KRIPTAN
TOKEN DESIGN

1 November 2018

KRIPTAN

The White Paper Pack contains 3 Companion Documents . For a comprehensive understanding of our vision for the Kriptan Identity Network and how it will become a new privacy preserving Global Identity Network, the reader is advised to read all documents.

WHITE PAPER

LEGAL DISCLAIMER

Please read the following notice carefully before proceeding to read this White Paper document issued by Sedicii Innovations Limited, a company incorporated and existing under the laws of Ireland (hereinafter – the "Company"). This notice applies to all persons who read this document. Please note this notice may be altered or updated.

The White Paper does not constitute any relations between you (hereinafter – "you" or "Holder") and the Company. Acquiring of Kriptan Tokens is available only after accepting the Terms of Token Sale (hereinafter – "T's&C's").

Acquisition of Kriptan Tokens does not present an exchange of cryptocurrencies for any form of ordinary shares of the Company and a Holder of Kriptan tokens is not entitled to any guaranteed form of dividend, Holders of Kriptan Tokens are only entitled to certain rights within the T's&C's . Kriptan Tokens are not intended to constitute securities in any jurisdiction. This White Paper does not constitute a prospectus or offer document of any sort, and is not intended to constitute an offer of securities or a solicitation for investments in securities in any jurisdiction.

This White Paper is for information purposes only. The contents of this White Paper are not a financial promotion. Therefore, none of the contents of this White Paper serve as an invitation or inducement to engage in any sort of investment activity.

Prospective acquirers of Kriptan Tokens should carefully consider and evaluate all risks and uncertainties associated with the cryptocurrencies, Sedicii Innovations Limited and their respective businesses and operations, the Kriptan Tokens and the Kriptan Token offering. Familiarise yourself with all the information set out in this White Paper, Risk Notice and the T's&C's prior to any purchase of Kriptan Tokens. Ensure that you are aware of all of the would be risks prior to obtaining Kriptan. The Risk Statement details all potential risks that you should consider. We recommend that you seek out independent financial advice before engaging in any sort of business endeavour.

RISK STATEMENT

No regulatory authority has examined or approved any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements, or rules have been complied with. To the maximum extent permitted by the applicable laws, regulations and rules, Sedicii Innovations Limited and its affiliates and their respective officers, employees or agents, in relation to the Company's and the Kriptan website and Kriptan Tokens, will not be liable for any damages of any kind, including, but not limited to, direct,

consequential, incidental, special or indirect damages (including but not limited to lost profits, loss of revenue or third party loss whether foreseeable or otherwise, trading losses or damages that result from the use of or the loss of use of the Company's or the Kriptan website and Kriptan Tokens).

For the avoidance of doubt, the Company expressly disclaims any and all responsibility for any direct or consequential loss or damage of any kind whatsoever arising directly or indirectly from: (i) reliance on any information contained in this document, (ii) any error, omission or inaccuracy in any such information, (iii) any action resulting therefrom, or (iv) usage or acquisition ofproducts, available through the website.

You acknowledge and agree that you are not purchasing Kriptan Tokens for purposes of investment, speculation, as some type of arbitrage strategy, for immediate resale or other financial purposes.

Some of the statements in the White Paper include forward-looking statements which reflect the Company's current views with respect to an execution roadmap, financial performance, business strategy and future plans, both with respect to the Company and the sectors and industries in which the Company operates. Statements which include the words "expects", "plans", "believes", "projects", "anticipates", "will", "aims", "may", "would", "could", "continue" and similar statements are of a future or forward-looking nature. All forward-looking statements address matters that involve risks and uncertainties. Accordingly, there are or will be important factors that could cause the Company's actual results to differ materially from those indicated in these statements. These factors include but are not limited to those described in the part of the T's&C's entitled "Risks", which should be read in conjunction with the other cautionary statements that are included in the T's&C's. Any forward-looking statements in the White Paper reflect the Company's current views with respect to future events and are subject to these and other risks, uncertainties and assumptions relating to the Company's operations, results of operations and growth strategy. These forward-looking statements speak only as of the date of the White Paper.

Prospective buyers of the Kriptan Tokens should specifically consider the factors identified in the White Paper and T's&C's which could cause actual results to differ before making a purchase decision. No statement in the White Paper is intended as a profit forecast and no statement in the White Paper should be interpreted to mean that the earnings of the Company for the current or future years would be as may be implied in this White Paper.

Introduction

At its core, the Kriptan Network is a global identity verification network. It enables real-time identity verification by trusted identity providers (governments, banks, telcos, utilities), ensuring that businesses can react quickly to new information. At the same time, it is designed to provide the highest possible levels of privacy. Data is never exchanged or copied. Instead it is always verified using an advanced form of cryptography, known as zero knowledge proofs (ZKPs). We believe that the digital asset economy requires a new foundation for public trust and that only public blockchains can engender that trust. Our ground-breaking privacy technology underpins this new trust model, by guaranteeing that no personally identifiable information or private business data is ever recorded on the blockchain. However, it is also clear that **total anonymity is not the way forward**. We accept that there are legitimate reasons to allow financial regulators, tax officials and law enforcement agencies to audit the financial ecosystem and that they should have the power to investigate wrongdoing where there is reasonable cause for suspicion. When this is the case, our platform provides regulators with the capabilities they need to investigate asset transfers with appropriate judicial oversight.

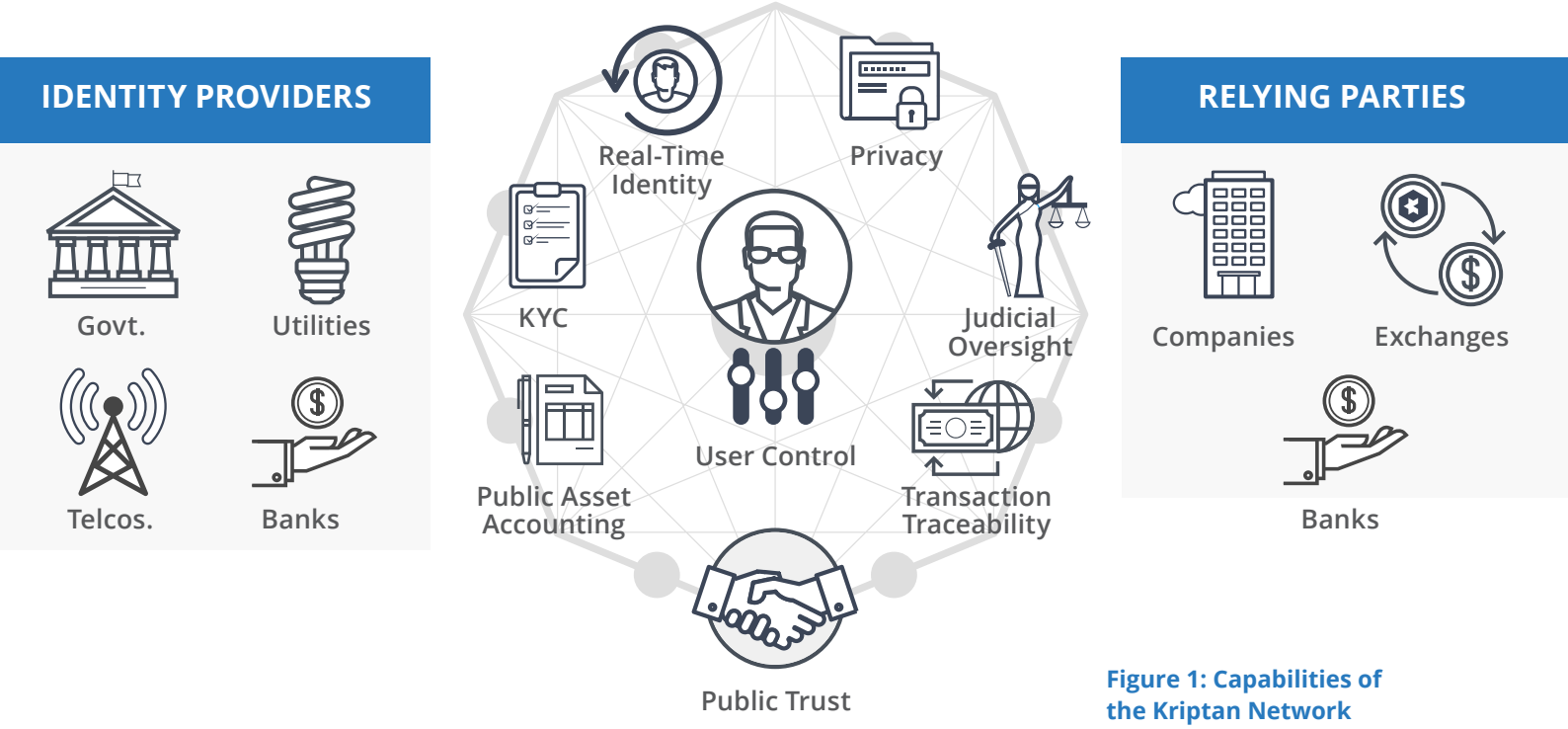


Figure 1: Capabilities of the Kriptan Network

Kriptan is also **more than an identity verification network.** The combined capabilities shown in Figure 1 work together to build one compelling feature that truly sets it apart: **it allows any business or government to create their own fully-regulated digital asset.** Without these foundational identity capabilities regulated digital assets wouldn't be possible, as the principle of Know Your Customer (KYC) is a core requirement of all regulated financial services. We build on the core identity / KYC capabilities to enable **on-chain privacy with off-chain auditability.**

The Kriptan Network provides **a shared infrastructure for businesses, governments and individuals.** It therefore requires a very specific business model to ensure its long term viability. This paper will explain how this business model will work. It is, after all, an enormous challenge to build a global identity network. The hardest part of that challenge is at the start, when there are few users and a small number of relying parties (who need to verify identity-related data) and identity providers (who can verify that data). The challenge is to find ways to reward those who embrace the risks involved in being the earliest to join. This document explains more about the mechanisms built into the Kriptan token to incentivise this shift, by rewarding early adopters for their belief in this new privacy paradigm. We will introduce the concept of a **two-sided network token**, and show how value flows and is captured in this personal information economy.

Within the Kriptan Network, the same mechanism we use to ensure the on-chain privacy of all Kriptan token transactions can also be used by any third-party digital asset. We ensure that Kriptan tokens are fully regulated in any jurisdiction and the same approach can also be applied to any digital asset. What is common across all new digital assets is that they will require robust identity capabilities, advanced privacy capabilities, tools for regulatory oversight and public trust. Today, only the Kriptan Network can provide all of these. This document describes how the Kriptan token is designed to capture the value generated by the future exponential growth of these regulated, digital asset transactions.

Bootstrapping the Kriptan Network

Does the Kriptan Network really need a token to work? This is a very important question. It may appear at first glimpse that the answer is that no token is required. In theory, the network could work without it, where Relying Parties (RP) pay Identity Providers (IdP) for services directly. Another way of asking this question is, can we scale a global identity network without a token? The answer is "maybe". Multi-sided networks like Uber, Airbnb and Alibaba have succeeded without a token, through a combination of luck, strategic astuteness, growth hacks and diligence. But more often than not, new multi-sided networks fail to reach a critical mass of users.

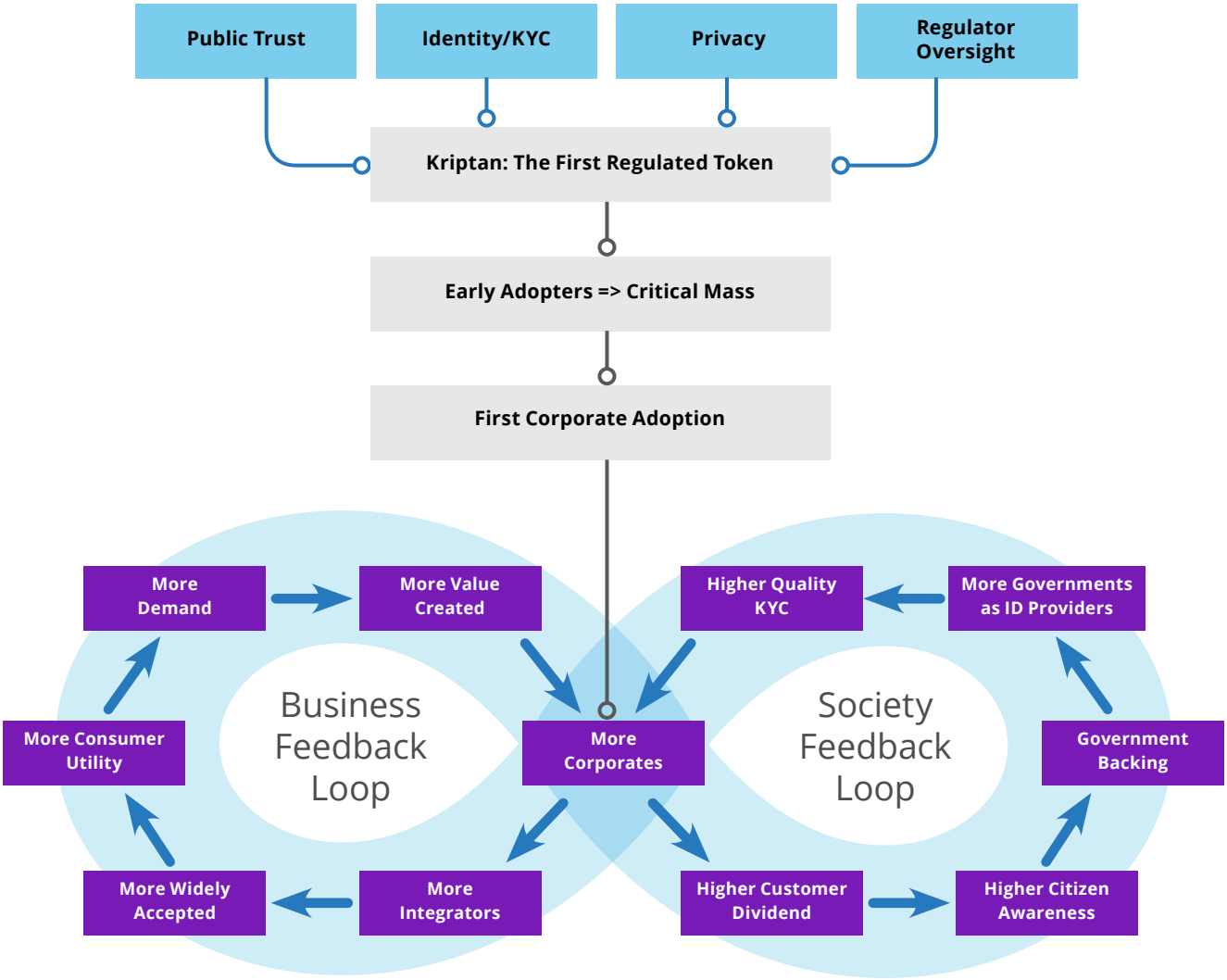


Figure 2: The Virtuous Cycles of Kriptan Growth

When you add tokens to multi-sided networks interesting things can happen. Multi-sided networks, also known as platforms, match demand with supply. This matching of supply and demand is called liquidity. Like liquidity on a trading platform, it is the likelihood that there is a buyer ready to purchase the goods you are selling, at the very point in time you want to sell them. In the identity case, it is the probability that the Kriptan Network has a verified identity for the user that an RP wants to trade with. Or it's an IdP who has a critical mass of Relying Parties willing to pay for the strong identities they can provide. This liquidity must be there in every jurisdiction, in every market sector and for every identity attribute. So for example, if I'm a Relying Party who needs to check credit risk, then I need an IdP that can vouch for the person I want to trade with. In this case, having the government as the IdP may not be what is needed: they can confirm passport or driving licence details, but would not provide insights into my probability of financial default. So maybe I need a specific credit score attribute that only four vendors in the market can provide. The goal of the Kriptan Network is to get all of these vendors to partake in the network. The token therefore creates two virtuous cycles that drive adoption of the network.

Figure 2 depicts how these two cycles can reinforce each other. The cycles behave as follows:

- Through a strategic partnership fund we will invest in any project that can contribute to the goals of the Kriptan Network. We have set aside 30% of the tokens to fund such projects.
- Once a company becomes a strategic partner, they have a vested interest in the success of the network, so they will encourage other businesses in their network to join.
- We will ensure that every user who creates an identity on the network will receive Kriptan tokens every time their identity is verified. These tokens will be locked up for up to three years so that users have a vested interest in the long-term success of the network.
- Once users have a vested interest in the network, we hope they will evangelise the network to other users. Every user is also a citizen, so we hope to encourage citizens to lobby their governments to join the network too, to act as Identity Providers. Citizens whose governments have joined the network will have a higher level of assurance on the Kriptan Network and will therefore receive a higher reward in Kriptans for each verification.
- As we hit a critical mass of verified identities, we now provide the foundational enablers for regulated digital assets, where corporates or governments can launch their own token-based incentives.
- This closes off the social loop, where more accurate KYC and government support leads to more corporations joining the network.
- The second loop is fed by a growing ecosystem. As more businesses adopt token-based business models there will be more service providers, better tooling and more experienced developers.
- This will lead to wider adoption of tokens by the affiliate networks that grow around these token economies.
- This in turn leads to the final steps of the left loop: customers get more utility from the network, they tell their friends about all the great value they are getting, this creates more demand for tokens, which increases the value of each economy.
- As other corporates see more and more success stories, where innovative business models are driving greater returns, new corporations will want to create their own tokens.

We believe these two powerful feedback loops will drive enormous business value. We also believe that it wouldn't be possible to bootstrap this network without using a token. The token also serves to demonstrate the power of token-based incentive mechanisms when building platform economies. This is the key lesson we would like every major business to take on board i.e. the Kriptan Network should be a showcase of what is possible with tokens. In the next section we provide more details about how the token will work.

The Kriptan Token

Background

Many utility tokens have a design flaw that stems from their use as a medium of exchange. As Bitcoin was the first viable crypto-asset, many of the crypto-assets that followed tried to mimic the currency aspects of its design by requiring users to pay for services using the token. Given the highly volatile nature of digital asset valuations, this creates some major headaches for users, who now need to deal with exchange rate risk. For businesses, it also creates further issues related to tax, accounting, asset custody, authorisations etc. However, there is a bigger risk that is harder to see: velocity.

The Equation of Exchange[1] was stated by John Stuart Mill in 1848 as:

$$MV=PQ$$

In a token-based economy, M is the size of asset base, P is the price of the resource being provisioned (in our case, this resource is verified identity attributes) and Q is the quantity of the resource. The key variable is V, the velocity, representing how often the asset changes hands per time period. The faster tokens circulate in the economy, the lower M needs to be for the same economic output, and so the price of the asset will fall. See also Buterin[2] and Burniske[3].

Digital assets are very easy to move around. As the infrastructure for trading tokens continues to improve, costs are reduced and so there is very little friction when exchanging tokens. In this case, many users will not hold tokens and instead will buy them when they need them. Similarly, someone who sells goods in return for tokens may have no reason to hold the tokens either, in which case they will sell the tokens as soon as they receive them. This results in a very high velocity, and so a low token price. In extreme cases the price could be close to zero.

For the Kriptan token, we have designed a new mechanism that is a hybrid of two existing approaches: discount tokens and work tokens. This approach works to ensure that velocity stays as low as possible, thus ensuring that the tokens are useful as a store of value.

Discount Tokens

Originally conceived by the Sweetbridge[4] project team, a discount token[5] is a digital asset which allows the holder to get a discount on some service, where the discount they receive is proportional to the number of tokens they hold. In this way each token acts like a perpetual voucher, providing access to a service at a discount. The maximum discount that is provided is set by the network. The percentage discount per token varies with network usage, according to a set formula. In this way, as the network grows, the discount available per token will increase, so that early adopters will find they have a surplus of tokens which they can sell on the open market. There is no incentive to hold these extra tokens as, above a fixed limit, they will provide no economic benefits (i.e. no further discounts). They also have the property of being more valuable to users than to speculators, as users get the market value plus the discount value (which is not available to speculators).

The combination of these two properties should mean two things:

(a) over time, speculators will sell their tokens to users

(b) over time, users with surplus tokens will sell their extra tokens to other users. As this levelling out of token allocation proceeds, we should get close to a state where every user should receive the maximum discount allowed.

See [5] for more information on discount tokens, including an in-depth description of the mathematical formulas involved.

Non-Staking Work Tokens

A work token[6] is a digital asset which is required by any person who wants to run a validator node on a decentralised network. These validator nodes (also known as keeper[7] nodes) validate network transactions and get a fee for providing this service to end users. Often, these validator nodes must stake tokens in return for being allowed to collect fees for validation services. The tokens they own are locked in a smart contract.

In the Kriptan Network these validator nodes are called Zero Knowledge Proof Verification Engines or ZVEs for short. ZVEs will activate tokens. These activated tokens act as a right to validate transactions and the validator can therefore collect fees. Unlike staked tokens, there is no concept of “slashing”, where tokens are forfeited if an invalid transaction is authorised. ZVEs can only sustain value by providing reliable verifications i.e. they fail or succeed based on their reputations. Additionally, if ZVEs were found to be verifying fake identities and invalid transactions they would instead be removed from the Kriptan Network. Kriptan Tokens therefore act as non-staking work tokens. The amount of tokens that an ZVE holds will serve as a limit on the amount of fees they can take in. Private companies who run ZVE nodes will want to maximise the revenue they can make from validating transactions. They will buy Kriptan Tokens when it makes economic sense to do so i.e. when they can buy tokens at a price that allows them to increase their profitability.

The Two-Sided Network Token

A Kriptan Token is useful for two groups. The token provides a right to discounted network access for Relying Parties (RPs). The *same* token also acts more like a network "licence" for ZVEs, where the licence fee is proportional to the revenue a ZVE can earn by providing services on the network. We have two competing groups that we are incentivising to hold tokens, each holding them for different reasons. The intention is to design the system so that both groups can achieve their goals. This design could work for any two-sided network, where one side of the network sells a service and the other side pays for access to the service, with a broker in the middle to handle the transaction. For that reason we've called it a Two-Sided Network Token, in the hope that this design will have wide applicability.

The token design goal is to get the system to an equilibrium, or "steady state", where all RPs will have activated tokens up to the maximum discount they can achieve and all ZVEs will have deployed the maximum tokens allowed for them to obtain the maximum revenue possible. We want to do this in such a way that at this steady state, no party needs to compete for tokens. In other words, we should reach a stable price for tokens where there is no room for speculators or no rewards for market manipulation.

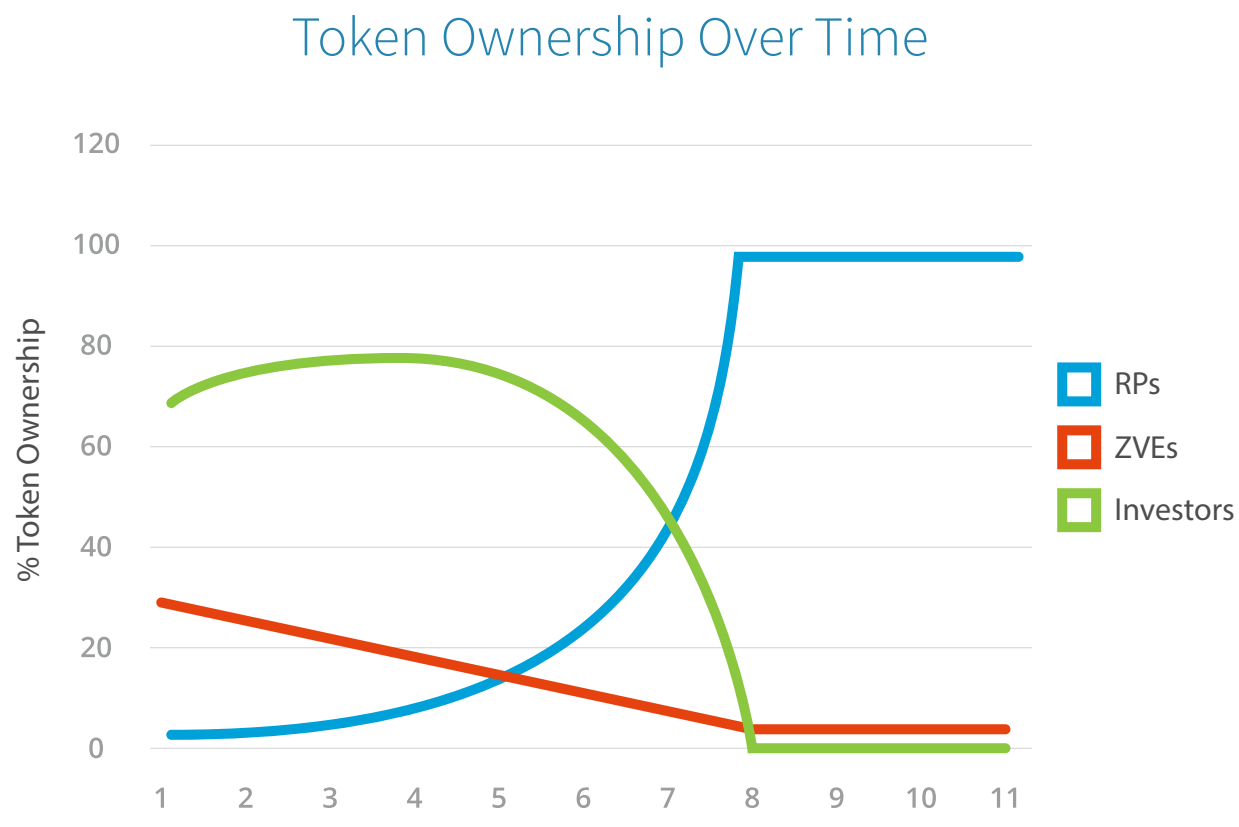


Figure 3: How We Would Like Token Holding To Evolve Over Time
(NB: this highly speculative – just for illustrative purposes)

Figure 3 shows how we would like token ownership to evolve over time. The units of time in Figure 3 are not specified, as we don't want this to be construed as a projection – it's purely for illustrative purposes. Initially tokens are granted to the Kriptan Foundation and to Sedicii, their advisors and early investors. Kriptan Tokens will also be granted to IdPs to encourage them to become early adopters. Users will earn tokens for participating in the network. IdPs and users are "investors" in the sense that their tokens will appreciate in value as the network grows. Our hope is that they will *invest* time in evangelising the network to others. The key message is that over time all tokens should be owned by the ZVEs and RPs and that all other participants would no longer retain tokens.

To achieve this, we need to solve three problems:

- We want to find a point at which token ownership is balanced between RPs and ZVEs, a ratio of token ownership where, if no new parties join the system, neither side has any reason to buy or sell tokens.
- We want this balancing point to be stable, so that if token ownership moves away from this balancing point, incentives are there for participants to buy / sell tokens to move it back into balance
- We should anticipate that network growth will cause more demand for tokens, and so we should pre-emptively adjust the token activation limits (see below) to ensure tokens become available for new entrants to the market to buy and activate.

This design can be considered to be an anti-Ponzi mechanism. By actively ensuring that latecomers can join the network at a fair token price, we can ensure the network can last in perpetuity. At the same time, in the early stages of network growth, there will be opportunities for early adopters to gain from the success of the network. The discount rights and network licence rights token-buyers acquire in the early stages, will exceed their needs as the network grows. This is because, as we shall see below, the token activation limits will automatically adjust with network growth, so the number of tokens they need to hold will fall over time, allowing them to sell the surplus tokens on the open market.

Finding The Balancing Point: T_{max}

We have a network with I Relying Parties (RP) who have activated t_r tokens, along with m ZVEs who have each activated t_i tokens. The combined number of transactions on the network per period is n, and each transaction completed at price, p_j. The total number of tokens in circulation is fixed, and is represented by t_c. β represents the discount token parameter, where the maximum combined discounts available to RP token holders is given by $\frac{1}{\beta}$ (so a β of 2 provides participants with a 50% discount).

A key part of the token design is that it uses state feedback. X represents the state of the network, including the number of RPs and ZVEs on the network, the number of tokens activated by each party, the number of transactions and the value of those transactions. This allows us to build a token design that is responsive to changes in the network state. In 2.1 (below) we show that G is a function of X. In other cases, we do not make this explicit. For example, t_{max}, which represents the maximum number of tokens that all ZVEs combined can activate, is also a function of the state, X.

The aim here is to determine an appropriate formula to calculate t_{max}, based on the requirement that new ZVEs will only join the network if their "fee" for using the network allows them to run a profitable service. So we must find a future steady state of the network where the number of tokens a ZVE must hold are in line with this "fee". We use the term *fee* in quotes as the ZVE will buy and hold tokens not pay a fee, but the cost to them can be modelled as an annual fee (as per below). We also assume that RPs will hold all the remaining tokens, so we need to ensure that the tokens they hold provide the economic returns that they will require.

The GDP of this economy is given by the following formula:

$$G(X) = \frac{\sum_{i=1}^{m} t_i}{t_{max}} \sum_{i-1}^{n} p_i - \frac{1}{\beta} \frac{\sum_{r=1}^{l} t_r}{(t_c - t_{max})} \frac{t_{max}}{\sum_{i=1}^{m} t_i} \sum_{j=1}^{n} p_j \quad \textbf{(2.1)}$$

The two components of G break down as follows:

- The left component represents the total GDP of the network if RPs held zero tokens. As ZVEs activate tokens, this will increase until the term: $\sum_{i=1}^{m} t_i \to t_{max}$, so $\frac{\sum_{i=1}^{m} t_i}{t_{max}} \to 1$, and so $G(t, p; X) \to \sum_{j-1}^{n} p_i$
- The right component represents the total discounts available to RPs as they activate their tokens. RPs can activate tokens up to $(t_c - t_{max}), so \frac{\sum_{r=1}^{l} t_r}{(t_c - t_{max})} \to 1$ as all RP tokens are activated. RPs get further discounts when ZVEs haven't activated tokens up to the limit allowed. When all IdP tokens are activated $\frac{t_{max}}{\sum_{i=1}^{m} t_i} \to 1$.
- When all RP and ZVE tokens are activated up to the maximum allowed then this term goes to $\frac{1}{\beta} \sum_{j=1}^{n} p_j$

At steady state, all RPs will have activated tokens up to the maximum discount they can achieve. ZVEs will also have deployed the maximum tokens allowed for every ZVE to obtain the maximum revenue possible. We want a value of t_{max} so that, at steady state, the following should be true:

$$t_{max} = t_c - \sum_{r=1}^{l} t_r = \sum_{i=1}^{m} t_i \quad (2.2)$$

There will, of course, be competitors to the Kriptan Network. IdPs and RPs will get to choose which identity verification network they use. This competition between networks will ensure that IdPs will only join, if the fee to use the network is a small percentage (say, in the order of 1%-4%) of the revenue they can generate using the network. This fee is represented by γ, which is the percentage of total network GDP that all combined IdPs will pay per time period, when the network is at steady state. It is also equates to the total revenue generated by ZVEs. As ZVEs will buy tokens that provide them with a right to use the network in perpetuity, we can model this a perpetuity[9]. To buy this perpetuity, all the ZVEs together would have to buy t_{max} tokens, at price, $c_{zve.}$ The net present value (NPV) of this is given by:

$$NPV = \frac{\gamma.G(X)}{r} = t_{max} * c_{zve} \quad (2.3)$$

where r is the discount rate (not to be confused with β which determines the discounts that RPs get). A discount rate of 8% implies that the owner of this perpetuity is in a position to invest their funds elsewhere for a return of 8% per period. Instead we are asking them to buy tokens. We would expect ZVEs to buy tokens if the price per token was:

$$c_{zve} = \frac{\gamma.G(X)}{r.t_{max}} \quad (2.4)$$

At the same time, the tokens provide a savings per year to the RPs. The savings they can expect to receive are the right side of 2.1 divided by r (to give the NPV of the perpetuity) and by t_c - t_{max} to give the NPV per token:

$$c_{rp} = \frac{1}{r\beta(t_c - t_{max})} \frac{\sum_{r=1}^{l} t_r}{(t_c - t_{max})} \frac{t_{max}}{\sum_{i=1}^{m} t_i} \sum_{j=1}^{n} p_j \quad (2.5)$$

At steady state, we want the token price to be the same for RPs and ZVEs. If we set $c_{zve} = c_{rp}$ and solve for t_{max} we can then determine what token ownership looks like when we have a stable network. We can then work back from there to determine how we can encourage the network to evolve to this stable endpoint. Putting 2.4 equal to 2.5 we end up with:

$$\frac{\gamma.G(X)}{r.t_{max}} = \frac{1}{r\beta(t_c - t_{max})} \frac{\sum_{r=1}^{l} t_r}{(t_c - t_{max})} \frac{t_{max}}{\sum_{i=1}^{m} t_i} \sum_{j=1}^{n} p_j \quad (2.6)$$

From 2.1 we get to:

$$\frac{\gamma}{r.t_{max}} \frac{\sum_{j=1}^{m} t_i}{t_{max}} \sum_{j=1}^{n} p_j - \frac{\gamma}{r.t_{max}} \frac{1}{\beta} \frac{\sum_{r=1}^{l} t_r}{(t_c - t_{max})} \frac{t_{max}}{\sum_{i=1}^{m} t_i} \sum_{j=1}^{n} p_j = \frac{1}{r\beta(t_c - t_{max})} \frac{\sum_{r=1}^{l} t_r}{(t_c - t_{max})} \frac{t_{max}}{\sum_{i=1}^{m} t_i} \sum_{j=1}^{n} p_j \quad (2.7)$$

Before we attempt to solve for t_{max} we can look to simplify this by noting that the intention is for all of the ZVEs to activate the tokens up to t_{max} in which case:

$$\sum_{i=1}^{m} t_i \rightarrow t_{max} \quad (2.8)$$

Similarly, if ZVEs are using t_{max} tokens, then RPs can activate tokens up to t_c - t_{max} so:

$$\sum_{r=1}^{l} t_r \rightarrow t_c - t_{max} \quad (2.9)$$

From 2.8 and 2.9 and after cancelling out the r and $\sum_{j=1}^{n} p_j$ terms:

$$\frac{\gamma}{t_{max}} - \frac{\gamma}{t_{max}} \frac{1}{\beta} = \frac{1}{\beta(t_c - t_{max})} \quad (2.10)$$

Solving for t_{max} we get:

$$t_{max} = \frac{(\gamma\beta - \gamma)}{(1 + \gamma\beta - \gamma)} t_c \quad (2.11)$$

In other words, if we want IdPs to pay a 2% fee per annum (γ = 0.02) to use the network (a fee which goes to the ZVEs), and we want RPs to get 50% discount (β = 2) on the services they can access, in a network with 20 billion tokens, we should expect ZVEs to activate a maximum of 392.16 million tokens, with RPs activating the remaining 19.608 billion tokens. If instead, the same 20 billion token network wants to charge IdPs a 4% fee (γ = 0.04), with a 10% discount (β = 10) for RPs, then ZVEs would need to activate 5.294 billion tokens.

Activation Limits

The activation limit for RPs is:

$$a_{max} = \beta \frac{\sum_{r=1}^{l} t_r}{l} \qquad (2.12)$$

Every RP can activate tokens, t_r, up to a_{max}. A problem arises when $\sum_{r=1}^{l} t_r > t_c - t_{max}$. In this case when an RP activates new tokens, the smart contract will automatically adjust a_{max} to get a new a_{max} which includes the latest activation of tokens. It does so by reducing all activations by $\frac{t_c - t_{max}}{\sum_{r=1}^{l} t_r}$.

We can then activate tokens for the RP up to the newly calculated limit. Note that all other RP activations (and hence the discounts they receive) have been dynamically reduced as the network state, X, changes.

It's important to note that when an RP activates a_{max} tokens they get free access to the network (not a discount of $\frac{1}{\beta}$. However, we can see that as more RPs join the network, while the limit will decrease, there will be more RPs competing for tokens, so that the total discount for all participants tends to $\frac{1}{\beta}$ as all RP tokens are activated.

The activation formula for ZVEs is:

$$b_{max} = \frac{\sum_{i=1}^{m} t_i}{m} \qquad (2.13)$$

As per the RP case, when a ZVE tries to activate tokens such that $\sum_{i=1}^{m} t_i > t_{max}$ a new limit is calculated by reducing the activated tokens for ZVEs until $\sum_{i=1}^{m} t_i \leq t_{max}$.

As the token activation limits adjust dynamically, we can be assured that as the network grows, new participants can activate tokens as they acquire them. The goal is to ensure that network access remains affordable. Even though we expect the price per token to increase as the network grows, we have also made sure that the number of tokens required to achieve RP discounts (or generate revenue for ZVEs) falls over time. By ensuring that only activated tokens are counted, we avoid incentivising ZVEs or RPs to hoard tokens for the purpose of manipulating the activation limits.

We do, however, accept that an investor who holds tokens for the long term, as they are expecting network growth, will cause an increase demand for tokens. We also accept that IdPs may want to hold tokens in the early stages of network growth, to capture the gains in token value from this growth. This will reduce the supply of tokens, increasing the price and may even make discounts prohibitively expensive for RPs (where the NPV of the tokens is greater than the discounts they could deliver). However, RPs will also be able to anticipate network growth, so they may also want to acquire tokens (above fair value based on discounts) if they believe that the network will continue to grow. Overall, we believe that this competition for tokens will be healthy for the ecosystem as a whole. IdPs will have higher costs in the early stages of the network (as they train staff, integrate systems etc.), so these incentives help to justify the extra expenditure. Overall we feel this design is fair and will be highly robust when confronted with attempts at market manipulation.

A Note On Inflation

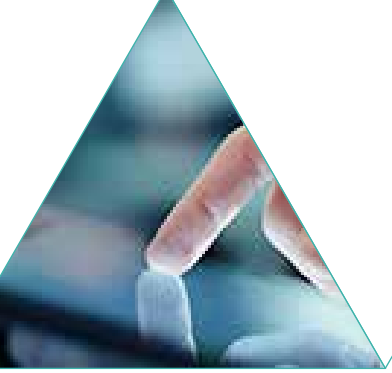
We believe that a fixed token issuance is appropriate for the Kriptan Network. The reason for this is aligned with the Two-Sided Network token design we have chosen. We aim to simplify the analysis required by Kriptan Network users by removing any uncertainty that inflation would cause.

When inflation is fixed there is a risk that the wrong value will be chosen as the inflation rate. When inflation is variable, the inflation level can be set by governance rules, which creates its own uncertainty, or it can be calculated by an algorithm, introducing additional complexity that potentially makes it harder for users to build a model to determine fair value.

When the inflation rate is set to zero, the decision for a Relying Party is greatly simplified: the rational thing to do is to buy tokens when their market price is below their fair value price to them, which is easy to calculate (as per above). Similarly, in the case of ZVEs, the rational node owner can project the future profits they can earn. Where the market price of the tokens is below their calculation of NPV based on their projections, they should buy tokens. The lack of inflation makes both of these calculations easier.

There is one argument (see Wenger[10]) that the lack of inflation can cause over-exuberance in the market. We believe that by clearly articulating the risks involved in growing a global identity network and by open and transparent communications, we can ensure that market participants will factor in the appropriate discount rate when calculating the NPV of the tokens.

As the growth rate of the network stabilises, the mechanism we have designed should keep the token value within a relatively small range.

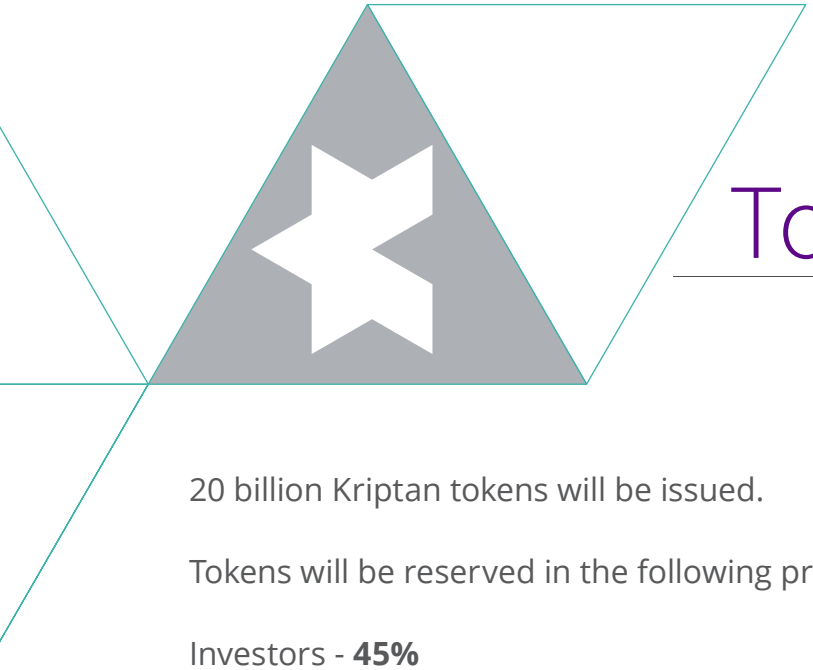


The Token Smart Contract Interface

The Kriptan Network is designed to facilitate the high assurance identity needs found in the highly regulated environments of governments, large enterprises and NGOs. However, we also want the Kriptan token to be accessible to everyone, as we want everyone to partake in this new privacy-centric approach. We are keen to make it available for anyone to purchase from any crypto-asset exchange. We want the token to be supported by all major wallets. However, we also have to ensure that the wallets and exchanges that support it adhere to the high regulatory bar that we wish to set.

So why are we going to such great lengths to make Kriptan a regulatory-friendly digital asset? The answer is that we want Kriptan tokens to be a showcase for what comes next. Once we have proven Kriptan as a high assurance ecosystem, the next step is to use the network for the creation of digital assets that conform with laws around data protection, privacy, KYC and anti-money laundering. Therefore, we are very keen to set the highest of standards for the token.

Third-party wallets and exchanges will need to make the modifications required to support the token. The token itself will not be transferable unless the owner has a verified identity on the Kriptan Network, so we will work with wallets and exchanges to ensure they make this clear to their users and that the user experience is aligned with the goals of transparency and regulatory compliance. As we will see in the next section, 30% of the token allocation is set aside for Strategic Partners. Part of this allocation will be shared with wallets and exchanges who adopt the Kriptan token and for other digital assets that are powered by the network.



Token Structure

20 billion Kriptan tokens will be issued.

Tokens will be reserved in the following proportions:

Investors - **45%**
Sedicii & Advisors - **15%**
Strategic Partners - **30%** (early adopters, customers, promoters, early liquidity)
Kriptan Foundation - **10%**

We are currently in discussions with institutional investors with regard to a private sale, with a potential public sale to follow later in 2018.

Further details are available on request at **contact@kriptan.org**.

Team

Executive Team

The executive team comprises expertise in identity, KYC, and cryptography.

Rob Leslie

is Founder and CEO. Rob has been the primary driver of the company and has successfully gained recognition for Sedicii at a significant number of technology and innovation competitions. Rob has a successful track record of establishing and growing businesses to considerable scale and was part of the original management team in Dell Japan that established and grew the business to almost 300 employees and $300M turnover in 4 years. He is a co-founder of Kyckr (ASX:KYK) which is listed on the Australian Stock Exchange in September 2016 and provides organisational identity services for KYC & AML services to banks and other regulated financial institutions. Rob is a World Economic Forum Technology Pioneer and has been invited to speak at Davos on Cybersecurity, Identity and other technology issues affecting the world's economies. He holds a B.Eng. degree in Electronic Engineering from Dublin City University.

Patrick Curry OBE CEng

is Director of Innovation & Strategy. He is a strategic information management expert with a strong background in military contingency operations, command & control, crisis decision making, secure collaboration in supply chains and business continuity. He has worked in a range of senior information-centric operational management roles across UK government, international aerospace and defence sectors. He specialises in the use and management of information to support operations in trusted environments within and between collaborating organisations in US, NATO, Europe and Asia. He is also CEO of the British Business Federation Authority (BBFA – www.bbfa.info) which enables the implementation of federated identity & access management and secure collaboration across industry and is expanding into cyber resilience, Internet governance, sharing of sensitive cybersecurity and counter-fraud information, involving EU, NATO, law enforcement (including Interpol) government and industry organisations from over 35 nations. He wrote the Information Sharing Framework for the military Multinational Experiment 7, which tested cyber crisis management including air traffic management, energy and telecoms. He has a leading role in blockchain and DLT development in the UK. He is also an ISO editor for international standards on identity management, privacy and blockchains. Patrick is a chartered engineer and holds UK government security clearances.

Miguel DeVega Rodrigo

is Chief Technology Officer (CTO). Miguel holds a Ph. D. in machine learning and cryptography from the Université Libre de Bruxelles and a Masters in Engineering from the Madrid Polytechnic University. He is passionate about data science, deep learning, big data analytics, machine learning, lean management and agile methodologies. He has authored 27 patents, published in international journals, lived in 5 countries and worked at both big (Siemens, Nokia) and small companies. He is a serial entrepreneur having previously co-founded 4 startups including Dialective, Wumoo and I-Flike-U. He has worked on digital assistants (chatbots), with special emphasis on conversational user experience and optimisation. He is currently working on cryptographic processes used for authentication and identity verification.

Clare Nelson, CISSP, CIPP/E

is VP Business Development and Product Strategy, North America. She was formerly Founder and CEO of ClearMark Consulting. She was VP Business Development for mobile security leader Mi3, as well as TeaLeaf Technology (acquired by IBM). She has held executive positions at Dell, Novell and EMC as well as startups where she wrote encrypted TCP/IP variants for a government agency. She is a subject matter expert, with extensive publications and speaking engagements on Multi-Factor Authentication, (MFA), Biometric Recognition and Privacy. She lives at the nexus of cybersecurity, privacy and identity. She is a co-founder of C1ph3r_Qu33ns, a cybersecurity mentoring organisation. She holds a B.S. in Mathematics from Tufts University.

Advisors

Our advisors represent global experts in business, financial services and technology investment.

Benny Higgins

is a former Chief Executive of Tesco Bank and Group Strategy Director for Tesco PLC. He was formerly also a member of the Tesco Executive Committee. He is now Executive Chairman of ASX listed Kyckr (ASX:KYK)

Benny has extensive experience within the financial services industry. During a career which started in 1983 at Standard Life, he has held senior positions within the worlds of investment management, retail and business banking.

From being a Member of the Group Executive at Standard Life, Benny moved to RBS (in 1997) as Chief Executive of Retail Banking. He was with RBS until 2005. During this time he led the successful integration of NatWest Retail Banking - the largest single merger in UK banking for some time.

Before joining Tesco Bank, Benny served as Chief Executive Officer of the Retail Business of HBOS plc.

He achieved a First Class Honours degree in Mathematics from the University of Glasgow. He qualified as a Fellow of the Faculty of Actuaries in 1986. He is also a Fellow of the Chartered Institute of Bankers in Scotland and a member of the of the Treasury Task force on Financial Inclusion and the Scottish Government's Financial Services Advisory Board (FiSAB).

As a member of the Commonwealth Games Legacy Board, Benny maintains close ties to his home town. He is also a Director of Scottish Financial Enterprise and a Prince's Trust Ambassador.

Nigel Aston

is Consultant and Chief Strategy Officer at Blok-Tech, where he is engaged in broad range of consulting on strategic and competitive intelligence issues with particular focus on security and blockchain. This includes innovation with blockchain architecture to provide a more secure access and distribution to information. The information can include vehicle information plus telemetry that makes it especially suitable for environments with high security requirements and mutually physically unknown actors. Nigel has a strong background in dealing with international institutions in the private and public sectors. He has held a range of executive leadership positions at Amadeus including Senior Advisor Corporate Strategy for developing longer term strategic initiatives. As a UK civil servant, he held positions ranging from manager of a Government Employment centre, to member of a Cabinet Minister´s office, to regional employment policy and culminating with responsibility for policy on incoming tourism to the UK. Nigel represented the UK at the Council of Ministers, with the European Commission and with the OECD and the UN World Tourism Organisation. Nigel has a degree in politics from the University of Hull and a diploma in management from the Henley Business School of the University of Reading.

Albert Wong, AM
B Com, F FINSIA, MSDIA, FAICD

Company Director and Consultant

Mr. Wong has over 35 years of experience in the stockbroking and investment banking industry. He commenced his career with investment bank, Merrill Lynch in 1981 based in Sydney, with secondments to New York and Chicago. In 1988, he was admitted as a Member to the Australian Securities Exchange and was in partnership with Andrew Forrest (Founder of Fortescue Metals Group) at Intersuisse Securities between the years of 1988 until 1990, following which he became the principal, prior to selling out in 1995 to the current owner Phillip Capital of Singapore. Following this, Mr. Wong established the Barton Capital group of companies including Barton Capital Holdings Limited and eStar Online Trading Limited (both listed on the ASX in 1997 and 2000 respectively). Mr. Wong was the business partner to the late former NSW Premier, The Hon. Neville Wran AC QC between 2004 – 2012 and was responsible for the successful listing of numerous companies on ASX over the years. He has served on many listed boards, including Founding Chairman (now Non-Executive Director) of ASX listed Kyckr Limited.

He has been a senior adviser to the Nanshan Group in relation to its activities in Australia and was pivotal in its acquisition of its 20% stake in Virgin Australia from Air New Zealand in June 2016. Mr. Wong is a Fellow of the Australian Institute of Company Directors and Fellow of FINSIA.

Andy Honess
JumpXL

Founder and Owner

Andy is a seed investor and advisor to the software industry.

In his 30 year career, he has held UK and international senior sales and Managing Director positions in the enterprise software space, including IBM and Siebel Systems and helped take QLIK from start-up to a NASDAQ IPO for $749m in 2010.

He specialises in guiding tech start-ups to high-speed growth and is a mentor and Entrepreneur-in-Residence for over ten incubation and accelerator programs across the UK. He reviews and mentors over 200 companies a year.

He has built the Business Alignment Management™ methodology designed specifically for start-up and scale-up businesses, with value selling principles at its core.

He holds an honours degree in Business Information Systems.

Stuart Hillston

serves as Chief Executive Officer of Constellation Capital. Stuart is a hands-on technology investor and a specialist advisor to early stage entrepreneurs primarily in the software,medtech, digital and mobile sectors. He is a mentor to a number of start-up accelerator initiatives, including Wayra, and has experience of both managing and rapidly building start-up companies. He serves as Member of Advisory Board at Ensygnia Ltd. and has been an advisor to Sedicii since its incorporation.

Sven Donhuysen

Sven's background is in business and technology, which led him to build up several international companies in the global telecommunication, mobile and internet sector. Sven has held various leadership and management positions in the course of his career. His role as a business angel lets him build the bridge between entrepreneurs and investors, thereby laying a particular focus upon ideas promoting disruptive technologies. Always seeking the unusual while thinking about how the world can be made a better place, Sven is definitely a business activist par excellence. His positive attitude combined with his own experience and confidence that individuals emerge even stronger from crises make him the ideal supporter and promoter for international start-ups.

Sven is Chairman of Leo Investment AG and has over fifteen years' experience in various managing positions worldwide. He built up and managed several companies as CEO and managing several successful fund-raisings (last one 20 Million USD) He provides large experience in finance, reporting, governance and leverage of financial assets.

Brendan Dillon

Brendan is a digital asset strategy consultant. He is a highly experienced entrepreneur, start-up advisor and strategy consultant. Since 2016, he has worked as an independent blockchain consultant, providing research, advisory, crypto-economic design and strategy consulting services to corporations, start-ups and investment funds. He produced one of the world's first frameworks for digital asset analysis and the first deep-dive analyst report on a digital asset. He was the founder and CTO of AdaptiveMobile, the leading network security firm in the telecoms space, growing the company to over 150 staff. Brendan has a B. Eng. in Electronic Engineering from Dublin City University.

References

[1] Equation of Exchange, John Stuart Mill: https://en.wikipedia.org/wiki/Equation_of_exchange

2] On Medium-of-Exchange Token Valuations, Vitalik Buterin: https://vitalik.ca/general/2017/10/17/moe.html

[3] Cryptoasset Valuations, Chris Burniske: https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7

[4] Sweetbridge: https://sweetbridge.com/

[5] Zargham, Bulkin and Nelson; Raising Social Capital - Tokenizing a Customer-Driven Business: https://images.sweetbridge.org/main/WP-Sweetbridge-Discount-Tokens.pdf

[6] Nick Tomaino, On Token Value: https://thecontrol.co/on-token-value-e61b10b6175e

[7] Ryan Zurrer, Keepers—Workers that Maintain Blockchain Networks: https://medium.com/@rzurrer/keepers-workers-that-maintain-blockchain-networks-a40182615b66

[8] Two-Sided Networks, Wikipedia: https://en.wikipedia.org/wiki/Two-sided_market

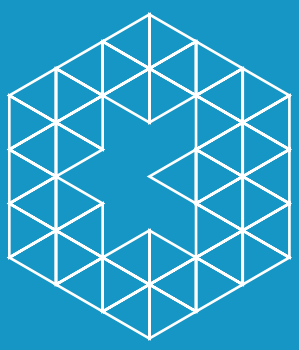
[9] Perpetuity Formula: http://financeformulas.net/Perpetuity.html

[10] Albert Wenger, Monetary Policy for Crypto Tokens: https://continuations.com/post/161700099130/monetary-policy-for-crypto-tokens

[11] ERC20 Token Standard: https://en.wikipedia.org/wiki/ERC20

[12] Ethereum: https://www.ethereum.org/

[13] The Kriptan Network: Technical White Paper



KRIPTAN