each peer a public, global trust value based on their history of activity – clearly displaying a form of "rating" for each peer. Those with lower ratings are shown not to be trustworthy, and thus, are interacted with less by their peers.

Simply put, the algorithm assumes that if any given peer a trusts any given peer b, then it would also trust the peers trusted by b. Every peer calculates a local trust value for each other peer it has interacted with, based on the either satisfactory or unsatisfactory transactions it has had with each one. These local trust values are determined by each peer, and when peer a wants to know if they should trust peer b, say, before making a transaction, peer a would ask all other peers it knows to report on their local trust values of peer b and weigh their responses according to the trust values peer a has for each of them.

3.2.2 Proof of Virtue (PoV) Reward System

Using a model similar to the EigenTrust algorithm, Verus will introduce the idea of Proof of Virtue (PoV) **enhancement** to the PoS algorithm initially released in **Phase I**. In PoV, we intend to weight staking contests with both Verus stake and "Virtue", a special "currency", expected to be tracked on a Virtue autochain, and used as a **trust rating** of identities within the network.

In a similar way to the "amount of stake" used when staking, Virtue will add another component to the probability of being selected to process a block of transactions on the Verus Network. Its probabilities upon introduction will not change returns on the Verus PoS system, but addresses will gradually be able to improve earnings with a Virtue weighting – **based on recorded activity and behavior.**

In order to ensure that Virtue is both a rare and valued property, which drives correct behavior, it will neither be purchased, nor sold. Verus holders will have opportunities to earn a small measure of Virtue, which can then be further increased by staking the Virtue itself, when attesting to a fact for the network, validating information, or providing another measurable benefit to the network.

Since Virtue will have intrinsic value on the Verus network, there will be methods for transferring it through wallet ownership – for cases of probate or other necessity – but such behavior as a tool for trading in virtue will not provide a secure or intended method of

exchange.

The Proof of Virtue model will effectively be a **modified** form of PoS that is not based just on monetary value, but also on long term measurement of contribution, which will affect trustworthiness and earning power in the Verus network. The intent is to provide opportunities for more people to participate in the growth of a **positive functioning network** and to prevent potential attackers from being able to easily buy their way into an attack, adding yet another layer of security.

We expect to keep the PoW component as part of Verus security system for an indefinite period of time. We also expect to leverage the dPoW security of Komodo and its notarization into the Bitcoin blockchain as well.

3.3 Polls, Voting, and Elections

3.3.1 The Importance of Secure Polling

A great deal of research has delved into the best way to achieve confidential, verifiable, and transparent (CVT) elections electronically – with a few notable systems actually used in real life situations. These attempts, however, have been plagued with significant limitations, limitations that almost always risked either revealing the identity of a voter and thus eliminating confidentiality, or allowing attackers to impersonate legitimate voters, and put the validity of the vote into question [1].

This was shown in one of the first majorly adopted North American electronic voting systems, the Diebold AccuVote TS, which was announced in the year 2000 [4], at a time when, as a result of the Florida 2000 presidential election, the general public began to recognize numerous flaws in the widely-used punch card voting system [2]. Despite multiple studies discussing electronic voting systems – studies which clearly warned of security risks such as insider threats, issues with auditing, and network vulnerabilities – by 2004, the Accuvote TS system was deployed for major political elections in 37 US states [2], resulting in multiple serious problems that impact the legitimacy of numerous election results since, due to inherent flaws in its design that were never fully addressed [3].

Firstly, the "solution" that the system introduced to deal with voters submitting multiple ballots – and to solve the ballot anonymity problem – was to issue a single personal voting 'smartcard' to each vote. This smartcard, unfortunately, did not contain a complete identity, but instead contained a common election key among voters that voting machines simply checked to determine if the card belonged in the correct election [2]. The lack of any cryptographic unique identification on these cards was a significant security flaw, as user-programmable smart cards and readers almost instantly became commercially available on the internet for reasonable prices – making it extremely easy to mass produce homemade copies. Furthermore, due to the lack of a truly secure boot loader, operating system, or application, the system had numerous potential attack vectors, many of which were quite simple for an adversary. For example, any attacker with access to the operating system had the ability to modify ballot program files through the standard Windows Explorer application already included on each machine.

These serious failures in previously adopted electronic voting systems have literally **changed the course of history**, affecting the outcomes of major political elections that

decide the state of world politics. This highlights the importance of creating a system that is truly confidential, verifiable and transparent, and indicates the magnitude of one problem we plan to solve with Verus.

3.3.2 Running, Recording, and Scaling Polls - Transient, PoS Chains

Using autochains, Verus will dynamically create parallel voting chains on demand for each poll in its ecosystem. This creates improved, isolated security and allows for scaling in a virtually unlimited manner.

The Verus wallet, which will be used for voting, will also have the ability to validate blocks through proof-of-stake, blocks which, when enabled, will allow voters who are validating the election to earn rewards. These rewards will either be paid in Virtue for intrinsic polls, when available, or from outputs of the payment transaction that instantiated the poll. When a poll is complete, results are posted back to the main Verus chain. The chain used to run it can then be archived or deleted, and it is typically abandoned.

3.3.3 Poll Content and Distributed Hash Tables

While blockchains make excellent databases for permanent, non-repudiable records and public key management, they are not the best solution for storing large amounts of data, due to their massive duplication across the distributed network. Instead, a better model for distributed storage would look something like the Interplanetary File System, or IPFS, which is a peer-to-peer file system based on the Kademlia [18]19 protocol in an implementation that currently works well enough to use as storage for create/read/delete operations using hash commitments on the Verus blockchain to represent and index content.

While we are evaluating the IPFS, we are also looking at other distributed hash table solutions, such as Open DHT [26]. A key requirement for the Verus network is that mobile devices be able to participate in its operation. Open DHT is an efficient C++ library intended for use with small devices. IPFS does not yet seem to have much support for mobile at this time, though it does have a Javascript library that can be used from the browser or mobile apcancations [24].

Until IPFS is supplanted with another implementation, Verus applications will assume that when off-chain content is needed, it should be retrieved from IPFS, and for future compatibility, we will add a storage and version specifier. In order to store supporting poll or other content for dApps, the content owner must ensure that the content is pinned in IPFS, until it is no longer needed. By **Phase IV**, or earlier if there is significant demand, we expect to either support or provide a blockchain-metered storage solution that is more integrated and automatic to use for poll makers. Two options for such a system include a cross-blockchain integration with a decentralized payment/pinning solution, or to offer a simple service that charges in Verus to store and automatically pin content for specific lengths of time in IPFS.

3.3.4 Voting Models and Types of Polls

Verus will support numerous types of polls, those that use weighted or unweighted voting, that seek to expose truth or opinions, and polls that rate and choose collectively. In order to

create a sensible taxonomy for polls, one that people will understand, we define the following types of voting:

1. Multiple choice
2. Weighted multiple choice
3. Ranking
4. Rating

We also define the following types of polls:

1. Polls to classify
2. Polls to select
3. Polls to rank
4. Polls to rate

We do not expect Verus to support all voting and poll types in the early phases. In fact, until **Phase IV**, the Verus core team plans to focus on known requirements of multiple choice and weighted multiple choice voting. During or after completion of **Phase IV**, expanding support for voting and poll types will be higher priority.

Each type of Verus poll may support confidential or public voting, live or delayed poll results, online or offline vote authorization, and lottery selected vote authorization. We will roll out working vote models in phases, as well, initially providing solutions for weighted and unweighted selection voting, which fits well for both political and opinion polls as well as content classification and ID verification.

3.3.5 Intrinsic Polls

Once Virtue is activated, the Verus network itself will run specific, intrinsic polls that will be regularly available to identities with Virtue, based on a statistical lottery and weighted by their actual measure of Virtue. Participating in these polls, which will be used to classify content and perform basic, human verification functions, enables participants to help the system classify and rate content across Verus applications, enabling a rating system rather than censorship to allow each voter to set preferences for the ratings of polls they may wish to see.

Miners who provision autochains for these intrinsic polls will get the same rewards as miners setting up autochains for commissioned polls. The content for these polls will be taken from other polls and will be used to classify and rate those polls for easier discoverability and the user experience of poll services.

3.3.6 Privacy

There is a fair amount of confusion among the public about privacy on the blockchain. One common belief is that Bitcoin transactions are private, when in fact all Bitcoin transactions, as well as the public addresses between which value is transferred, are public information [21]. As with the Verus token and its blockchain, poll autochains will also support zk-SNARKs to ensure that votes which have not been disclosed by a voter remain provably anonymous to all other parties, while still being verifiable by the person who holds the keys to the address that cast them. Currently, based on standard smartphone hardware specifications and the memory requirements of zk-SNARK transactions, mobile phones cannot generate z-transactions. In coming releases of new Zcash technology this year, the z-transactions will be more efficient and still provide the same privacy guarantees. When these technologies are available, we will work to support them on the Verus chain, as well as use the increased efficiency to enable z-transactions and all Verus features on mobile devices as soon as possible. Until that is available, we will work to provide a mobile wallet for Verus transparent transactions.

3.3.7 Content Classification

While Verus is designed to provide invaluable tools to people across the world, any system without censorship will also inevitably allow the underbelly of humanity to show through. That means that while we would want all people to participate, we recognize that in order for that to provide the most positive experience for all participants, we must use the Verus poll system itself to recognize, rate, and classify the content on its network, enabling those who provide such a service through participation in polls to earn, while enabling the selective filtering of content based on value judgements and classification of honest populations.

While we recognize that the best early use case for such capability is in rating and classifying non-intrinsic polls themselves, the ability to classify content is a fundamental strength that Verus will increasingly develop over time. At first, we expect such classification to be applied to relatively simple tasks for humans, such as identifying toxic comments, hate speech, or categories of information. Even though these types of classification systems have largely employed machine learning systems running against privately curated training data, our vision is for Verus content classification to enable people to earn, as they classify content better than any machine learning system, but in a way that can be followed by the best machine learning algorithms, and generalized at scale.

3.3.8 Truth vs. Opinion

When classifying content, especially when you start to consider challenging classifications, such as misleading, propaganda, generally accepted fact, accurate versions of history, vs. classification of what should generally be accepted as toxic or rated content that people could reasonably answer objectively, one must consider the difference between fact and opinion. Selecting the winner of an election is a matter of expressing an opinion. Classifying content according to level of toxicity is a question of determining the factual answer to the question: what does the majority of the voting population believe the classification to be. Determining

whether an image in one photo is the same image as that from another is a question with an objective, if not determinable answer.

To ensure that Verus polls support polls that attempt to discover accepted truths, facts, and even credible emerging arguments, Verus voters will often be able to stake and either earn or lose Verus and in later phases, Virtue, by answering in a manner that matches consensus. For other polls, which are recognized as opinion polls, all answers are equally valid contributions.

3.4 Random Sampling as a Service

The Verus system will randomized selection for many of its functions, similar to its **Phase I** PoS block validation system. Blockchain lotteries will be generalized and used for selection of participants in randomized polls and in other cases where pseudo-random sampling is desired. The general principles behind Verus lotteries are the same, regardless of whether something similar to Algorand [29] for guaranteed selection or an original Verus algorithm based on difficulty, such as Verus PoS is used for selection. Lotteries use the blockchain as a random oracle and are based on the assumption that the exact value of a specific block hash from a past block in the chain cannot be modified by a byzantine participant to weigh the odds in their favor.

3.4.1 Participating in a Lottery

Since the Verus network is completely decentralized, all lotteries, including PoS, are potential, and there is no central server selecting and sending messages to those who qualified in a lottery. When lotteries are implemented as a general feature, if you would like to participate in any Verus lottery or poll that is distributing tickets via lottery, you must first determine that you qualify for the poll's requirements. You will then need to submit a transaction that proves that you have a valid claim and spend the output transaction of the lottery ticket to your address using that proof. By default, that spend will authorize you to be a validator on the autochain for the poll you are participating in, by providing you with the currency of that poll. You may validate the poll by leaving your wallet running, getting potential rewards in Verus or Virtue for both activities.

Lotteries will be useful for selecting subpopulations based on identity and claims people make about themselves or that others claim about them, which they are willing to share. While detailed discussion of Verus identity is beyond the scope of this paper's release, the Verus system will provide self-sovereign identity with the ability for identities to make very flexible claims and have them attested to by other identities. For example, a lottery may look for males between the ages of 18 to 25 among identities willing to share that information, which will even be possible to verify as strongly as through a validated passport or driver's license. Other polls may not require the same evidence backing claims. Polls may also have restricted voting, such as local political polls, where verification and authorization for the poll must be provided explicitly, often by mail to a physical address or in person in the form of a QR code or electronically delivered transaction to your Verus wallet.

3.4.2 Proof of Stake Lottery

A block validation lottery is a somewhat different form of lottery which allows you to claim the right to validate a block and its associated reward based on proof-of-stake (for autochains) or 50/50 PoW/PoS (for the main chain). The lottery requires that a prior block hash 100 blocks past combined with a qualifying UTXO of the destination public key hashed with the staking block height and then divided by the UTXO value must be under the current proof of stake validation difficulty. By dividing by the UTXO value, Verus weights proof-of-stake or proof-of-virtue in proportion to the amount of stake or virtue in the UTXO. If no one who qualifies to validate a block is online or no one responds with a submitted block validation in a certain amount of time, the blockchain will wait until someone mines a block using proof-of-work.

3.4.3 Ticket Harvesting Lotteries

There will be multiple ways to acquire tickets to participate in any particular poll. The manual ways emphasized so far may include receiving a poll with QR code in post or email or perhaps directly from someone taking a poll. In addition to these direct ways to receive a voting ticket, Verus will enable polls to be posted on the poll blockchain as transactions, the tickets for which are distributed from its outputs by lottery. This will work when the Verus ID functionality is available, and will enable polls to require presence of specific claims or attestations on an ID, as well as the number of participants to select in the poll by creating one transaction output for each, which is spendable by a cryptocondition [17] that defines the lottery conditions and random difficulty. The difficulty determines how often a particular block will match any attempt to harvest a ticket from that block.

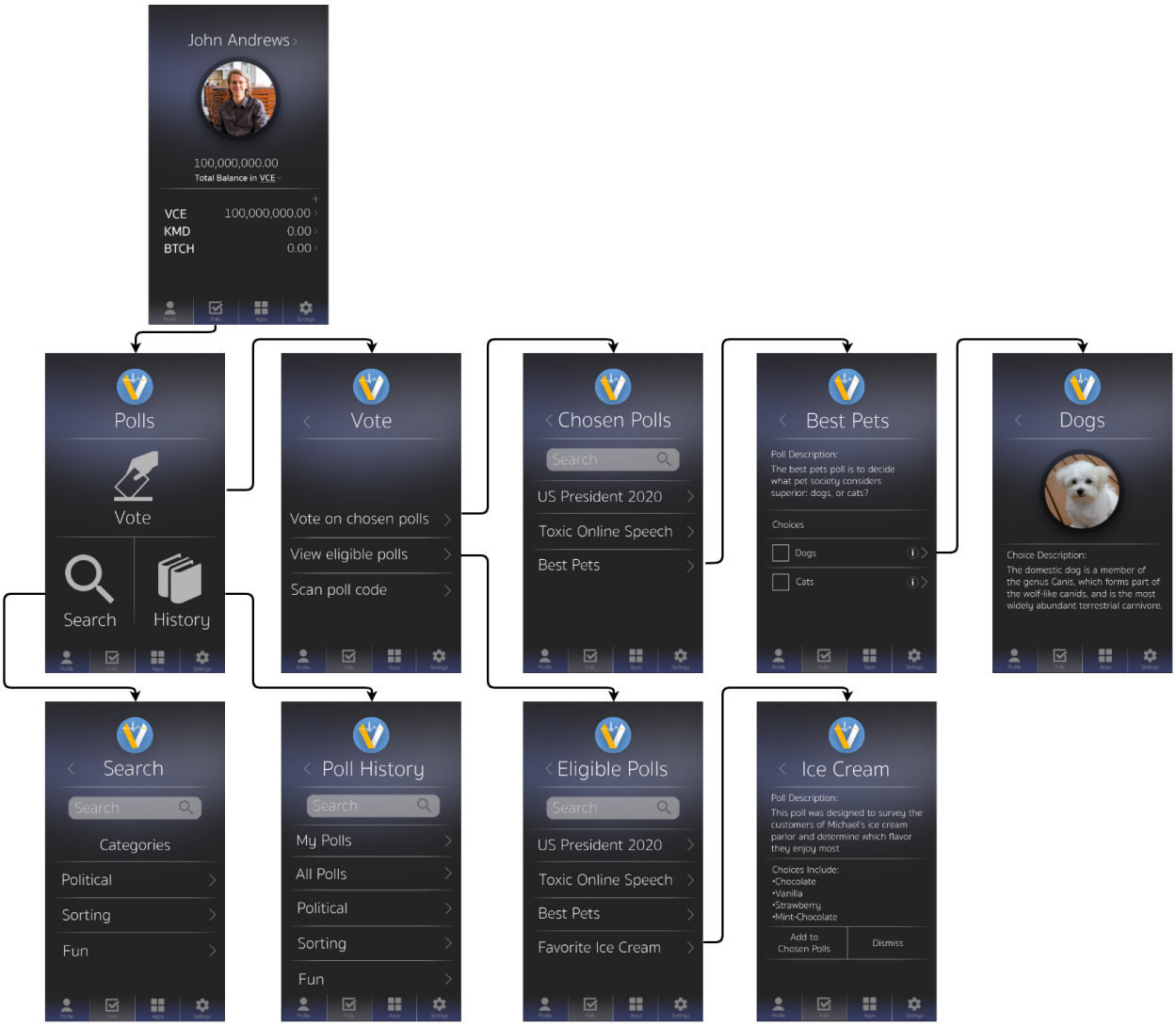
3.5 Machine Learning Integration

Verus enables humans to share and expose human knowledge through voting mechanisms to make decisions, express opinions, and classify accurately. The data used for that classification, as well as the classifications or decisions themselves provide an ideal source of training data for machine learning systems across any domain of human knowledge or opinion. As corporations gather, sequester, and learn from massive amounts of personal data in order to compete and boost their bottom line, rather than accrue to society's benefit, these massive private databases serve to affect and influence human populations by knowing more about them than others, or even than they know about themselves.

Since Verus enables humans to use voting mechanisms to classify and make decisions, and stores the results of this process in IPFS and on the blockchain, we will train machine learning algorithms on these results over time, allowing them to eventually classify and make decisions consistent with human decisions and values at an even higher scale. This will enable Verus to perform certain tasks automatically, such as the recognition of false or incorrect identification data among participants in the system, the initial classification or rating of certain content that can be overruled, but may not be appropriate for all audiences, and much more. The end result of this is a more secure and trustworthy network, built on consensus and trustless principles, leveraging worldwide human knowledge as a base of information and machines for scale.

A major Verus advantage over almost any other system in its use of Machine learning on human data is the innate privacy it provides to those whose data is used for learning, along with the default that all resulting information be made public, unless those making polls pay the Verus community a going rate to keep the data for themselves. In today's society, the goal of most machine learning systems is to match consumers with products they are likely to buy and/or manipulate them into an actual purchase, thus generating revenue. This creates a situation that can create unintended negative consequences when algorithms disregard any positive or negative effects its predictive abilities may have on society [23]. For example, if the algorithm recognizes that people with depressive episodes are more likely to gamble, and thus buy airline tickets to gambling-oriented locations, such as Las Vegas, it will advertise those airline tickets to those people. In the Verus system, machine learning algorithms will be able to learn from human beings, while being limited to accessing only the data users permit, and at the same time, being unable to easily target any specific individual.

3.6 Verus Mobile Polls



In addition to a desktop wallet that supports Verus and other Komodo platforms or compatible applications, mobile support is a high priority and will provide yet another layer of convenience for users, enabling them to use, earn, and spend Verus in everyday life. We intend to provide a Verus mobile experience that functions as a wallet, self-sovereign identity, provides easy access to the polling and earning applications, and is intended to server as an extensible application browser, capable of supporting additional applications that leverage the Komodo or compatible ecosystems. While we have already begun thinking about and storyboarding design and development of user experiences, we do not expect any mobile experience to be ready until completion of **Phase II** at the earliest. Even when the first mobile experiences are ready, they will not include the support for private transactions that we intend to enable as a foundation for confidential, mobile polling and communications. To get a feel for the way we envision Verus experiences working in practice, below is an example of some poll screens from early designs.

4 Implementation and Roadmap

After researching options from building the technology ourselves to leveraging unreleased advanced projects, to using one of the few well thought through blockchain application platforms, we decided to start building the Verus project as a friendly fork of Komodo and its asset chain technology, enabling us to both become a contributing member of and also enhance and extend the Komodo platform as Verus builds blockchain platform technologies and real world applications of PBaaS.

By leveraging proven zk-SNARK zero knowledge privacy technologies and Komodo's delayed proof of work (dPoW), which notarizes the main Verus blockchain into Komodo's blockchain, which is then notarized into the Bitcoin blockchain, we underpin Verus with a foundation of state-of-the-art privacy, security, and interledger transaction capabilities as our baseline. Above that, we have already developed advanced features that further enhance security, improve decentralization, and prepare for the implementation of autochains and proof of virtue.

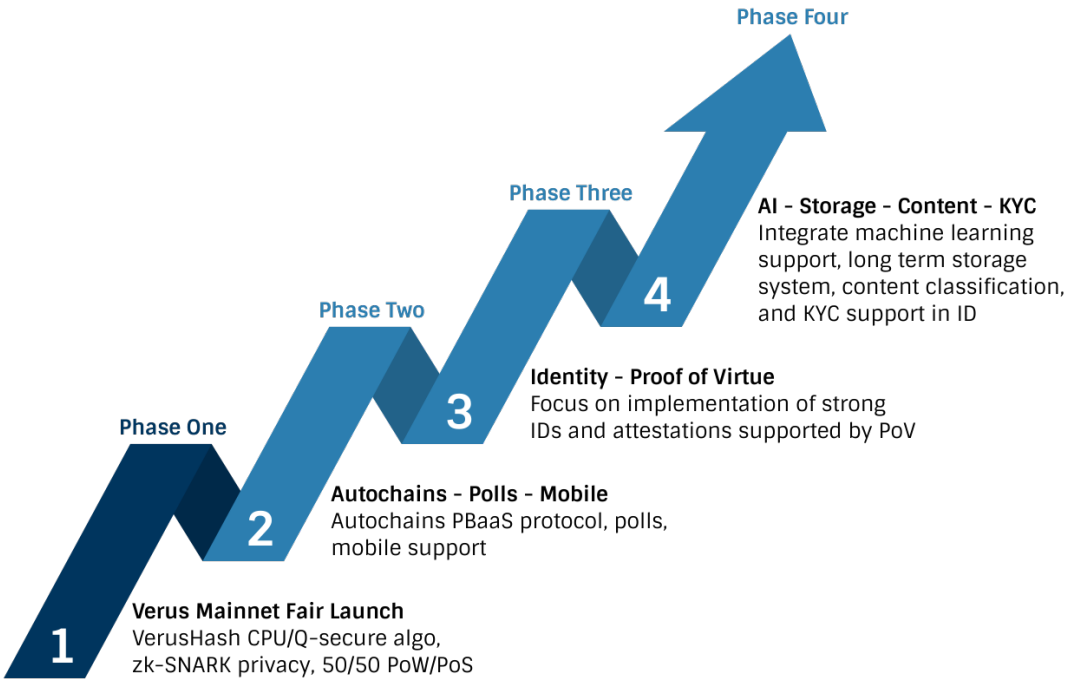
We will maintain our own open source fork of the Komodo platform and collaborate with the Komodo team when possible to develop new features or capabilities that can be accessed cross-chain by projects across the Komodo platform and even other blockchains that are simply compatible with Komodo's Interledger Protocol implementations. We will maintain our development as an open source project and contribute back to the broader open source community, as we leverage the contributions of others that have made it possible for us to begin realizing our vision as a community.

All that said, roadmaps are never perfect. Unless we significantly underpromise and prioritize a date so highly that no feature or capability is important in and of itself, targeting timeframes and milestones without specific target dates allows us to be ambitious in our goals and adapt to a changing world as we deliver. Even in **Phase I**, which we have delivered as of the writing of this paper, we adjusted our plan, and in an uncharacteristic turn of events, delivered even more than we had originally planned. We do not expect that to always be the case, and we will focus more on correct and complete phases than specific dates when possible. Sometimes, as with any major endeavor, the right choice is to recognize an

unexpected opportunity or obstacle, take two steps to the right or left, and only then proceed forward.

For the purpose of this whitepaper, we will discuss four phases of the Verus vision. We do not see these four phases as a completion of the vision as much as four phases of an ongoing mission to advance Verus and its contribution to society that we can currently express. From its inception and throughout the project, the Verus chain will serve as our fungible value chain, and use of Verus tokens on this chain will be the core value around which we continue to develop the Verus vision.

The first Verus chain, which is already available at the time of this white paper's release, includes zk-SNARKs for privacy, both transparent and private addresses, a brand new CPU-mineable hash algorithm for proof of work, a brand new proof of stake algorithm, and a unique emission schedule among fair launch cryptocurrency projects. Each phase of our project's development will introduce capabilities and experiences that provide independent value on their own, further leverage Verus Coin to power operation, and create a foundation upon which to build the next phase.



We intend and hope for the Verus project to become a worldwide, inclusive community effort, which welcomes and rewards those who contribute. Although we articulate these first four phases here, we see these phases as just the beginning, and we hope you will join us by participating in and contributing to the Verus project to make our world a better place.

4.1 Phase I – Mainnet – 50/50 PoW/PoS – Time Locks – Fair Launch

In phase one, the Verus main network began with a slow start and 15 minutes advance notice at 7:15am GMT, Monday, May 21st, 2018.

The Verus network began emitting first 0 block reward, rising linearly each block over the course of 7 days until block 10080 to its peak of 384 coins per block. The Verus emission schedule is as follows:

Era 1:

Block 0 - 10080 reward: 0 to 384, rising linearly and changing each block

Era 2:

Block 10080 - 53279 reward: 384
Block 53280 - 96479 reward: 192
Block 96480 - 139679 reward: 96
Block 139680 - 182879 reward: 48
Block 182880 - 226079 reward: 24

Era 3:

Block 226080 - 1277279 reward: 24
Block 1277280 - 2328479 reward: 12
Block 2328480 - 3379679 reward: 6
. . . halving indefinitely every 1051200 blocks (approximately 2 years)

We also added another fair twist on the launch that we believe will contribute to a more stable value growth in the Verus currency, without any unusual risk of dumping by any single party. During the first 5 months, Verus will have an accelerated reward curve for mining and staking, with a halving every month. During the first two months, when the block rewards are at or above 192 Verus, mined blocks will have time locked coinbase transactions, preventing spending, staking, or transferring of those coins for a period that varies from approximately 3 months after the genesis block, based on numbers of blocks, to 2 years and 3 months. These time locked coins provide a smooth release of the Verus currency supply as well as incentive to all of their owners to support the long term success of the Verus network and project.

From the very beginning of its operation, Verus operated with a dual proof of stake / proof of work mechanism for all participants. Verus mining with the VerusHash algorithm, as of this point, is a CPU-only algorithm, designed with a Haraka512 V2 [30] core to be quantum secure and to maximize performance on modern CPUs. While VerusHash was designed to be CPU-optimized and did not begin life with GPU or ASIC miners capable of beating CPUs in its mining, the Verus developers have no illusions that it is possible someone might develop either a GPU or ASIC-based miner that could be meaningfully superior to CPUs.

To ensure that such a solution if developed, remains open, jl777, lead developer of the Komodo Platform, has offered a 1 Bitcoin bounty to any developer who can make and publish in an open manner, a GPU miner for the VerusHash algorithm that can significantly outperform the current CPU miner. In order to win the bounty, the source code for the miner must be available under open source licensing. To be eligible for the bounty, any implementation must be able to perform 5x better than a modern, high thread-count, high clock-rate CPU on a GPU costing under $1000. By bringing up the Verus network this way, we established an immediate, baseline set of functionality, above which we can build out our project and community around a functional coin and project, as we stay in sync with advancements in the underlying Komodo platform.

Verus phase one release was pre-announced on Bitcointalk [28] with zero premine, and team members mined and staked along with everyone else to generate coins. In addition to coins mined by individual team members for their own benefit, the Verus developers intend to donate most of their mined and staked earnings to a community Verus foundation along with other donating community members who will join us, in order to support the ongoing growth and project development by core developers and the community for years to come.

4.2 Phase Two – Autochains, Polls, Verus Mobile

As soon as we completed phase one, we entered phase two, which includes release of this white paper, activation of the community through donations of some of our mined coins, and a push to finish planning for, development and release of mobile support, autochain capability, and the ability to setup, and then easily run CVT polls at scale.

4.3 Phase Three – Identity, and Proof of Virtue

In phase three, we plan to further improve the mobile experiences, implement the identity system, including support for strong, decentralized identity and attestations, separating photo IDs and other photo content into components that can be separately verified in unbiased human polls. At this point, we intend to support optional KYC strong identities, via both notarization of identities as well as poll-based identity verification. This will also be the first phase that supports Verus chain validation PoV enhanced PoS.

4.4 Phase Four – Integrated Machine Learning, Content, Storage

In phase four, Verus will begin to truly leverage the foundation built in phases one, two, and three by focusing on broad content classification capabilities for off-chain content, improving storage management support in its distributed hash table implementations, supporting storage monetization in some way, and providing open source, public implementations of machine learning systems that can learn from data on the Verus network to solve real world challenges of today and tomorrow.

5 Forward Looking Statements

This paper includes predictions, statements of intent, discussion of plans, estimates or other information that might be considered forward-looking. While these forward-looking statements represent our judgment and expectation of what the future holds, this is not an offer or solicitation to purchase any product, good, service, or security. All statements herein are subject to risks and uncertainties that could cause actual results of the Verus Project's development to differ materially. Furthermore, we intend to use the Verus blockchain as our open source development platform – contributing these technologies under permissive licensing for the betterment of society, not focusing solely on profit of anyone affiliated with the Verus project. You are cautioned not to place undue reliance, especially in any financial decision, on these forward-looking statements, which are subject to modification, update, or change for legitimate reasons both within or beyond our control. By expressing our vision and goals, the Verus Core developers are not obligating ourselves to revise or publicly release the results of any revision to these forward-looking statements in light of new information or future events.

References

[1] S. Estehghari and Y. Desmedt, Exploiting the client vulnerabilities in Inter-net e-voting systems: Hacking Helios 2.0 as an example, Proc. 2010 Electron. Voting , no. Section 4, pp. 027, 2010.

[2] Kohno, Tadayoshi, et al. Analysis of an Electronic Voting System. IEEE Computer Society Press, 2004, Analysis of an Electronic Voting System, http://avirubin.com/vote.pdf

[3] Hursti, Harri. "SECURITY ALERT: May 11, 2006 Critical Security Issues with Diebold TSx ." Black Box Voting, Black Box Voting, Inc, 11 May 2006, http://www.blackboxvoting.org/BBVtsxstudy.pdf

[4] Diebold Election Systems. AVTSCE source tree, 2003. http://users.actrix.co.nz/dolly/Vol2/cvs.tar

[5] Willet, JR, et al. "OmniLayer/Spec." GitHub, JR Willet, 24 Jan. 2017, http://github.com/OmniLayer/spec

[6] Stone, Andrew. "Bitcoin Cash Scripting Applications: Representative Tokens (OP_GROUP)." Medium, Medium, 16 Oct. 2017, http://medium.com/@g.andrew.stone/bitcoin-scripting-applications-representative-tokens-ece42de81285

[7] Abed, Gabriel, et al. "Colu Local Network." Colu Network, Colu Technologies DLT Limited, Jan. 2018, http://cln.network/pdf/cln_whitepaper.pdf

[8] Assia, Yoni, et al. "Colored Coins White Paper - Digital Assets." Google Docs, ColoredCoins, June 2017 , http://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit#heading=h.wxrvzqj8997r

[9] "Ethereum Blockchain Congestion Triggers Outrage." Global Coin Report, Global Coin Report, 12 Dec. 2017, http://globalcoinreport.com/ethereum-blockchain-congestion-triggers-outrage/

[10] Sedgwick, Kai. "The Ethereum Blockchain Is Congested by Cats." Bitcoin News, Bitcoin News, 4 Dec. 2017, http://news.bitcoin.com/ethereum-blockchain-congested-cats/

[11] "Delegated Proof-of-Stake Consensus." Delegated Proof-of-Stake Consensus - BitShares, Bitshare, 8 June 2015, http://bitshares.org/technology/delegated-proof-of-stake-consensus/

[12] Buterin, Vitalik. "A Proof of Stake Design Philosophy – Vitalik Buterin – Medium." Medium, Medium, 30 Dec. 2016, http://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

[13] Poelstra, Andrew. "On Stake and Consensus." WP Software, 22 Mar. 2015, http://download.wpsoftware.net/bitcoin/pos.pdf

[14] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, http://bitcoin.org/bitcoin.pdf

[15] Lee, James. "Komodo: An Advanced Blockchain Technology, Focused on Freedom." Komodo Platform, Komodo, 12 Mar. 2018, http://komodoplatform.com/wp-content/uploads/2018/03/2018-03-12-Komodo-White-Paper-Full.pdf

[16] Mercer, David, and Duke Leto. "HushList Protocol Specification." Git Hub, http://raw.githubusercontent.com/leto/hushlist/master/whitepaper/protocol.pdf

[17] Thomas, S., and R. Reginelli. "Crypto-Conditions." IETF Tools, 9 Jan. 2017, http://tools.ietf.org/html/draft-thomas-crypto-conditions-02

[18] Maymounkov, Petar, and David Mazieres. "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric." Parallel & Distributed Operating Systems Group, http://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf

[19] Benet, Juan. "IPFS - Content Addressed, Versioned, P2P File System." IPFS, http://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[20] Kamvar, Sepandar D., et al. "The EigenTrust Algorithm for Reputation Management in P2P Networks." The Stanford Natural Language Processing Group, http://nlp.stanford.edu/pubs/eigentrust.pdf

[21] "Some Things You Need to Know." Some Things You Need to Know - Bitcoin, 2015, http://bitcoin.org/en/you-need-to-know

[22] "NEM Technical Reference." NEM, http://nem.io/NEM_techRef.pdf

[23] Tufekci, Zeynep. "We're Building a Dystopia Just to Make People Click on Ads." TED: Ideas Worth Spreading, Sept. 2017, http://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads

[24] "IPFS js-ipfs Javascript Github Repository" https://github.com/ipfs/js-ipfs

[25] Thomas S., et al. "A Protocol for Interledger Payments",http://interledger.org/interledger.pdf

[26] Savoir-faire Linux Inc. "A C++ 11 Distributed Hash Table Implementation," http://github.com/savoirfairelinux/opendht

[27] Goldstein, Jacob, and David Kestenbaum. "The Island of Stone Money." NPR, NPR, 10 Dec. 2010, http://www.npr.org/sections/money/2011/02/15/131934618/the-island-of-stone-money.

[28] Toutonghi, Michael. "[ANN] Verus (VRSC) - Zk-SNARK Privacy, CPU-Mining, 50/50 POW/POS, Fair Launch." Bitcoin Forum, Simple Machines Forum, 21 May 2018, http://bitcointalk.org/index.php?topic=4070404.0

[29] Gilad, Yossi, et al. “Algorand: Scaling Byzantine Agreements for Cryptocurrencies.” MIT CSAIL, 24 Sept. 2017.

[30] Klbl, Stefan, et al. “Haraka v2 – Efficient Short-Input Hashing for Post-Quantum Applications.” International Association for Cryptologic Research, 24 Dec. 2016.