Zercados Token White Paper

Simple Economics and Info

- **Zercados Token is a Binance Smart Chain contract.**
- **A fixed amount of tokens are issued, 1 000 000 000 tokens.**
- **No new tokens are minted**
- **No tokens are burnt.**
- **Maximum of 500 000 000 tokens to be sold on pre-sale and ICO**
- **Target price during pre-sale and ICO is USD 0.001 / token**
- **Market cap on launch is 1 000 000 USD**
- **Of the remaining tokens 400 000 000 are reserved for developer rewards.**
- **Remaining 100 000 000 tokens are reserved for marketing and issueing costs.**
- **Management and shareholders are not awarded any tokens.**
- **40% of Zero Avocados Ltd's pre-tax profit is used to buy back tokens on open market exchanges yearly.**

References and more info

Zero Avocado Ltd (UK): www.zeroavocado.com

Avoozer KV Smart Phone: www.avoozer.com

AvoVPN Ecosystem: www.avovpn.com

Zercados Token Website: www.zercados.com

Continue reading for more in depth information.

The History

When Edward Snowden leaked the ‘going ons’ of the NSA to the public it raised the attention not only of the public but also the attention of politicians and larger cooperation’s. NSA’s tracking and spying on people was so extensive it was far beyond what many had ever guessed it was, but it was nothing new. It had been going on for years and it still is. The Snowden leak was just an alarm bell for ordinary people as it had now come out in the media in a much larger scale worldwide.

Snowdens information also directed the view towards big tech companies. How did they treat our personal data and what was the reason for them collecting all this? Does anyone really need to know your exact position every 10 min for countless years back? How does knowing what you searched for online 5 years ago really benefit a company? Who you meet? What you watch?

There is simply too much data collected on each user of a simple smart phone. We all have them today and most would agree that we can’t or wouldn’t want to live without them.

So if you worked for an international company and you wanted to hold a private conversation while in an important business meeting, or if you are active in a political organisation in opposition, maybe in a less democratic country, how do you ensure that your conversation and data is private?

The reality is that if you are using a smart phone with IOS or Android, you have no privacy, it’s that simple.

Facebook owned WhatsApp is a recent example. The change in the terms and conditions recently caused an outcry from users. Who hasn’t discussed something with a friend only to see ads related to this pop up after that?

While WhatsApp is clearly not a secure alternative, what about Telegram or Signal? They are popular communication apps. While much better with their security they are still accessible for authorities when they want to know information. Legislation recently introduced in many countries such as the EU directive that forces communication providers to give access to authorities when ever they are asked for it has also caused concerns.

Clearly we need to prevent crimes and stop criminals in every way we can, but when does this invade your privacy without you being a criminal? When will this type of access be misused? Never some say, but the Edward Snowden leak showed that misuse is exactly what it ends up in and those that have the right to privacy, lose it.

When we started looking at ways to offer secure communication, we also looked at some of the systems that claimed to offer “absolute secure communication”. Encro Chat and SkyECC are two systems that have been written a lot about in the media in the last year, but how secure was it really? Not at all apparently!

The conclusion was a simple one to make – if communications use a server, encryption levels do not matter, its accessible to someone if they really want access.

The Development

When you know what you need there are two ways to go about getting it. One option is to develop it from scratch, making something that has never been done before and creating something amazing. The other option is to have a deep look at what is already available and think about how this can be changed or adapted to fulfil the needs you have. We looked at both options and came to the conclusion that there were already some pretty good open source projects available albeit in different development stages.

After lot of consideration we decided that the Tox project (tox.io) had most of the required concept and code correct. Not only was it a project that was developed after the Edward Snowden leak as mentioned above, but it was community driven and not financed by big tech companies. There was less risk of someone buying their way in to the project to control it, and more importantly it was open source. We could view the code and functions and we could adapt it to our needs to provide a secure communication tool. Tox is a peer-to-peer chat. It doesn't use servers where messages are routed or stored, so there are no places to look for messages sent to anyone. The data laws granting prying authorities access to any server that holds communication is not effective against a Tox client. Just what we needed, secure privacy. Tox does have its weaknesses and we needed to overcome them.

Anyone can download a Tox Client (tox chat app) for their Android phone, there are several versions out there already. So why would we be different? What would we change to build a market that protected privacy, individual security and the right to communicate? It's protecting freedom of speech, the very core of democracy.

The Tox client had some weaknesses when you looked at how it works, the main one is the meta data and IP address of the user. Additional to this, if installed on an Android phone you are then in the hands of Google who already collect all the data of their users. How would this ever be secure and private?

We needed something more, we needed a Tox client installed on a phone that was not using Android or iOS. A phone that protected its users in a different way, a smart phone that offered not only a secure way to communicate, but that protected its users privacy in a real way.

We started looking at the alternative smart phone operating systems that were avaliable on the market. We needed to continue on the "open source" road, you can gain trust from users by heavy marketing, or you can simply show them openly what you do and how things work so that there is no hiding. If you can prove what you are doing, you don't need trust and the result is you gain trust anyway. Open source it has to be!

We spent considerable time looking at Ubuntu's old development, Ubuntu Touch. It is now supported by a large and very dedicated community around the world, UB Ports, and it offers a stable and secure operating system for smart phones that as a core has the users privacy and security in mind and it is also open source.

Now we had the start, the seed of a concept. A smart phone with a stable and secure open source operating system that protects the users privacy and security with a Tox client on it for secure peer-to-peer communication. But we needed more! We still had the meta data and IP address problem in the Tox client to solve.

If we create a virtual private network, a VPN, that is only accessible from the smart phones we supply, we create a “circle of trust”. A circle that connects the smart phone users on a private encrypted network, a network where they can connect to other services with the same privacy and security. For some users there would never be a reason to act outside if the network, if the services on the network, the circle of trust, was extensive enough to cover most privacy concerns.

Out of this thinking the AvoVPN network was born. It’s more than a VPN service, it’s a whole ecosystem for privacy. By integrating other services in the “circle of trust” a complete privacy ecosystem is created and the services within that ecosystem act as connections to services outside of the ecosystem too, connecting users of both worlds. By keeping the inside access to the ecosystem exclusive to a specific smart phone, we also create the security for the same smart phone.

At this stage of the development Zero Avocado Ltd is born. It’s a business and needs to be registered as such. The name “Zero Avocado” came from an internal joke among us. It seemed that technology and fruit was connected somehow, Apple, Blackberry, Raspberry Pie and so on. So we jokingly started with Avocado. But since we had no plans whatsoever to sell any avocado fruits, we added Zero in front of it. This is how the company behind the development and systems became “Zero Avocado Ltd.”.

Building a Business

As the smart phone was the key, both to the original idea of secure and private communication, as well as to the extended “privacy ecosystem” it seemed obvious to focus on this development first. Staying along the lines of the “Zero Avocado” name we named the smart phone “Avoozer” (avoozer.com).

The use of UB Ports open source OS for the phone gave us access to a skilled community of developers that not only helped us develop the smart phone, but more importantly the customized apps we needed.

Developers were hired on a project by project basis rather than employed and this is a business model we will continue to stick too. Not only can we find the best team for each individual development of the Avoozer smart phone, but we can cost estimate it very precisely and value each development with a business sense taking in to consideration what it does for the end user base of the phone and the privacy ecosystem as a whole.

Our first model of the Avoozer privacy smart phone, Avoozer KV Beta, was soft launched in June 2021.

Some have asked us why we use the “KV” as a name for our smart phone. The K & V stand for Ka & Veil. Ka in Egyptian mythology is the part of your body that remains after you die, in the modern world this would be the data you leave behind. Veil is another word for protect, shield and hide, exactly what we want to do with the users data. Ka Veil – KV. The Avoozer KV Beta privacy smart phone.

On the Beta version we loaded custom apps we developed. One of the main items was of course the secure communications app, the Tox client, now named Toxza. It provides exactly what the initial idea was, a way to communicate privately without any servers where messages are routed via and stored for future inspection by someone else.

Other custom apps developed include a “GPS spoofing” app. If android and iOS phones are so busy tracking your location and websites you visit are so keen to know where you are all the time, we decided that a fake GPS location was a good idea to offer, simply pick your desired location on a map and that is the GPS data used by the phone if a website or app is trying to use this data. You can of course turn off GPS coordinates completely on the phone too.

Further to this we added a custom made Matrix client for accessing the Matrix network of chat groups. The current matrix client on the Avoozer phone is called Zafluffy and is a simple standard matrix client while we develop some new thinking around the whole matrix network with our Lemozer concept. There’s more about this later in the white paper.

A TOR browser is of course included as is several other apps that focuses on secure, private and anonymous ways to access information and communicate. All without the normal tracking done by Android and iOS phones.

We also needed the very important exclusive virtual private network, VPN, the actual “circle of trust” for it all to work. In true Zero Avocado style we launched AvoVPN (avovpn.com). AvoVPN uses the highly trusted and tested OpenVPN structure to supply access to alternative IP address locations in several countries and areas around the world. OpenVPN is again open source and allows us to customise settings and functions to ensure we provide the service we want to offer, and it gives the users the trust in the system as its easy verifiable. AvoVPN does not use logs or down-throttling, it’s there to provide the Avoozer users with the encryption and privacy needed. It also means that Avoozer users can use any un-secure wifi access point, such as in their local McDonalds, or Starbucks or at airports and hotels and still remain private, secure and anonymous.

The AvoVPN forms a key part in the whole privacy ecosystem as it allows us to connect users with services in a closed and private network, whilst still leaving some of those services accessible to users outside of the ecosystem.

One thing we needed to integrate to the privacy ecosystem was social media interaction in some form without the spying and invasion of privacy that Big Tech is so busy with.

Big Tech often act as prosecutors and judges at the same time when it comes to deciding what is allowed to be said and what is not. While we understand and support the idea of what is legal and what is not, the laws and regulations vary from country to country. Why then should a private company be allowed to alone decide what is right or what is wrong?. Democracy is based on having a working legal system with courts and courts can decide what is legal and what is not in the country they are empowered to do so. Why do private companies need to interfere and interpret this on their own and who is given this power within private company?

We saw it when Twitter decided to ban a sitting president from expressing himself on their platform. Trump got banned as many know, not only from Twitter but also from Facebook. It’s not about

being pro-Trump or not, it’s what happens when the tide turns? Who decides who is allowed to express themselves and who isn’t?

Starting a social media platform from scratch is pretty much a dead route. Before you find enough regular users of the new platform the first few users have lost interest as there is not sufficient content. This puts a start up in an evil circle of always having too little content and users to grow by natural interest. It’s the fact that keeps Twitter in business no matter how badly they behave towards their users.

This thought led us to looking more closely at the Matrix network. It’s a decentralized “room chat” platform that already has over 25+ million users discussing a wide range of topics actively, The Matrix network also makes it easy for a user to set up their own private server where they alone can decide who can access it and register whilst still offering access to the rest of the Matrix network and its users. The French Army decide that this was the way for them to build a private and secure network for communication and many other have followed suit. The Matrix network simply offers opportunities for development that are too good to miss out on for the privacy ecosystem we are building.

What if we could take the matrix network and bridge it with other communication networks, such as telegram channels and create a twitter like experience for the user? And do this all on the ecosystem itself but with access also for those outside this “circle of trust”. This is how Lemozer ? (Lemozer.com) was started. It’s one of our main developments as we wanted Avoozer users to have access to secure and open chat groups that combine access and users within the privacy ecosystem and those outside of it. Giving users access to the Matrix system is simple, but we wanted to create a better user experience for it. While we of course make a custom app for the Avoozer smart phone for this, we will also offer Android and iOS users an app to enjoy the same user experience but without the privacy and security the Avoozer phone offers.

The privacy ecosystem also allows for many other future developments we have in the plan, such as encrypted email service within and outside of the ecosystem, anonymous and encrypted cloud storage and of course decentralized crypto exchange to mention a few. Privacy, security and anonymity requires many services to form a full ecosystem.

One easy way of keeping track of where we are in our development is to follow the constantly developing and updated roadmap for the whole ecosystem on its the Zercados website, zercados.com.

Zercados

This white paper is of course about the Zercados Token, so we need to explain the thinking and function behind the token and its development.

If you read all the information above we guess that you already have an idea of how the token will be used and why. But we want to explain why there is a need for a unique token like Zercados in the privacy ecosystem as well.

We always had the idea that an anonymous form of payment within the system would be required. How do you sell a smart phone ensuring privacy and anonymity if the only payment option is a credit card? You don't, so an alternative form of payment is needed.

Since we also use a rather large base of independent software and app developers to build and expand the ecosystem, we wanted a way to reward the developers that was not only fiat based payments. If you are an open source developer and you are building a system for us, Zero Avocado Ltd, and you know that "this can be a great thing" then most likely you would want a way to remain part of that success financially as well. This is where the Zercados Token plays an important role.

By giving independently contracted developers rewards in Zercados Token they effectively become part of the business future as Zero Avocado Ltd will use 40% of its pretax profits to buy back Zercados Tokens on the open market exchanges. This means that the yearly results of Zero Avocado Ltd directly effects the tokens value on the open market. A developer who has built a system for us, can choose to sell part of his tokens or even all of them. If he has built something he knows is good and has potential, he is more likely to hold some of the tokens if not all, and let future profits made in Zero Avocado have a positive effect of the rewarded tokens value.

The Zercados token will also be the only crypto payment accepted within the ecosystem itself. No matter if this is for the actual purchase of an Avoozer smart phone, paying for upgrades to encrypted cloud storage or to purchase apps or other services within the ecosystem.

This means that the Zercados token has a natural function for the end users in a unique market while it at the same time offers those who develop the systems to enjoy future profits from their work. Each service added to the system, each app developed and each service paid for increases the value of the whole ecosystem and therefor its future profit potential too.

Potential Zercados user scenarios

1. A private individual or group of people want to order Avoozer phones but want to stay somewhat anonymous, they buy Zercados on an exchange to use as payment form for the Avoozer smart phones.

2. An Avoozer smart phone user wants to buy credit for his e-Sim on the phone to get data or call credits but wants to remain anonymous, he buys Zercados on an exchange and uses this to pay for the service.

3. Avoozer already has an affiliate system where people who market the phone can earn 10% commission on any sales generated of the smart phone. This commission can be paid out in Zercados enabling the affiliate to enjoy an increased value of their holding if the phone and its services sells well.

4. A software developer contracted by Zero Avocado Ltd to create an app for the Avoozer smart phone uses a team of developers he has contracted to help him build the app. He is rewarded in Zercados for his work and can share the Zercados with each of his developers giving each one the

chance to decide themselves when they want to convert the Zercados maximising their return for the work completed.

5. A user on the Lemozer Matrix version wants to remove adds, he pays with Zercados.

6. An independent app developer develops and app he wants to add to the Avoozer App Shop. Once verified and accepted by the app shop the developer can choose if he wants the app to be free with a possible donation button, charge a onetime fee for the app or charge for services in the app. All done with Zercados Tokens both for the app user and the developer.

There are many other functions and situations where the Zercados Token will fill a useful role and become a natural function within the ecosystem and each such situation increases the value of the ecosystem and the Zercados token directly.

The most important factor for those holding the token, short or long term, is the buyback of tokens by Zero Avocado Ltd.

As costs for developments in pure fiat currencies is lower due to the fact that a major part of the rewards for system service incentives are based on rewards paid in Zercados tokens directly to developers, it enables Zero Avocado Ltd to buy back tokens based on pre-tax operational profits from the entire ecosystem. This includes hardware sold such as Avoozer smart phones, e-SIM services, private hosted Lemozer matrix servers and all other services provided. 40% of the yearly pre-tax profit is used to directly buy back tokens on open market crypto exchanges. The tokens bought back can then be reused for further developments increasing the ecosystems offerings, value and potential profits.

Even potential add revenue from apps developed and the Lemozer Matrix system will be paid in Zercados, increasing the usage of the zercados token as a transactional payment form.

The benefit of this system is that initial holders of the Zercados Token can expect not only a market for the token of other investors, but more importantly a market where the buyers of the token are not price dependent as they will use the token at once to pay for a service as an alternative to a credit or debit card. This is the natural market for the token in the ecosystem.

Marketing

While all token and coin pre-sales and ICO’s require marketing, Zercados are in the unusual situation of having a working business concept behind it that ensures revenue and a natural integration and use of the token itself.

This means that marketing efforts are best spent on marketing the products and services offered in the ecosystem instead of just the token.

We did however have a look at how others market their launches and due to the rather weird and unrealistic “world changers” there are on offer, we decided to go a different route and keep it simple and real

That said, we as others will use telegram, social media and websites to gain interest in Zercados but even more so in the ecosystem itself. We don’t need 1000’s of fake or paid followers on telegram or

social media, having real live interested people with an active interest in the ecosystem benefits us much more and ensures a stable and healthy growth of the ecosystem itself and the Zercados token.

Is the Zercados token for you?

- Do you believe there is a market for truly secure and private communication? If YES then Zercados are for you.
- Do you believe there is a need for social media style interaction that combines secure group chat functions with public groups and is not judged by a private company but rather by local laws to ensure compliance? If YES then Zercados are for you.
- Do you believe there is a market for a privacy ecosystem as a whole? If YES then Zercado are for you.

For any further information or questions please contact us directly with any of the below options:

Twitter: @zercados_token

Telegram channel: https://t.me/zercados

Zercados| Zero Avocado Ltd| UK

Website: www.zeroavocado.com
20-22 Wenlock Road
London
N1 7GU
United Kingdom
Zero Avocado Ltd is registered in England & Wales, No 13233242