zelcash

innovative | intuitive | intelligent

white paper version two

TABLE OF CONTENTS

Introduction

Blockchain technology will change the world in ways that couldn't have been imagined five years ago. MarketsandMarkets predicts a 61.5% annual growth rate through at least 2021, and the World Economic Forum report predicts that by 2027 10% of global GDP will be stored on blockchain-related technology.[1],[2]

Blockchain's transparency, immutability, and disintermediation eliminate the need for a third party, reducing fees, enhancing security, and eliminating counterparty risk. It offers simplicity: Operations are added to a single public ledger, avoiding the clutter, chaos, and headaches generally associated with multiple ledgers.

Perhaps most important, blockchain empowers people, giving them more control over their transactions and interactions with information and financial dealings (not to mention their own data).

Clearly, blockchain offers tremendous potential to reshape privacy and security--and, ideally--transform the global economy.

But *only* ideally, at this point. Lack of accessibility and usability have stalled adoption. Scalability issues abound. Other challenges include distributed denial-of-service (DDoS) attacks, crashing exchanges, a lack of fiat gateways, and--especially for the average user--a baffling system of hex addresses. The result: siloed ecosystems, security vulnerabilities, and high--sometimes insurmountable--barriers to entry.

As outlined in this paper, we plan to address--even solve--these issues.

Our platform provides an intuitive, frictionless experience, facilitating cross-chain transactions in a simple and clean interface for users and developers alike. With Zel, we created an all-inclusive and standardised environment that allows developers to focus their efforts on the blockchain solutions. This will foster the free creation of DApps and smart contracts that are open to all.

The vision articulated and the solutions described in this whitepaper represent the first steps toward demolishing barriers, driving global blockchain adoption, and effecting disruptive transformation.

---

[1] "Blockchain Technology Market--Global Forecast to 2021" MarketsandMarkets research *Blockchain Daily News*
[2] Deep Shift Technology Tipping Points and Societal Impact --World Economic Forum www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Mission, Vision and Values

The Zelcash team was founded by like-minded individuals that believe technology can do great things for the development of mankind. We believe in the vision of a decentralised world, for the betterment of all. As a team, we have set a goal to become the **leader in blockchain front end and privacy development**. Our community is what will drive the project, with inspiration from others in the space. Our goal is to be leaders in the blockchain industry and let the technology drive the project with community involvement. Zelcash aims to create tools necessary for developers to expand on the impressive power of blockchain technology, led by our strong team and community, to deliver powerful technology available to all.

The culmination of Zel strives to be a fully decentralised and scalable worldwide network of compute power, enabling developers to utilise the power of the Internet untethered, provide easy-to-use transaction of value instruments to the “Unbanked” people of the world that have been all but forgotten by traditional monetary institutions, and expand on the seemingly infinite potential of blockchain technology.

Overview

The purpose of this paper is to provide in-depth detail on Zel's technologies and features that have been released or are pending release. We want this paper to be clear and accessible to all while, at the same time, ensuring that key technologies are discussed. It will *not* provide in-depth technical breakdowns for unreleased products until Zel Technologies has released--or is about to release--the products into the public domain. This will ensure that the development of Zel Technologies is not copied before the actual release.

Although some of Zel's products and services (such as ZelTreZ) are closed-source, they will be "code audited" by an independent third party. The Zel team strongly believes in open source; where we can, we will ensure that our software and technologies are released open source, along with the technical details.

To that end, this whitepaper is not intended as a technical reference or prospectus, but as a vehicle to reveal what we have accomplished so far and to communicate our vision and plans as we work on realising the true potential of Zel. In that spirit, please take note of the following disclaimer:

Disclaimer: Forward-looking Statements

The information in this whitepaper is purely descriptive and is not binding. Please note that 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 are subject to risks and uncertainties that could cause actual results of ZelCash development to differ materially. No information in this whitepaper has been reviewed or approved by any regulatory authority.

Furthermore, we intend to use the Zel 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 project. Therefore, do not place undue reliance, especially in any financial decision, on these forward-looking statements, which are subject change.

This whitepaper and its previous and future iterations are and will be available at zel.cash/whitepaper. The whitepaper is written in “The Queen’s English”. *Note: This paper will be frequently updated, sometimes without notice. Please confirm the version you are reading is the current one.*

1.0 Bitcoin

January 2009 marked the release of Satoshi Nakamoto's Bitcoin. As the first currency with no central backing or issuer and no physical backing, it represented a radical revolution in how financial systems would operate. Arguably much more important than the simple transaction of goods was the technology upon which it was based. Blockchain, also developed by Nakamoto, allowed the utilisation of distributed and decentralised consensus. By removing a centralised issuer or controller, the "electronic cash" would enable peer to peer transactions without the consensus or confirmation of a trusted third-party organisation.

Bitcoin was not the first electronic cash; Dei's b-money and others existed before Bitcoin. Their issue was reaching consensus. There needed to be a mechanism to counteract a nefarious actor trying to double-spend on the network. By utilising proof-of-work to verify blocks on the Bitcoin blockchain--in a similar method to Adam Back's Hashcash--consensus could be reached between nodes, allowing for the confirmation of transactions.

Blockchain has been evolving ever since. The development of various projects--most notably Ethereum--has shown new possibilities and uses for blockchain, expanding its potential.

1.5 Zcash

Zerocash(2014), which later became the Zcash project (2016), used zk-SNARKs (Zero-knowledge Succinct Non-interactive ARguments of Knowledge) to bring about truly anonymous peer-to-peer transactions. Building on Bitcoin, Zcash improved upon Zerocash with security fixes and adjustments, as well as improved functionality and performance. The same way Bitcoin became the first widely adopted electronic currency, Zcash became the first widely adopted anonymous electronic currency.

Also, Zcash started a fight against centralisation in the mining process that had been brought about by the SHA-256 ASICs that had hit the Bitcoin network; this (arguably) allowed the network to become centralised. The implementation of Equihash, a memory-hard, proof-of-work algorithm for mining, brought about a return to decentralised mining, with CPUs and GPUs. Although recently ASICs have been developed for Zcash's Equihash 200,9, other projects are keeping this decentralised

consensus mechanism alive with the development of modified Equihash and ProgPOW, as well as new concepts such as proof of useful work.

zk-SNARKs allow the execution of an operation--such as a transaction broadcast to a blockchain network, and the origin of the transaction, amount, and receiver of the transaction--to be completely hidden from public view.

Zcash’s continuing development, such as its recent Overwinter network upgrade and work towards z-transactions on mobile (lightweight) wallet, brings improvements that provide privacy in commerce in a similar way fiat hard currency does, but with the convenience of digital currency and the benefit of not being issued or controlled by a central authority.

2.0 Ethereum

Ethereum likewise expanded the possibilities of decentralised applications and its utilisation of blockchain, allowing developers access to an open platform for the development of applications, smart contracts, and much more.

From the Ethereum whitepaper:

> *What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.*

With this vision, Ethereum has been a driving force in many aspects of blockchain development and the the cryptocurrency industry. It brings the potential for a world where most--if not all--systems could benefit from blockchain technology and the features arising from it. Whether it is the tokenisation of assets or the ability to run ICO fundraises, it has empowered users to create a new internet, the likes of which could we could have barely imagined a few years ago.

Despite this, scalability issues--and concerns about how Ethereum will address them--persist. Limited to around 15-20 transactions per second, it is simply too slow to turn its vision into reality.

As we will outline in this whitepaper, Zel aims to solve the scalability problem, finally turning Ethereum's vision into reality. We have created an ecosystem of products and applications to achieve this goal, focusing on accessibility and usability.

3.0 Zel

Zel's technologies work in symbiotic relationships with each other and with technologies outside the Zel ecosystem. Zel is designed as an open system in partnership with closed source technologies. See Section 4.0 for the specific underpinnings of Zel.

4.0 Zelcash Core Functions

On its surface, Zelcash is a mineable digital currency based on the technological foundations of the cryptocurrency Zcash (previously known as Zerocash), which is based on Bitcoin. Zelcash utilises zero-knowledge proofs first coined in a digital currency by Zcash and utilised by many other privacy coin projects. This fact provides a relatively large network of developers for different teams providing improvements to the protocol over time to strengthen the core functionality of blockchain technology and zero-knowledge protocol base.

Unlike Bitcoin--whose claims of anonymity have been disproven in recent years--Zcash ensures user anonymity through the zk-SNARKs protocol (described in Section 4.2). With anonymity of end users of a transaction being a core tenet of the original Bitcoin vision, improvements and general evolution of the privacy idea should be welcomed by both privacy coin holders and users. Zel has chosen to utilise the privacy features of Zcash to enforce this anonymity vision, and to increase the adoption of such a feature set through a large, scalable network.

Zelcash offers economic incentive for our decentralised node network, ZelNodes, to offer a truly scalable, decentralised blockchain development network. This incentive is created through a portion of block rewards and, eventually through different economic models such as transaction fees or operation tariffs for DApps, to support our vision for a powerful and decentralised node network to allow separate blockchains, apps, tokens, smart contracts, and much more.

4.1 T_transactions

T_transactions are traditional Bitcoin blockchain-recorded transactions. These are done between addresses known as transparent addresses, or t-addresses derived originally from Bitcoin. These are most commonly used every day between wallets and exchanges. This is because they require less computational power to execute the transaction and can be sent from mobile devices and other portable devices.

4.2 Z_transactions

Z_transactions are shielded or private. These are sent between Z_addresses also known as shielded addresses. Zelcash inherited them from Zcash and therefore benefit from any of the technical advancements and developments the Zcash team makes on the development of Zcash and its protocols, such as network upgrades like the Overwinter fork.

If sent from one or more shielded addresses, the value of the transaction(s) is kept private. Only when there is a transparent address on the receiving end will the coins be deshielded (and the transaction no longer private). This will, as a result, reveal the value received only to that specific address on the blockchain. The original addresses or input address, along with the value sent, remains private when shielded in such a manner. The Zcash protocol describes this process in detail:

The value in Zcash is either transparent or shielded.

- Transfers of transparent value work essentially like Bitcoin and have the same privacy properties.
- Shielded value is carried by notes, which specify an amount and a paying key. The paying key is part of a payment address, which is a destination to which notes can be sent. As with Bitcoin, this is associated with a private key that can be used to spend notes sent to the address; in Zcash this is called a spending key.

Each note has a cryptographically-associated note commitment and a unique nullifier (so that there is a 1:1:1 relation between notes, note commitments, and nullifiers). Computing the nullifier requires the associated private spending key. It is infeasible to correlate the note commitment with the corresponding nullifier without knowledge of at least this spending key. An unspent valid note, at a given point on the blockchain, is one for which the note commitment has been publicly revealed on the blockchain before that point, but the nullifier has not.

A transaction can contain transparent inputs, outputs, and scripts, which all work as in Bitcoin [Bitcoin-Protocol]. It also contains a sequence of zero or more JoinSplit descriptions. Each of these describes a JoinSplit transfer which takes in a transparent value and up to two input notes, and produces a transparent value and up to two output notes.

The nullifiers of the input notes are revealed (preventing them from being spent again) and the commitments of the output, notes are revealed (allowing them to be spent in the

future). Each JoinSplit description also includes a computationally sound zk-SNARK proof, which proves that all of the following hold except with negligible probability:

- The input and output values balance (individually for each JoinSplit transfer).
- For each input note of non-zero value, some revealed note commitment exists for that note.
- The prover knew the private spending keys of the input notes.
- The nullifiers and note commitments are computed correctly.
- The private spending keys of the input notes are cryptographically linked to a signature over the whole transaction, in such a way that the transaction cannot be modified by a party who did not know these private keys.
- Each output note is generated in such a way that it is infeasible to cause its nullifier to collide with the nullifier of any other note.

Outside the zk-SNARK (shielded addresses), it is also checked that the nullifiers for the input notes had not already been revealed (i.e., they had not already been spent).

A payment address includes two public keys:

1. a paying key matching that of notes sent to the address, and
2. a transmission key for a key-private asymmetric encryption scheme.

“Key private” means that ciphertexts do not reveal information about which key they were encrypted to, except to a holder of the the corresponding private key, which in this context is called the *viewing key.* This unique key is used to communicate encrypted output notes on the blockchain to their intended recipient, who can use the viewing key to scan the blockchain for notes addressed to them and then decrypt those notes.

The basis of Zcash’s privacy properties is this: When note is spent, the spender proves only that some commitment for it had been revealed without revealing which one. This means a spent note cannot be linked to the transaction in which it was created.

From an adversarial point of view, the set of possibilities for a given note--its note traceability set--includes all previous notes, which the adversary neither controls nor knows to have been spent. This contrasts with other proposals for private payment systems, such as CoinJoin or CryptoNote that are based on mixing of a limited number of transactions and that, therefore, have smaller note traceability sets.

The nullifiers are necessary to prevent double-spending: Each note has only one valid nullifier, so attempting to spend a note twice would reveal the nullifier twice, causing the second transaction to be rejected.

4.3 Proof-of-Work

As Nakamoto improved on the work of Adam Back's Hashcash, he created a validation system that relies on cryptographic hashing rather than trust of a centralised system. Following on from Nakamoto's use of SHA-256 for Bitcoin came Litecoin's implementation of Scrypt, followed by Dash and Ethereum utilising X11 and Ethash, respectively. Recent developments (expanding on the idea of X11, which is a sequence of hashing algorithms where the output of one becomes the input of the next) came with the development of X13, X15, and X17.

BTC was intended to be mined by computer processing units (CPUs) referring to both hashing and voting with CPUs. But solvers for graphics processing units, (GPUs) were developed. As the value of Bitcoin increased and the incentive to mine became higher, it became viable for programmable hardware such as field-programmable gate arrays (FPGAs) to be utilised for mining Bitcoin. These had an advantage over both CPUs and GPUs. Following the development of FPGAs came the development of purpose-built mining hardware, Application-specific integrated circuits (ASICs) developed and soon dominated the Bitcoin network, meaning that in the same way it became unprofitable to mine on CPUs when GPU mining software was developed, the same fate for GPUs could be realised due to FPGAs.

Building on the idea of chaining many algorithms together in a sequence that was first implemented in X11, soon came X13, X15, X17. These operate similarly but with more algorithms, meaning it was harder for purpose-built machines to hash (mine) these algorithms.

Zelcash was based on Zcash for its privacy technologies and the benefits gained through them. But as many cryptocurrencies based off of Zcash inherited its POW consensus method and algorithm, it became economically viable to create ASICs for Equihash 200, 9. As many cryptocurrencies--BTCZ, BTG, SAFE and others--moved to a different set of N, K parameters, 144, 5 they began to show resilience against these ASIC manufacturers.

The Zel dev team set out to swap X16R for Equihash 200,9 to be the POW hashing algorithm for Zelcash. Development was well underway, incorporating zk-SNARK into the hash algorithm and to begin testnet, when credible rumors surfaced that FPGAs/ASICs were being developed for X16R that could be 100-1,000x more efficient at hashing than GPUs.

As we fight against ASICs, recent developments in FPGA hardware present another potential challenge. Although CPU PoW would be ideal, we understand that most of the mining community currently utilise GPUs and at the end of the day, we all have a sort of affection for GPUs. So the game then lends itself to countering ASICs and trying to preserve GPU mining.

Development on X16R algorithm for Zelcash was thus halted. The amount of work to incorporate privacy features into X16R and still not be ASIC-resistant was too high.

For these reasons, Zelcash will swap hashing algorithms to modified Equihash with N,K values of 144 and 5, the same approach as other privacy coins have performed recently. This will be a “stop-gap” to remain resistant to ASICs and FPGAs and allow some time to explore a more permanent path. Solutions are being constantly developed to keep GPU mining relevant, and thus keep a massive decentralised ecosystem of POW hash power. One such idea is progPOW, which will be researched and discussed by the Zel team in the coming weeks. In-depth description of future algorithms and strategems will be described in future iterations of this whitepaper.

As Zel aims to create a decentralised network, it only makes sense to keep the distribution of Zelcash itself which in turn allows for the creation of the ZelDev network, decentralised and as distributed as possible. We will continue to enforce our stance of being ASIC-resistant. The POW algorithm upgrade will be complete by end of July 2018.

Finally, our difficulty algorithm will be moving from the old Digishield V3 to Zawy’s LWMA. Zawy’s Linearly Weighted Moving Average (LWMA) brings a much higher consistency to block times and adjusts much faster than Digishield V3 to large hash increases. In our testing, Zawy’s LWMA is more than ten times fast at block retargeting then Digishield V3. The new difficulty algorithm will help mitigate against hash power and timestamp attacks as Zel releases more products, and likely brings more hash power to the network as the project grows. This move will also be made as part of the Zelcash network upgrade in July 2018.

4.4 Block Reward

At launch, Zelcash had a slow start of 5,000 blocks, after the Dev Fund was mined, and then from block 5,000 onward the block reward has been 150 Zelcash that goes 100% to PoW miners. As the development of ZelNodes approaches we will be modifying this

to accommodate the incentive for node ownership and, as such, a shift in rewards will be seen. This is to be guided by the team and decided by the community over the course of the next few weeks leading from this paper's release.

The intent of the adjusted block reward systems will be to ensure value to both the PoW-based mining community as well as the ZelNode ownership. This scale will be sliding, and thus adjusted as needed to ensure a proper reward model for all.

The block reward will be halved every 2.5 years, starting from date of the genesis block.

4.5 ZelNodes

The concept of ZelNodes emerged from a discussion of how to potentially scale a decentralised application, development and smart contract platform and network, such as Ethereum. Projects such as Lisk, Neo, and others have been able to do so. However, they face the risk of moving away from decentralisation, instead only offering the benefits of blockchain technology in a somewhat accessible way.

Ethereum is decentralised, so it faces issues of scaling as all decentralised networks seem to do. With DApps such as Crypto Kitties bringing Ethereum's network to its knees, the result is expensive transactions that are slow and increase the cost to interact with smart contracts that operate on its network.

This is not only an issue of cost; it could cause hiccups in DAOs and many other apps that operate on the network, making it unacceptable in the connected world in which we live. By creating an incentivised network, in a similar vein to DASH, Zelcash allows us to create a truly decentralised and distributed network of nodes. This would allow a scalable network, similar to Ethereum, with much higher transactional throughput. Utilising ZelChains (sidechains) allowing more transactions per second.

This is necessary if we are to move to a decentralised internet. Ethereum cannot currently scale to meet these demands. Uber provides a real-world example: With 12 rides a second, the network would saturate, meaning a competitor such as Lyft would not be able to operate on the same network. Although Vitalik Buterin's vision was for potentially 1 million transactions per second (TPS), currently it is 15-20. With concepts such as sharding under development, however, it is possible that Ethereum will be able to reach such numbers.

We are not inclined to throw out a random number without hard evidence, but theoretically--based on a working proof-of-concept--the Zel network will be able to reach a higher TPS than Ethereum in less time. With the scalability brought about by ZelNodes, we could theoretically match the VISA network's TPS. Note that this estimation of over 1000 TPS is just that, an estimation. We like to prove our tech before offering numbers that are subject to change, but we consider it a conservative estimate.

We will not speculate on true TPS until Mainnet is launched and well-vetted for many months so we can deliver a realistic number that is not hyperbolic or untested.

4.6 ZelNode Economics

Incentivised nodes used to secure a coin's network and process transactions have been around since the founding of DASH, an electronic currency. Since then, many projects have added the platform of Masternodes (MNs) as a vehicle to incentivise coin holders, lock up coin supply, and invigorate active trading and mining. Some projects have have been successful in their integration of MNs, while some newer micro-cap currencies have used the allure of MNs and massive, unrealistic returns to gain quick community growth and capital raises, which can lead to exit scams, market dilution, realised ROI drop, etc. To create a robust and decentralised development network of MNs, named ZelNodes for this project, collateralisation and rewards shall be designed to be realistic and considered a long-term investment.

ZelNodes will be a three-tiered node structure, requiring three different levels of collateralisation and system hardware specifications, and yielding three levels of rewards. ZelNode rewards will be distributed to the node holders from a chunk of each mined block in a ratio of 25% to ZelNodes, 75% to PoW miners, and is a sliding scale for future growth and incentivisation, meaning the ratio can be adjusted slightly as needed to maintain a large decentralised network of compute power (see section 4.5 for use case). A ZelNode will also require high availability, thus very stable uptime is necessary to receive the node reward; the required uptime percentage will be published closer to the release of ZelNodes.

Proposed ZelNode system hardware requirements:

Spec. Type	Zelnode Basic	ZelNode Super	ZelNode BAMF
CPU	2 vCores	4 vCores	8 vCores
RAM	4GB	8GB	32GB
Storage (SSD)	50GB	150GB	600GB
Bandwidth	2.5TB	4TB	6TB

For now, the three ZelNode tiers are named ZelNode Basic (lowest collateral required), ZelNode Super, and ZelNode BAMF (highest collateral required). Each ZelNode level has VPS system requirements, which translates to a more costly VPS service level. All ZelNodes will have an up-time requirement also, so time and system specification requirements will be tested by Zel to ensure conformity to the rules and that reward distribution is rightly deserved.

Proposed collateralisation and reward structure:

Tier Level	Collateral [Zel]	Reward % (of 25% of each block)
ZelNode Basic	10,000	15%
ZelNode Super	25,000	25%
ZelNode BAMF	100,000	60%

The wide range of collateral size enables a large number of people to participate in the ZelNode system if they so desire, and the non-linear scaling collateral/reward is required so that, for example, 10 Basic nodes cannot earn more than 1 BAMF node. The economic model was developed with an **estimated coin price for Zel of $1** USD by the end of 2018. Being a long-term investment, the cost associated with running a ZelNode is relatively inconsequential and is assumed to be speculative in nature, akin to speculative GPU mining, where instant profit is not the investor's sole requirement.

With the ability to slightly change the block reward ratio up or down, the Zel team has some ability to maintain a certain number of nodes on the network by increasing reward if the total number of nodes falls below a threshold, or decreasing rewards for the

reverse situation. This feature will be used exceedingly sparsely and is considered a “last-ditch” effort to maintain ZelNode adoption on the Zel network.

5.0 Dual Economies

Zelcash is the mechanism of transaction for the Zeldev platform. Onboarding processes, fees and services will be directly linked to Zeldev infrastructure and require Zel coin; however, we are researching possible long-term developments around a “dual economic model.” As the decentralised exchange and DApps are developed, the vision of a service-based economy, as well as a currency based structure will need to be developed.

Understanding the need for a robust network of miners, nodes and developers will solidify Zelcash and the Zeldev platform. As the development of the decentralised exchange (DEX) and DApps takes to the forefront, the need to fund and maintain developers is essential. Understanding that this is something to consider, a Foundation establishment is key to engage the community around the long-term funding models.

6.0 Zel Technologies

Zel Technologies works on a variety of projects and applications in addition to Zelcash. These all cohabit and interact in symbiotic relationships within the Zel ecosystem.

The project was founded on the idea of creating a decentralised blockchain network consisting of an Ethereum-like chain, with higher transactional throughput thanks to its consensus being found between ZelNode operators. Running off of the main Ethereum-like blockchain, the ZelDev chain will be ZelChains. ZelChains will operate like side chains in a Lisk-type environment allowing these blockchains to communicate with each other if they so require, but also being able to handle higher transactional throughput and benefit from running on the truly decentralised network.

This positions Zel to

- solve the scalability issues facing Ethereum and similar projects; and
- allow decentralised applications, smart contracts, decentralised oracles, voting systems, etc. to be developed in a scalable manner.

With this push, (started by Satoshi Nakamoto), we are moving away from the centralised internet we all knew just a few years ago (and still use today) to a decentralised internet and world.

Other projects such as ZelTreZ, ZelPay, Zel ID, and others allow us to create this ecosystem to develop technologies for the future.

6.1 ZelTreZ

ZelTreZ is a platform that emerged from the team's desire for a better wallet platform than was currently offered in the open-source space. Zel set about developing a lightweight and full-node wallet that just included Zelcash. It was designed to give users the option to choose which capabilities they needed. Through the beginning of this development, we began to realise the potential for the platform and as such the idea developed and flourished into what it is today. ZelTreZ is now a multi-asset wallet that offers both lightweight and full-node options for users.

Designed for ease-of-use with a fresh and lightweight UI, ZelTreZ is developing into a gateway for the cryptocurrency world. Currently supporting ZEL, BTC, LTC, ZEC, ETH, BTCZ, RVN, BNB, and HUSH, with new projects being listed every two weeks along

with updates and security improvements. ZelTreZ uses encryption to keep users safe; it allows us to create accounts without storing any user information remotely. As the development of Zel continues, the implementation of ZelDev will showcase our decentralised development network through ZelTreZ in the form of ZelDex, our decentralised exchange that will be offered natively within the ZelTreZ platform.

Along with being a storefront for DApps, it is also a portal for developers and students to learn about blockchain development and begin to utilise the ZelDev platform to develop their own DApps and blockchain applications. Currently available on Windows, Linux, and MacOS, ZelTreZ will be ported to a web app, Chrome plugin, Android, and iOS, allowing cross-device accounts and logins without storing any user information on our infrastructure.

6.2 Zel ID

Zel ID is an authentication system designed to enable users to maintain full control over their digital identities. It potentially allows users to keep property, health records, and other information on a decentralised, encrypted network rather than on paper or in centralised servers; this will give the user control over their information and privacy that is lacking in our current digital world.

Zel ID is powered by the same security concepts brought forward by Authparty, a Bitcoin/Counterparty-based authentication system developed by Zel team member Matthew Reichardt. Zel ID achieves zero-proof authentication by utilising signatures generated from your wallet's public and private keys. This virtually negates the need for 2FA, since authentication requires custodial access to your wallet. Your wallet, in this case, ZelTreZ, would be as essential as a cell phone or internet connection.

Unique authentication identities, called *Personas*, are then generated and utilised for zero-proof authentication with third-party providers and services.

The Zel Registry provides API access to the Zel ID authentication protocol. Via a generated Persona, a new identity called *Entity* is then generated and tethered to the Persona. This way, a third-party service authenticating via Zel ID would have three degrees of separation from your actual wallet identity, allowing for different Personas while still providing the potential for anonymity.

6.3 ZelPay

A simple but essential software, ZelPay could be used in point-of-sale terminals in stores as well as website plugins. ZelPay is being designed to give users ease of use and transparency, and to offer businesses either feeless or 1% fees on transactions.

The benefit of ZelPay is a unified application that offers ease of use both in-store and online, and it gives business owners access to high levels of analytics and sales details to help them develop and grow their business. ZelPay will be designed to allow businesses to accept not only all of the cryptocurrencies in ZelTreZ, but also fiat currencies potentially, in a tokenised asset chain that is one to one backed by, USD, GBP, EUR, YEN, or gold and other assets. This would allow freer and easier commerce with higher TPS capabilities than offered by other cryptocurrency solutions.

ZelPay will offer NFC (near-field communications) and QR-code options to facilitate contactless payment via the ZelTreZ mobile app along with e-commerce payments using a similar method, allowing a seamless and quick experience for both customer and merchant.

A hypothetical implementation for ZelPay and other blockchain applications:

We have already seen the adoption of self-service kiosks in grocery shops, eliminating the need for multiple human clerks. Instead, only one is need to ensure the machines work correctly and ID is verified for those purchasing alcohol. To take this idea further, staffless shopping experiences are being tested by Amazon and other companies, and these systems have already seen implementation in some cities.

This is achieved through a process that sounds complex but is, in fact, as natural and easy as using a smartphone. The shopper scans a QR code to enter the shop; this is their cart. When the shopper enters, they pick out the items they want and place them down at the “checkout” table. The table reads the RFID stickers that are on the items, generates another QR code or allows NFC payment, and the shopper is allowed to leave with their goods. This system could be improved, but it provides an excellent example of how technology can improve customer experiences and reduce costs for businesses.

6.4 ZelDev

ZelDev will be designed around developers to make working with blockchain as easily accessible as possible. We will achieve this by giving developers access to the ZelSDK and BDK, which will allow easy adoption of blockchain into their new or existing projects. There will be some template ZelChains to help developers get started and will allow developers to interact with them using Javascript. Also, smart contract templates along with token templates will be available also allowing for smart contracts to be written in Javascript. This lowers the barrier to entry for developers, as Javascript is the most widely used programming language. To deal with the transactions of tokens, they will be offloaded onto separate blockchains that will, when needed, communicate with the main ZelDev chain. This also allows higher transactional throughput and, for example, could reduce the impact when a particular chain is under maintenance.

Technical details regarding the ZelDev platform and products directly related to it will be shared at a later release date.

6.5 ZelChains

The main ZelDev chain along with ZelChains (sidechains) are blockchains that will operate on the ZelNode Network. This will allow true decentralisation in a scalable manner as compute resources are guaranteed to be available up to the total number of ZelNodes collateralised on the Zelcash network. This allows the ability to open up other resource pathways if one or more ZelChains become saturated, and will drastically increase the possible total transactions per second that Zel can process.

6.6 ZelDex

Currently, the largest exchanges for cryptocurrencies are centralised. In most cases the user does not own their private keys to the wallets of the exchange and as such does not own the cryptocurrency that is in their “exchange account.”

Although centralised exchanges currently offer much better experiences as well as more transactions per second, decentralised exchange are improving. With new ones offering users control over their private keys, we are at the start of a revolution in the

exchange market. The main issue that is stunting adoption of decentralised exchanges is the issue of scalability due in part to their infrastructure.

ZelDex will be built on top of the ZelDev Network as a showcase of its capabilities. The interface will be designed to be simple to navigate yet complex enough for advanced users. With integration directly into ZelTreZ, as well as being a standalone platform on web and mobile, ZelDex aims to be the first Dex with mass adoption in the space.

Also, open API calls will allow developers to utilise ZelDex in their applications for the exchange of tokens and currencies.

6.7 Dapp Store

The ZelDapp store will be a central hub for decentralised and some centralised applications, with a lower barrier to entry, with some rules and regulations to ensure legality. The app store is designed to allow developers access to a large user base on a cross-platform solution. ZelTreZ operates as a sandbox for these Dapps to operate inside of, allowing faster access and development time without having to wait for approval from certain companies.

ZelDapps differs from other blockchain offerings by its inherently low learning curve. The framework will be accessible via the SDK, which will likely be Javascript language, and possibly other languages as the platform is developed. Utilising an extremely popular programming language ensures easy access to development tools and accessibility to a wide range of both professional and hobbyist programmers.

At Zel Technologies, we believe people should be able to communicate freely and without restrictions. To that end, a messenger will be created as the first DApp. It may then be followed by a social media platform that allows people to express their opinions without censorship (within the law).

There will be little-to-no fee on the ZelDApp store. It will be designed to be a free and open market to enable developers to reach users.

7.0 Leadership and Contributions to Whitepaper

Founder- Miles Manley
Partner and Developer- Lumi Ibishi
Partner and Lead Developer- Tadeas Kmenta
Lead Advisor- Daniel Keller
Project Manager and Advisor- Parker Honeyman

Respect to: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
For the day it was created, Bitcoin forever changed financial freedom for those that choose a different path. Technology is the great leveler, to all those creating the future, we salute you!

-Zel Team

8.0 Future for Zel

Zel will be an ongoing, developing ecosystem. The team is dedicated to the world-changing benefits of blockchain and cryptocurrency. To that end, Zel will proactively engage with new and emerging tech, projects, and leadership development. We believe the space will need leaders to usher in new technology, and we would like to be at the forefront.

Moving forward, the Zel team will

- continue to develop new technologies based on the Zelcash model in both open and closed source projects.
- partner with others in the space to ensure the project is at the forefront of the crypto space.
- develop and foster a community around the Zel platform that will guide the values and deliverables of the business model.
- Develop and foster a charitable arm of Zel Foundation for the betterment of others though emerging technology.

9.0 Glossary

Altcoin--A cryptocurrency that's not Bitcoin.

ASIC (application-specific integrated circuit)--Silicon chips specifically designed to do a single task (hashing for crypto). In the case of Bitcoin, they are designed to process SHA-256 hashing problems to mine new Bitcoin.

Cross-chain technology--Allows two blockchains to exchange information and crypto assets at the same time.

DASH--A type of cryptocurrency based on Bitcoin software that offers anonymity features; previously known as XCoin (XCO) and Darkcoin.

Fiat money--Currencies with minimal or no intrinsic value but defined as legal tender by the government, such as paper bills and coins.

JoinSplit--data included in a transaction that describes a *JoinSplit* transfer, i.e. a shielded value transfer. This kind of value transfer is the primary Zcash-specific operation performed by transactions.

Litecoin (LTC)--Cryptocurrency created by former Google employee Charlie Lee in 2011. It allows for faster processing at lower cost.

NEO--Refers to the cryptocurrency *and* the name of a China's first open source blockchain. Like Ethereum, it can execute smart contracts or DApps, but in a somewhat centralised environment.

Overwinter fork--The first ever hard fork of Zcash addressing network and performance upgrades among other items, to strengthen the protocol for future network upgrades.

Multi Signature (multisig)--Multisig addresses allow multiple parties to require more than one key to authorise a transaction. Multisig addresses have greater resistance to theft.

Private Key--A private key is a string of data that gives a user control to a public key and address to allow transactions of cryptocurrency.

Proof of Stake (PoS)--An algorithm that rewards participants who solve difficult cryptographic puzzles to achieve distributed consensus. PoS has lower energy consumption than PoW.

Proof of Work (PoW)--An algorithm that rewards the first person or group of people [pool] who solve a computational problem to achieve distributed consensus.

Z-cash--One of the first privacy-oriented cryptocurrencies

Zel ID--An authentication system that creates an online Persona for the user, to be used in all aspects of life for any system of rules that requires verification and validation of a real-world identity.

ZelChains--The side chains that will run on the Zelcash network to provide usable compute power and scalability to decentralised application developers.

ZelDev-- The platform for decentralised application developers to interact with the Zelcash blockchain and ZelChains through easy-to-use SDK and BDK environments.

ZelDex--A decentralised exchange created by Zelcash to run on the decentralised network and to be provided through ZelTreZ and a standalone web portal, ZelDex will also be technology showcase for ZelDev.

ZelNodes--A multi-tiered, incentivised network of compute power for use by Dapp developers and token propagation that is robust, scalable, and truly decentralised.

ZelTreZ--The frontend platform for Zelcash, ZelTreZ is a multi-asset encrypted wallet, and will house the Dex, manage the ZelNode wallets, and contain the Dapp Store.

zk-SNARK--A privacy protocol pioneered in cryptocurrency by Zcash that allows for shielded transactions that ensure anonymity of the end users. (See Zcash whitepaper for technical explanation)

Resources

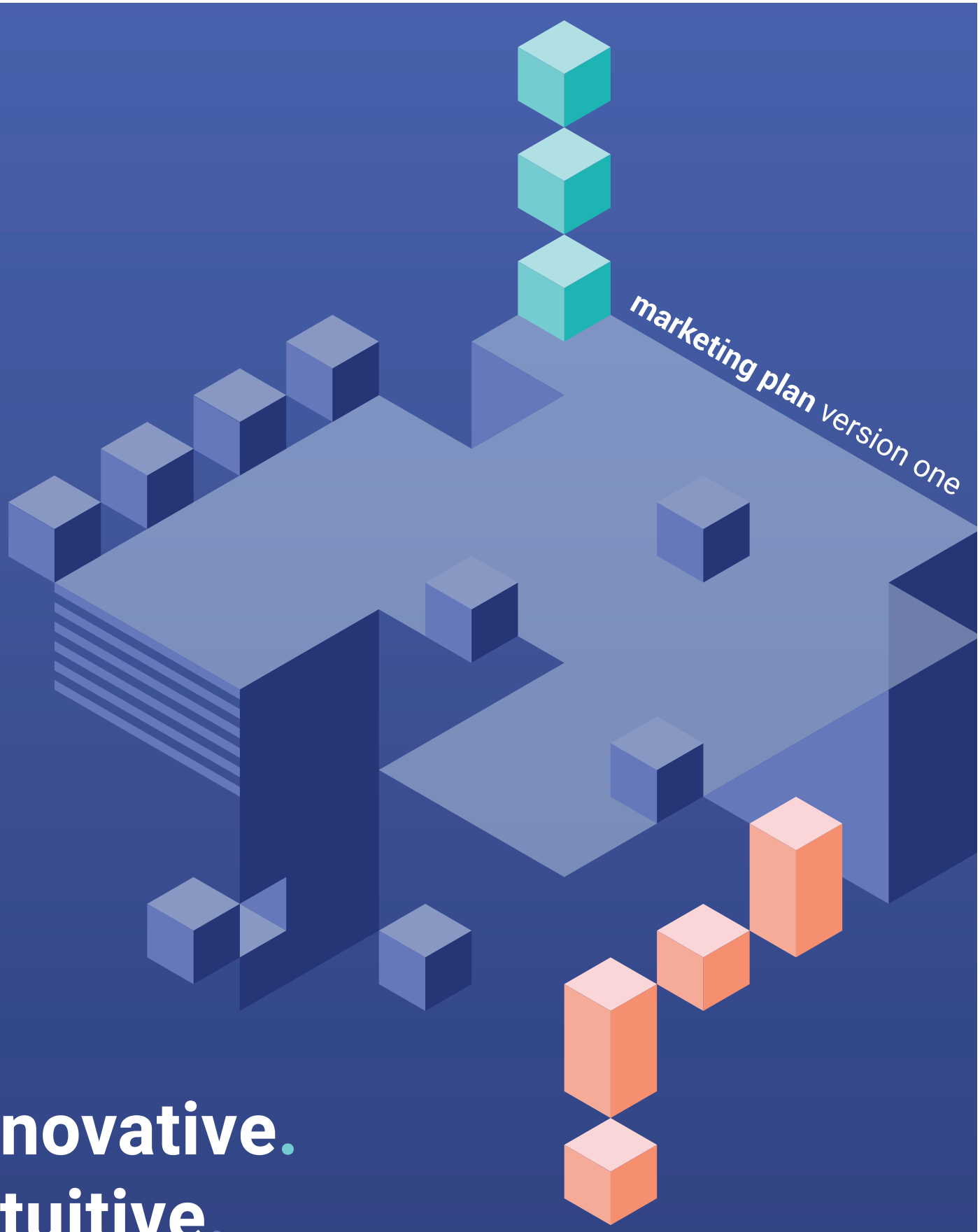
[1] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system

[2] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Zcash Protocol Specification Version 2017.0-beta-2.5.

[3] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. (2014) Zerocash: decentralised Anonymous Payments from Bitcoin

[4] Vitalik Buterin and the Ethereum Project: A Next-Generation Smart Contract and decentralised Application Platform, Ethereum

[5] Tron Black and Joel Weight: X16R ASIC Resistant Design



Innovative.
Intuitive.
Intelligent.

zelcash | zeltrez

ZelTrez Marketing Overview 1.1

Prepared: Daniel Keller

06-29-2018

Prepared for: ZelTrez

Section 1: The Scope of Marketing Plan

I. Initial team briefing and discovery phone call with ZelTrez management team
II. Coordination and planning with Teams (Breakout Teams)

Social Media and PR:

III. Obtain or create Social Media/Reddit/bitcointalk accounts
IV. Creation and publication of press releases, and articles in Bitcoin Talk and possible mainstream media communities
V. Cultivating and engaging users directly to draw interest through community/Social management
VI. Content Calendar creation and execution
VII. Create Marketing plan and strategy with the ZelTrez team
VIII. Website Audit for content improvement

High Level:

IX. Coordination with the legal team for proper guidelines and structure
X. External collaborate on strategy surrounding the coin and blockchain integration
XI. Outline coin model and rules for using it
XII. Collaborate on documentation to audit a Whitepaper
XIII. Collaborate with the ZelTrez team on creating a Prospectus document (Initial Coin Offering Memorandum) using documentation above
XIV. Collaborate on pitch Deck

XV. Introductions to exchanges for listing and possible involvement in the Coin offering, such as the Binance token and USDT.

Design

XVI. Create and redesign bitcointalk announcement and Reddit thread
XVII. Design professional infographic images for content and structure of ZelTrez Prospectus (Done, include in the prospectus)
XVIII. Branding consultation (Outside Hires)
XIX. Website Design Consultation

Development

XX. Coin creation (Rules, Governance, structure)
XXI. Crowdfunding contract
    A. Security Testing
XXII. Design and Develop ICO page
    A. Security testing and debugging

Section 2:

Analysis

1. Need to position ZelTrez in target markets
2. Improve branding and marketing messaging
3. Establish an active presence in targeted online communities
4. Communicate the advantages of ZelTrez across all mediums
5. Help polish website content, social and community channels
6. Educate community and audience about ZelTrez to increase interest and awareness
7. Engage Bitcoin/Ether holders, traditional investors, alternative investors
8. Build digital coin, crowdfunding contract, & ICO page
9. Help drive demand for Coin Offering

Goals:

1. Target audience and attract new users
2. Create momentum in the media:
    a. We will draft and publish press releases and articles to the Bitcoin/Crypto/ (Possible) Mainstream media
3. Cultivate a user community who will evangelize ZelTrez and its products (community management)
4. Increase brand recognition
5. Increase awareness of the platform
6. Ongoing Integration with cryptocurrency exchanges

Development Timeline
Examples of previous work:

1. **https://info.zel.cash/**

Marking Team will need to understand the process for the development of this unique project:

1. Scoping and Coin Strategy Discussion
2. Requirements Assessment
3. Agree on deliverables and timelines
4. Coin structure draft (Roadmap review)
5. Bi-Weekly community update call
6. Deliver initial tasks according to milestone 1
7. Revisit or revise timelines/deliverables if needs shift
8. Continue development and deliverables according to the timeline

Marketing Timeline:

Month 1: Building the Foundation
Research and Development of Marketing and Messaging

- Consultation with internal teams to extract value proposition(s)
- Review branding, story, messaging, and website copy for crypto audiences
- Review social and community channels
    - Help with Zelcash and ZelTrez thread content (BitcoinTalk/Reddit)
    - Publish these items accordingly
- Review documents/whitepaper/marketing information about Zelcash and ZelTrez to collaborate on a draft of Prospectus
- Finalize Blueprint
    - Draft and develop content and final reversioner marketing plan
    - Sign off on a marketing plan and content calendar with internal teams

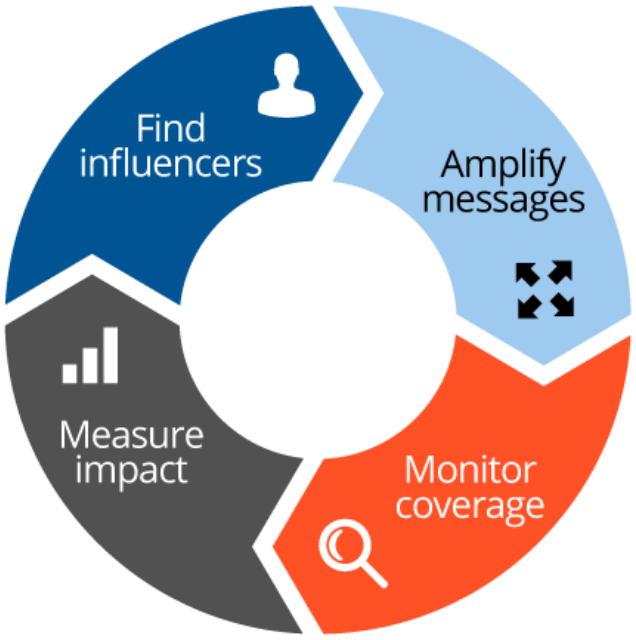
Putting up the frame
Building on Marketing/PR

- Building momentum with releasing initial announcements across all mediums
- Press to Cryptocurrency media and building possible interest in Mainstream Media
- Create buzz and awareness and educate the community and audiences of ZelTrez and the Zelcash platform
- Disseminate information about Zelcash and ZelTrez on Bitcoin/social media/community channels
    - Posting of and distributing content
    - Help with thread posts' replies
- Facilitate introductions and interviews with Bitcoin media

- Educational articles to Bitcoin/Blockchain/Mainstream media and community
- Create copy for Prospectus draft
- Create use case stories and communicate these across channels to generate business development

Ongoing: Continuous delivery and execution Marketing/PR/Begin

- Discuss with ZelTrez team governance and distribution rules for the Coin
    - Review and develop a coin outline with the development team and internal team
    - Release Bounty program to the community
    - Develop and collaborate on the design and current component ZeltreZ and Zelcash website
- Continue engaging interest in online discussions/community management
- Continued educational press leading to excitement pieces about the progress of ZelTrez, Zelcash, Zelnodes, and dEX
- Review progress and optimize for improvement



Section 3: Team Assigned to Project

Management:

- Daniel Keller – Lead Advisor and Marketing Leader
- Parker Honeyman – Advisor and Project Lead
- Miles Manley - Business Development

Marketing:

- TBD- Communications
- TBD- Community
- TBD- Social/Communications

Development:

- Tadeas Kmenta – Lead Coin and Platform Developer
- Lumi Ibishi – Advisor- Lead Graphics