Share Internet Data

trade megabits of internet for Tokens
blockchain enabled technology

Whitepaper

version of 6th June, 2018

This version is the 1st official private release and is to be treated as confidential info, pending further legal wording changes, if any, and thus it is only intended for Whitelist users or click here to login to your SID private area.

SID: Share Internet Data.

This might be the next game-changing technology that aims to enable a global internet access boom. Quote from the March 2017 Global Economic Forum press release: "Bringing the internet to the 4 billion people not currently online, which would add $6.7 trillion to the global economy and lift 500 million people out of poverty, new research has found".

Legal Disclaimer

As of the date of publication of this Whitepaper, SID Tokens have no known potential uses outside of the SID Platform ecosystem and are not permitted to be sold or otherwise traded on third-party exchanges. This Whitepaper does not constitute advice nor a recommendation by SID Limited (SID Ltd), its officers, directors, managers, employees, agents, advisors or consultants, or any other person to any recipient of this document on the merits of the participation in the Token Sale. Participation in the Token Sale carries substantial risk and may involve special risks that could lead to a loss of all or a substantial portion of such an investment. Do not participate in the Token Sale unless you are prepared to lose the entire amount you allocated to purchasing SID Tokens. SID Tokens should not be acquired for speculative or investment purposes with the expectation of making a profit or immediate re-sale. No promises of future performance or value are or will be made with respect to SID Tokens, including no promise of inherent value, no promise of continuing payments, and no guarantee that SID Tokens will hold any particular value. Unless prospective participants fully understand and accept the nature of SID Tokens and the potential risk inherent in SID Tokens, they should not participate in the Token Sale. SID Tokens are not being structured or sold as securities. SID Tokens are sold as a functional good and all proceeds received by SID Ltd may be spent freely by SID Ltd, absent any conditions set out in this Whitepaper. This Whitepaper is not a prospectus or disclosure document and is not an offer to sell, nor the solicitation or any offer to buy any investment or financial instrument in any jurisdiction and should not be treated or relied upon as one. This Whitepaper is for information only. Written authorisation is required for distribution of any or all parts contained herein.

All information here that is forward looking is speculative in nature and may change in response to numerous outside forces, including technological innovations, regulatory factors, and/or currency fluctuations, including but not limited to the market value of cryptocurrencies.

This Whitepaper is for information purposes only and is subject to change. SID Ltd cannot guarantee the accuracy of the statements made or conclusions reached in this document. SID Ltd does not make and expressly disclaims all representations and warranties (whether express of implied by statute or otherwise) whatsoever, including but not limited to:

- any representations or warranties relating to merchantability, fitness for a particular purpose, suitability, wage, title or non-infringement;

- that the contents of this document are accurate and free from any errors; and

- that such contents do not infringe any third party rights. SID Ltd shall have no liability for damages of any kind arising out of the use, reference to or reliance on the contents of this document, even if advised of the possibility of such damages.

This Whitepaper includes references to third party data and industry publications. SID Ltd believes that this industry data is accurate and that its estimates and assumptions are reasonable; however, there are no assurances as to the accuracy or completeness of this data. Third party sources generally state the information contained therein has been obtained from sources believed to be reliable; however, there are no assurances as to the accuracy or completeness of included information. Although the data are believed to be reliable, SID Ltd has not independently verified any of the data from third party sources referred to in this Whitepaper or ascertained the underlying assumptions relied upon by such sources.

Please note that SID Ltd is in the process of undertaking a legal and regulatory analysis of the functionality of its SID Tokens. Following the conclusion of this analysis, SID Ltd may decide to amend the intended functionality of its SID Tokens in order to ensure compliance with any legal or regulatory requirements to which we are subject. In the event that SID Ltd decide to amend the intended functionality of its SID Tokens, SID Ltd will update the relevant contents of this Whitepaper and upload the latest version of this to its website.

Any SID Tokens could be impacted by regulatory action, including potential restrictions on the ownership, use, or possession of such tokens. Regulators or other circumstances may demand that the mechanics of the SID Tokens be altered, all or in part. SID Ltd may revise mechanics to comply with regulatory requirements or other governmental or business obligations. Nevertheless, SID Ltd believe they have taken all commercially reasonable steps to ensure that its planned mechanics are proper and in compliance with currently considered regulations.

CAUTION REGARDING FORWARD-LOOKING STATEMENTS

This Whitepaper contains forward-looking statements or information (collectively “forward-looking statements”) that relate to SID Ltd’s current expectations and views of future events. In some cases, these forward-looking statements can be identified by words or phrases such as “may”, “will”, “expect”, “anticipate”, “aim”, “estimate”, “intend”, “plan”, “seek”, “believe”, “potential”, “continue”, “is/are likely to” or the negative of these terms, or other similar expressions intended to identify forward-looking statements. SID Ltd has based these forward-looking statements on its current expectations and projections about future events and financial trends that it believes may affect its financial condition, results of operations, business strategy, financial needs, or the results of the Token Sale or the value or price stability of the SID Tokens.

In addition to statements relating to the matters set out here, this Whitepaper contains forward-looking statements related to SID Ltd’s proposed operating model. The model speaks to its objectives only, and is not a forecast, projection or prediction of future results of operations.

Forward-looking statements are based on certain assumptions and analysis made by SID Ltd in light of its experience and perception of historical trends, current conditions and expected future developments and other factors it believes are appropriate, and are subject to risks and uncertainties. Although the forward-looking statements contained in this Whitepaper are based upon what SID Ltd believes are reasonable assumptions, these risks, uncertainties, assumptions, and other factors could cause SID Ltd's actual results, performance, achievements, and experience to differ materially from its expectations expressed, implied, or perceived in forward-looking statements. Given such risks, prospective participants in a Token Sale should not place undue reliance on these forward-looking statements. Risks and uncertainties include, but are not limited to those identified in the Token Sale T&Cs. These are not a definitive list of all factors associated with making a contribution to SID Ltd, in connection with its operations.

SID Ltd undertakes no obligation to update any forward-looking statement to reflect events or circumstances after the date of this Whitepaper.

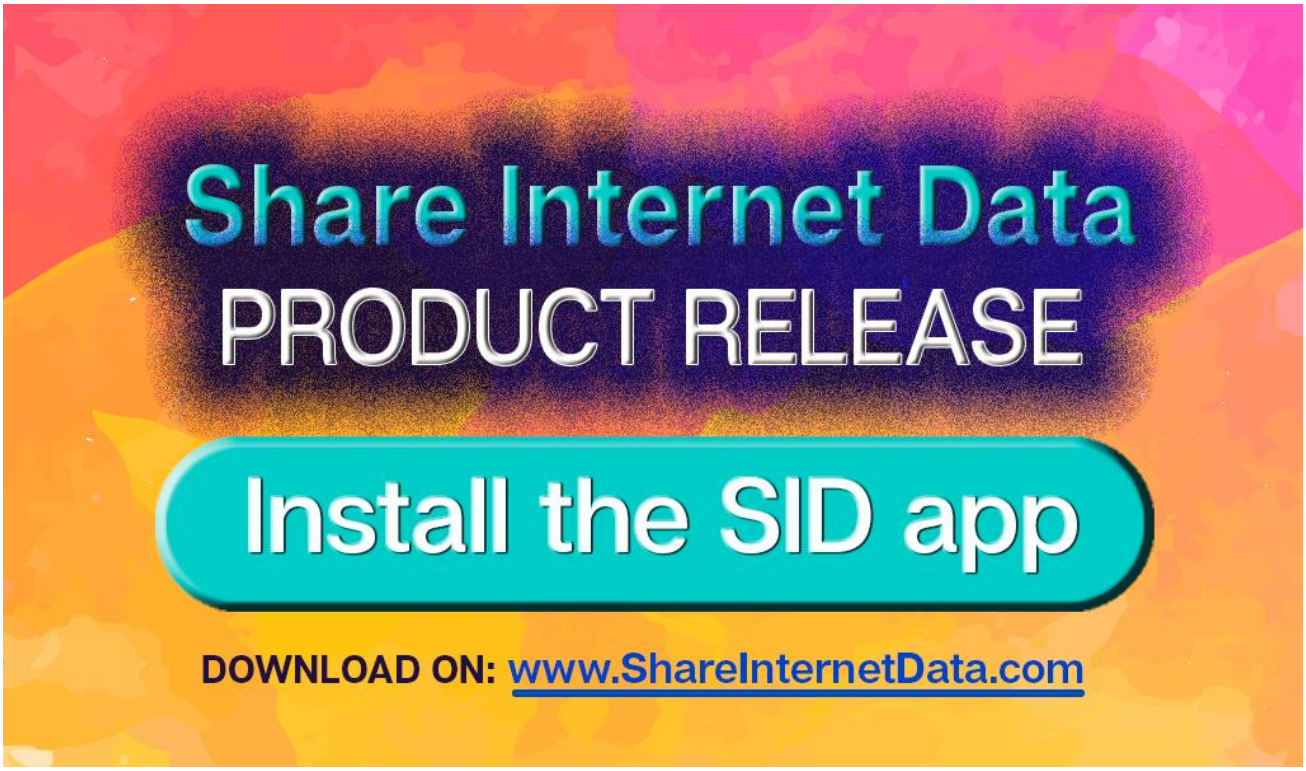
SID Ltd's business is subject to various laws and regulations in the countries where it operates or intends to operate. There is a risk that certain activities of SID Ltd may be deemed in violation of any such law or regulation. Penalties for any such potential violation would be unknown. Additionally, changes in applicable laws or regulations or evolving interpretations of existing law could, in certain circumstances, result in increased compliance costs or capital expenditures, which could affect SID Ltd's profitability, or impede SID Ltd's ability to carry on the business model and the SID Tokens model proposed in this Whitepaper.

Abstract

SID (share internet data) is a peer-to-multi-peer decentralized internet sharing system that allows sharing internet from one person to another in an automated manner.

One of our key missions through this project is the following: “To lift as many people as possible out of poverty by means of giving the less fortunate a way to access internet for free”. SID aims for Users to be able to get in future free internet access by obtaining tokens in exchange of consuming advertising. Such obtained tokens can then be used to consume internet megabytes from other nearby Users in exchange for tokens, meaning SID Tokens are intended to be use on the SID platform as a functioning good.

This trading of tokens for megabytes, is aimed to motivate Users with mobile data to share their mobile internet data bundle with other nearby Users. Till today any non-consumed mobile data at the end of each month, on most traditional network operator User contracts, is simply lost. In the same way our decentralized system made up of Smartphones and tablets of our Users, incentivizes Users to also share their private Wi-Fi and business internet without giving their private or business password to any other person; simply a User can “share internet data” (SID) securely through their own mobiles with other nearby Smartphones. The first SID app commercial product release was done on 6th February 2018.



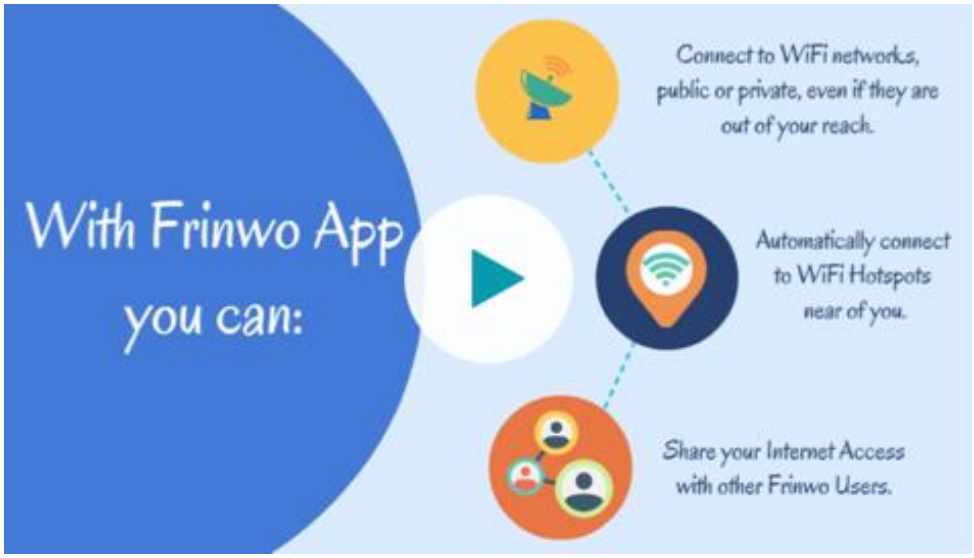
Index

1 Company statement

SID (Share internet Data) Limited is company registered in Gibraltar with company number 116861, registered offices at 3rd floor, Suite 932 Europort, Gibraltar GX11 1AA, Gibraltar - Europe. SID owns all the assets of Frinwo S.L. including its intellectual property and Brand. Frinwo was founded in Dec 2016 to develop the patent pending technology. Frinwo S.L. is the exclusive R&D cost centre for SID.

The key company mission of SID is:

To be a humble contributor to lifting people out of poverty through internet provisioning, by a means of sharing internet through nearby smartphones Users



The mission is simple, clear and measurable through the number of users that will access, in future, free internet provided by nearby SID users or through the SID platform or through third party services that are or may be use in future a SID SDK, in their own products. Internet access aims to allowed people to participate in the Digital Economy.

In order to make it attractive for individuals with internet to share part of their own free Wi-Fi internet with others, SID is aiming to incentivise users to install SID on their smartphones by giving them in future extra services. For example, allowing messaging even when a user has no internet himself to use neighbouring users to send his encrypted message to its destination. Also, an in-app SID browser aims to provide internet browsing capability to Users to check emails or Facebook, Twitter or LinkedIn messages and so forth online.

The SID technology has been protected by patent pending intellectual property. However, the management and founders are believers in the open market principle. The more devices that implement our innovative technology, the more mobile free internet access points are made available. A key company strategy is to complement organic growth with third party growth by means of commercial license agreements with companies such as our client Dunkin Donuts franchise of Spain, Dunkin Coffee. This strategy is a win-win for both companies: SID users get more free internet access points across the globe, for example a company such as Samsung would get potentially a service that aims to create an eco-system around their hardware device. In this event Samsung smartphone users would become more inclined to stay with Samsung instead of switching to other brands. The expectation of creating the start of a true eco-system within for example Samsung, Facebook or Tencent's WeChat by incorporating the SID SDK inside, thereby enabling free internet sharing between all Samsung smartphones and tablets aimed to create media coverage on the subject and intended to resulting in certain users from Samsung competitors deciding to purchase a Samsung smartphone or even switch from their current mobile phone to start using Samsung smartphones potentially with the SID technology inside.

It is important to note the commercial value to, for example, Facebook, WeChat, Alibaba, eBay or Amazon of incrementing the time their users are connected to the internet as a consequence of using the SID SDK is of incredibly high value. Because their income depends strictly on their customers using their services and that requires internet connectivity.

SID aims to also expand into other revenue sharing business channels, such as potentially by integrating our SID SDK in an adapted MiFi device becoming a Mobile Virtual Network Operator (MVNO) or alternatively make a revenue sharing deal with a traditional Mobile Network Operator (MNO) to sell mobile data to end-Users at actual cost. At cost means, that SID would make the margin equivalent to the percentage of internet data sourced from free Wi-Fi hotspots on the SID network or sourced from other nearby SID Users.

2 Summary

SID (share internet data), is a peer-to-multi-peer decentralized internet sharing system that allows sharing internet from one person to another in an automated manner, designed on the back of two pending patents from 2015 and 2017 respectively. Whilst currently the SID system is free to use, in the next few months until post an ITO (Initial Token Offering), in future SID aims for SID Users be able to get certain free internet access by obtaining tokens in exchange of consuming advertisings. Such obtained tokens can then be used to consume internet megabytes from other nearby Users in exchange of tokens. Those trades can be done through our secured servers or simply secured by a blockchain, such as Stellar.

This trading of tokens for megabytes, in particular, is aimed to motivate Users with mobile data to share their mobile internet data bundle with other nearby Users. Till today any non-consumed mobile data at the end of each month, on most traditional network operator User contracts, is simply lost. In the same way, our decentralized system made up of Smartphones and tablets of our Users, incentivizes Users to also share their private home Wi-Fi without giving their private password to any other person, simply a User can “share internet data” (SID) securely through their own mobiles with other nearby Smartphones.

A major focus is aimed at marketing SID (share internet data) service also in emerging markets in order to achieve a higher impact on its company mission. In Emerging markets, the Android operating outpaces the iOS on average by more them 6 to 1. For consumers in developing markets, the smartphone is the primary (or only) device for accessing Internet services. Apps must be data efficient to meet the special requirements of these users:

Mobile networks provide often in those emerging markets significantly less bandwidth and quality than in mature markets. (Some users are often on GPRS or EDGE.)

Many users buy data bundles in small increments (e.g., 10Mb) and only periodically (e.g., on weekends). Wi-Fi usage is massive (e.g., in cafes) … but Wi-Fi speeds are often far lower than in mature markets.

Share internet data (SID) is aimed therefore to be the single most important feature in our SID Eco system, which we aim to offer also to selected third party Licensees, as an SDK, aimed at helping to expand faster globally the “Share Internet Data” service.

We propose a solution, different to the status-quo, where users only obtain internet directly from traditional service providers or mobile network operators or Wi-Fi hotspots. This is achieved by using our innovative crowd sourced internet in a peer-to-peer or peer-to-multi-peer structure overseen by a patent pending proprietary technology. The trading of tokens for megabytes of shared internet is aimed to be done in an automated way through Stellar protocol, similar to contracts secured by a blockchain. Such trades aim tentatively to create a more liquid token (virtual voucher) market. At the moment one of the technical hurdles that we are still trying to resolve is the abusive high amount of commission charged currently (also referred to as transaction fee received by so called miners) by the mayor crypto currencies (on bitcoin blockchain or ether blockchain). For example a Bitcoin transaction to confirm within 6 blocks (none urgent 60min) with 1 input and 1 output (as at 29 Nov2017) costs around USD 1.82 according to https://estimatefee.com/ which is unacceptably as its even higher than the expected lowest USD 0.01 micro transactions value itself of our future SID users trading tokens (voucher) when consuming megabytes with a rough value in the order of magnitude of USD one digit cents per 10 megabytes. So, in conclusion a bitcoin blockchain is discarded as our trading platform needs to charge a magnitude fraction of a USD cent or as close to zero as possible.

It is however a bigger hurdle to convince people to share their mobile internet data, therefore any potential future incentive(s) aimed to help somehow the less fortunate, if any, are aimed to be applied equally to all our SID users. Therefore, those users sharing their mobile data with nearby users are aimed to get paid in tokens (voucher credits) for such consumed internet megabytes of data, instead of letting it go to waste at the end of each month. Actually traditionally, people would have given the password of their home Wi-Fi to visitors thereby exposing the security of everything connected to their internal Wi-Fi network. In our SID solution the User who is home shares internet with visitors through his Smartphone and thus not needing anymore to give his private Wi-Fi password to anybody but instead aims to tell any visitors to download the SID APP.

This Whitepaper proposes an internet sharing ecosystem which can offer:

- The share internet data (SID) system that enables sharing internet megabytes of data between nearby users decentralized and fully automated and managed by the Users' smartphones' themselves. ***DECENTRALISATION IN THE TRUE SENCE THAT TH ENDUSER OF SID DECIDES IF IT SHARES INTERNET WITH OTHER SID USERS OR NOT!!!***

- The token (voucher credits) trades are aimed to settled automatically once an internet connection is lost, with the smartphone that did share his internet by executing the trade transaction on a software code (similar to contract) for the Stellar blockchain, where his wallet (voucher account) aimed to be credited and the user wallet (voucher account) of who obtained internet aimed to be debited in the same amount. The user who obtained internet should then receive on his smartphone an updated wallet balance (voucher account credit balance) with the executed debit transaction at the first next time it connects to the internet.

- The SID systems is aimed to be a few months post ITO (initial token offering) a decentralised system, only interacting with the blockchain to confirm token trades (voucher credits) respectively, for consumed megabytes OR to confirm tokens received (voucher credits) received for advertising consumption.

- The SID system functions through an APP downloaded on smartphones or tablets, and they function for Android devices even when in Users pockets aimed to be without any user interaction. Aimed to automatically pay or in other words trading tokens (voucher points) for consumed internet for those who receive internet from others, or in the case of those giving access to their internet they get paid tokens (voucher credits) for the internet megabytes of data given to nearby Users. Payments are trades.

- The decentralised "share internet data" (SID) system aims to contribute to the liquid of the token (vouchers).

- As per the patent pending technology implemented in the SID system APP, the SID app is aiming to extend the radio range of Wi-Fi hotspot through the auto configuration of our APP to use nearby smartphones which are connected to an internet source (be it Wi-Fi or Mobil data) as ***internet hosts*** sharing such internet with other SID users who are not in radio coverage of the Wi-Fi hotspot but are in range of the SID smartphones' ***internet host***.

- Also, as per the patent pending technology implemented in the SID system APP, it aims to provide extended indoor radio coverage where mobile data coverage is not sufficient inside some buildings or simply saturated in crowded places. By means of the auto configuration feature of our APP that uses nearby smartphones which are connected to an internet source (Wi-Fi or Mobile data from a different mobile network from a nearby user) as ***internet hosts***, meaning as internet sharing sources.

- The previous, also applies when Users are Roaming with their smartphones or tablets and are intended to be able to consume internet shared by nearby ***smartphones hosts*** connected to their local Wi-Fi. In fact, roaming users may not have most passwords when abroad) or their local Mobile Data (as roaming costs are abusively high between most countries except for between EU countries.

- Our SID system does not use any remote VPN Cloud-server to tunnel the internet access through to hide the actual internet resource accessed, as that is forbidden in countries such as China and Russia.

- Our SID system does not use any functions that can be controlled through the SIM, meaning the SID system does not use any smartphone or tablet internal tethering or hotspot feature.

In order not to damage the brand aimed to be used commercially, this SID system solution was being tested using other brands, like the Frinwo brand and we kept the SID brand from the 1st commercial product release on 6 February 2018. The commercial brand is **ShareInternetData** or simply **SID** for short, as the name says exactly what our decentralized system does. We could however use instead or in addition to SID a variety of other brands such as **FreeInternet4All** or **FreeInternetForAll** or **Frinwo** but we welcome from Users alternative names or trademarks so long

the corresponding domain names can be purchased at a reasonable rate. A list of domains that we have acquired from which we can also choose from, is listed in Appendix 1.

It is to be noted that our tokens (vouchers) can increase or decrease in value. A comparison would be the ride on an Uber taxi can be cheaper or more expensive for the same route depending on the time of day and the actual users' demand. In that same analogy the cost for say 100 megabytes of Mobile data shared from one of our SID users (Uber driver) may cost more or less depending on the price he paid for mobile data bundle or from the amount of demand from other Users wanting to get internet shared by him. Therefor the number of tokens (voucher credit points) paid per 100 megabytes may vary over time or in different regions. But similarly, if Users who received Tokens (Voucher credit points) want to cash some of them out (like an Uber driver cashing out his earnings on his Uber account into actual cash in a given currency) then the value of those tokens (vouchers) may also vary.

3 SID project overviews.

The “share internet data” (SID) project, has been under development since over a year now and has gone through the following stages till to date.

Feb. 2015

A PCT patent has been filed on 3 February 2015 “System and method for a global wireless indirect internet connect system” as PCT/GB2016/050241 and published in 2016 as patent nr WO2016124915A1. For those interested in full access of such pending patent, here is the URL: https://www.google.com/patents/WO2016124915A1?cl=en

The pending patent has already entered recently examination phase, as of 1 September 2017 in Europe as application number 16705984.9 (PCT/GB2016/050241) and as of 2 August 2017 in the US as application number 15548351 (PCT/GB2016/050241).

Dec. 2016

The patent was assigned to a start-up called Frinwo S.L. co-founded by one of the authors of the patent and a development team (R&D team) who would go on to implement the core technology of the above patent in software codes as proof of principles. The objective was to develop over the next years 3 SDKs (Software Development Kit), meaning a black box software module) and a working proof of principle or an APP and Server to proof its functionality. The 3 SDKs were these:

AutoWiFi SDK:

When integrated in a 3rd party APP under license or in an APP, this SDK aims to connect the Smartphone or Tablet automatically to internet sources from global Wi-Fi access points of the same network, in example of a future SID network. All passwords of the network are stored in an encrypted manner on a secure server and are downloaded in a block of a region/country or a radius (1km, 5km, 10km, 100km or 500km depending on the number of ***internet hosts*** per radius as to limit the amount

of data to be downloaded) from the position of the user´s smartphone at time of APP download and updated at certain regular times thereafter.

SID SDK:

When integrated in a 3rd party APP under license or in our own SID APP, this SDK aims to connect the smartphone or tablet automatically to internet sources through other users Smartphone's' or Tablets that have the same APP installed, in example the SID APP. Herein the smartphones or tablets that have a direct internet source function as ***internet hosts smartphones*** for other smartphones or tablets that do not have direct internet access. It is this SDK that concentrates most of the novelties of the pending patent filed by a founder.

Chat SDK:

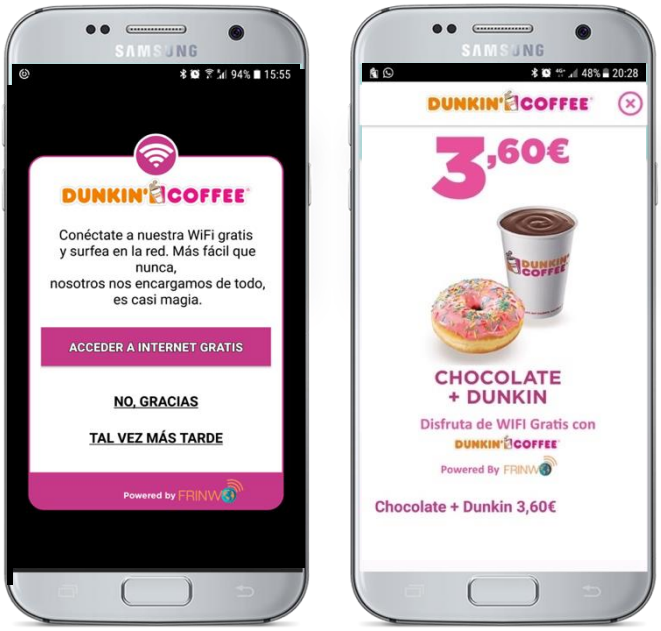
When integrated in 3rd parties APP under license or in a future SID APP, this SDK aims to allow Smartphone Users to chat with other Smartphone Users that have the same APP installed, in example the SID APP even when nearby users are not sharing their internet access. This SDK however is interdependent of the above SID SDK because the Chat SDK relies on using the same secure proprietary communications channel from the SID SDK. So, this one will be considered for potential development as last priority if at all.

July 2017

One of two SDKs under development was completed, namely the **AutoWiFi SDK** and was consequently implemented in the APP of a real 3rd party client, as proof of concept. The client's testing has been completed satisfactory and released their APP to its own users on 27th November 2017. The client's name is "Dunkin Coffee" which is Dunkin Donut´s franchise for Spain. With around

59 stores the **autoWiFi SDK** is integrated into the Dunkin Coffee APP. This converts all the shops of that Dunkin Coffee franchise into internet hosts, aiming to connect all Dunkin Coffee users automatically to the corresponding Wi-Fi access point when a user is getting close to any of their coffee shops. All passwords are intended be changed and aiming not to give anymore passwords to clients but rather aimed to be told to download the Dunkin Coffee franchise APP intended to get automatic access to the internet across all their stores in Spain. Formal marketing campaign launch by Dunkin Coffee franchise was planned be done starting from the 1st week of February 2018. The next step aims to integrate, in the future, also the SID SDK in their APP to extend the range of their Wi-Fi coverage through nearby Smartphone's and to allow Dunkin Coffee Users to also have internet access when not at their store by sharing internet data between nearby Smartphone's from other Dunkin Coffee or other SID Users.

See below actual real live smartphones pictures of the Dunkin Coffee APP for real users made in December 2017, where our **autoWiFi SDK** technology works when downloading the Dunkin Coffee APP in Spain. There were around 250 thousand downloaded APPs of the Dunkin Coffee APP, with around 91 thousand active monthly users which are auto updated gradually with the attest Dunkin Coffee iOS and Android APP with our **autoWiFi SDK** inside (shown as "**Powered by Frinwo**" and from which SID users are aimed to be able to share internet with, when Smartphone's are nearby.



Sept. 2017

Work was started by one of the authors of the previous mentioned 2015 filed pending patent to come up with the technical solutions that was needed in order to truly have a distributed internet

sharing system that can operate in a decentralized architecture. Such system needs to be scalable at a global level. An initial title was decided by its writer and sole inventor, namely "SYSTEM AND METHOD FOR DISTRIBUTED INTERNET SHARING". This was seen as crucial, in order to be technically bullet proof for the product roadmap, as outlined in this Whitepaper. Some key parts of the patent, whist writing this were tested by its author as to assess its novelty and to convince himself that a particular technical issue or shortcoming was solved when implementing a particular embodiment or claim or combination thereof.

Nov. 2017

The first alpha version of the development of the second SDK was completed for Android, namely the **SID SDK** and is currently available only on the Android Play Store for potential Users or potential future token (voucher) buyers. Such proof of principle SID SDK has been wrapped around with a basic user interface strictly to visualize some key internal functions. Those interested to evaluate our core technology can download it from the Google Play Store searching for "**PatentPending**" or by clicking on this URL: https://play.google.com/store/apps/details?id=com.patentpending&hl=en

Those potential Users or future token buyers who install this APP strictly and only for evaluation purpose on their Android Smartphone and Tablet, need to consider the following carefully:

- The **PatentPending** APP is the **SID SDK** with a user interface wrapped around it only to make some of the internal function visible to the User evaluating our core technology based on our patent pending intellectual property rights. Therefore, the **PatentPending** APP is encrypted.
- The **PatentPending** APP will NOT be updated regularly on the Play Store because the main focus is to complete the commercial version of our own SID APP with that SDK inside. At the time of completion of this Whitepaper that SID APP commercial version was already released months earlier and can be downloaded from our website: www.ShareInternetData.io
- **The minimum Android requirement for the evaluation APP called PatentPending is Android 5.1 and the APP has only been tested up to Android 7 as those were the only smartphones operating systems available to us until early Jan 2018. No further updates of the PatentPending will be done from now onwards.**
- The evaluation APP, called **PatentPending** with the **SID SDK** inside, has certain protections as to ensure our intellectual property rights are protected. In that way the **PatentPending** APP in a

Smartphone operates and auto-connects sharing internet with other nearby Smartphone's who also have the **PatentPending** APP inside, even in background if both devices have up to Android 7.

- The password to activate the evaluation SDK when downloading the **PatentPending** APP is: **ProofOfPrinciple**. Password is not case sensitive. We reserve the right to change the password and/or remove the PatentPending APP form the Google PlayStore at any time & without notice.

Nov. 2017 continued.

The SID Co-Founder completed, after several months of work, the filing of the strategic pending provisional patent as sole inventor and registered at the USPTO on 21st November 2017. Several extracts of this provisional patent have been used further down in this Whitepaper now that intellectual property protection has been obtained with the filing date as the priority date.

Jan. 2018.

The Android 7 issue of not auto connecting in background has now been fixed but it took around 2 months to find an acceptable solution simply due to restrictions imposed by Google on the Android 7 operating system update. This is always a technical and company risk when we and all other companies globally depend on the operating systems updates from Apple, Google and smartphones manufacturers like Samsung who then use a variant of the Android operating system. Once there are sufficient smartphones with Android 8, only then will we be able to assess what issues and if any need resolving, if possible at all or if a work around needs to be found and how many months that may take.

Once the previous mentioned issue was resolved a production release version has been prepared fixing the typical issues of some app crashes on a functional basics and so forth. Testing looks promising and a formal commercial end-user release for testing of a production version SID system is planned for end of Jan 2018. To get the approvals process started by Apple and Google a version of SID as of 20th January was uploaded, resulting in a rejecting from Apple and an acceptance from Google. The issue with Apple was resolved and resubmitted and finally accepted. With this it becomes easier as from now on its basically only uploading SID app updates to both stores. We plan to upload app updates with fixes as they come along regularly, as a result of scaling and more users using the SID Apps.

However, the decision is now made that the trademark Share Internet Data, or SID for short, is going to be used for the 1st commercial product launch and thus a company was registered in an

ICO / ITO (Initial Coin Offering / Initial Token Offering) friendly Gibraltar and achieved incorporation certification on 31st January 2018. By 4th January SID Ltd entered into an SPA (Sale and Purchase Agreement) with Frinwo S.L and purchased all its relevant assets.

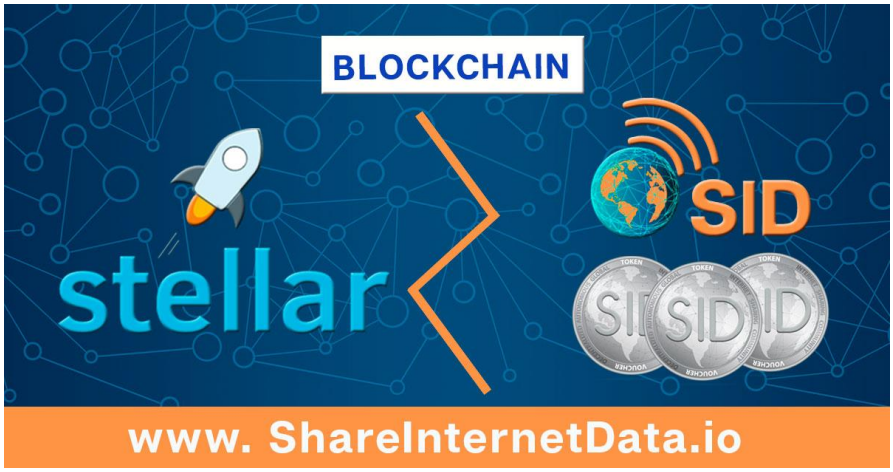
Than by January 6th 2018 SID Ltd Chairman & Co-Founder announced publicly in the morning CET time-zone, first through Linked-in, the formal 1st commercial release of the SID APP. That same day in the evening CET time-zone SID Ltd entered into a Board Advisor Agreement with LDJ Cayman Fund Ltd represented by David Drake aimed to allow for the purchase of future SID Tokens and join SID Ltd as a Board Advisor, together with the other ICO/Crypto/Blockchain Board Advisor that joint shortly after, namely Simon Cocking, and Vladimir Nikitin the Nr1 to 3 on icoBench.com. Other Board Advisors include our 1st woman Board Advisor Wannipha Buakaew, Amarpreet Singh, Nikolay Shkilev, Christiam Nyborg, Kerry Ritz.

4 Which blockchain will be used?

The principle objective of a Blockchain for Share Internet Data (SID) is to ensure the highest possible form of security, transparency, and efficiency of executing the trades of Tokens (vouchers) for Megabytes transactions and keeping SID future users' Wallets up to date and safe. To this end, we are in discussions with major custodians which are able to offer rich APIs which we can interface with, in order to provide the sort of efficiency and transparency that potential regulators and the Users of our system can take absolute comfort from.

The system aims to handle cross border, multi-micro-trades settlements operating around the clock including the regular transfers of traded Tokens to the future SID Users wallets. Further details, if any, to be announced in due course on our website.

So far, the single biggest reason why the choice of which blockchain Share Internet Data (SID) was not firmly closed for the first year, is due to an exhaustive technical due-diligence. The value of our future trades of tokens (vouchers) are in the order of magnitude of 1 dollar/euro/sterling cent for consuming roughly 10 Megabytes of shared internet data. Therefor the cost per transactions of the ultimately selected blockchain had to be an extremely small fraction of a cent AND the transaction itself has to be in the region of a few seconds. This is aimed to be resolved by the choice of blockchain but unfortunately it can't be Bitcoin or Ethereum based blockchain, so in the end only one really ticked all the right tick boxes, namely the STELLAR blockchain. So, we have chosen Stellar as our blockchain.

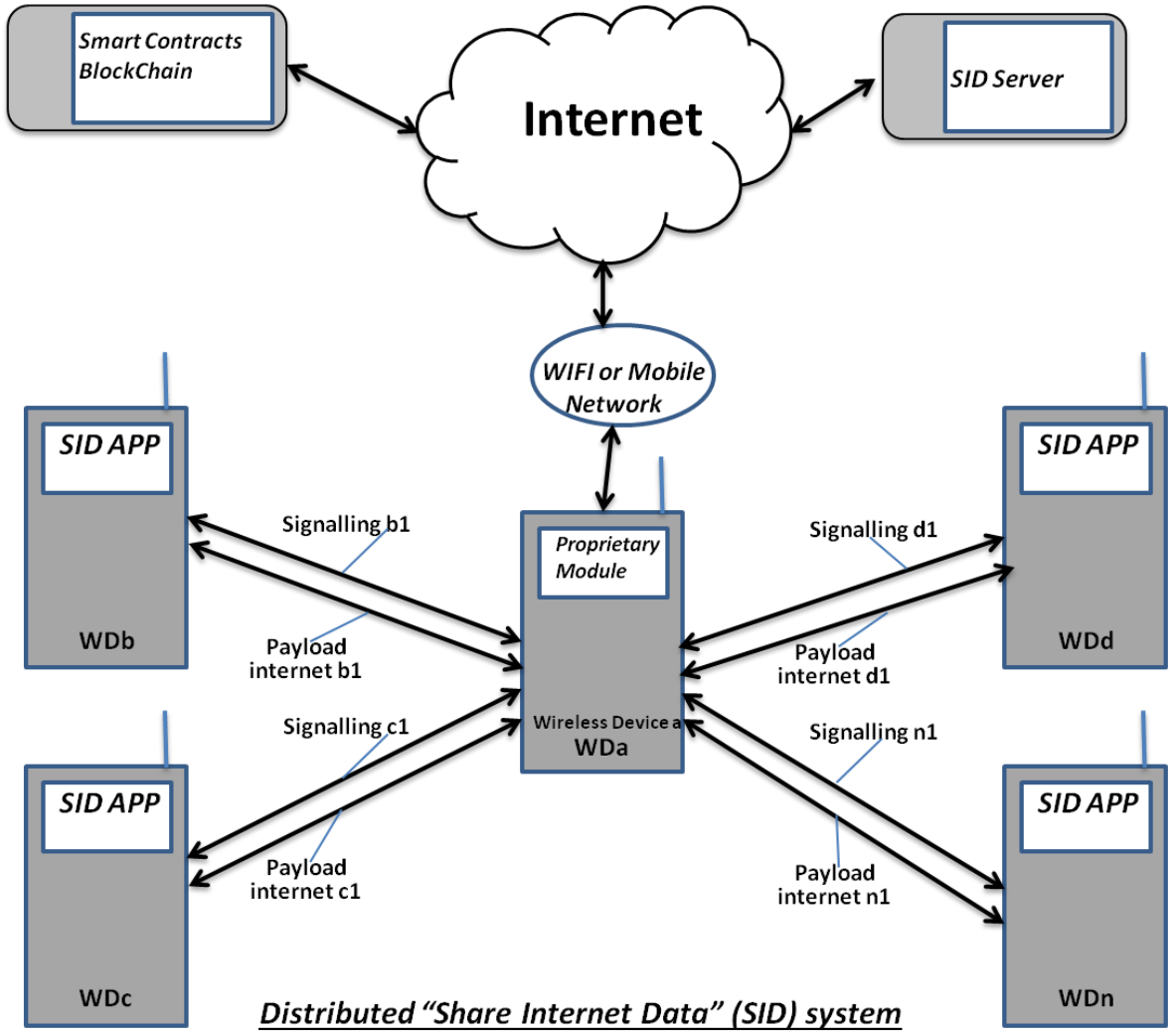


5 How does the Share Internet Data (SID) system work?

5.1 Share Internet Data (SID) top-level system

In order to better understand the ins and outs of the working of the key technology of the SID system, we start from a top-level view of the SID system and then we go down to the more detailed technical description of the core technology.

A great starting point is from a simplified version of the top-level system drawing, shown below.



The SID technology is depicted in the previous top-level system drawing as "Proprietary Module" which in effect is what we developed as the "SID SDK". In practical, it means that both the **autoWiFi SDK** and the **SID SDK** are integrated into the SID APP, downloadable onto a Tablet or Smartphone

(WDa to WDn) or even into a future adapted MiFi Device. Further down more about the MiFi device but right now let's focus on the biggest market, namely the global Smartphone market.

We can see that Smartphone WDa has internet access through a network. This "Network" gateway to the "Internet" could be a Mobile Network Operator or a Wi-Fi network, whilst all other smartphones WDb to WDn have no internet access for whatever reason; not in Wi-Fi range or no Wi-Fi password or no mobile coverage or no mobile data credit left. Here is where our SID technology kicks in, when the Smartphone WDb User, without any direct internet access, is nearby Smartphone WDa User then the Smartphone WDb "SID SDK" aims to automatically interact with the Smartphone WDa "SID SDK" over a secure encrypted "Signalling b1" channel exchanging all necessary info such as, have sufficient Tokens (Vouchers) and the frequency channels that are seen free or least interference radio channels and so forth. Such signalling channel is in effect an ultra-low power consumption narrow band radio connection, such as a Bluetooth Low Energy channel which payload is encrypted by the SID system with a 256 AES encryption but might change to a 128 AES encryption to reduce further consumption. With that info received by the Smartphone WDa "SID SDK" aims to automatically respond to the Smartphone WDb "SID SDK" over the same secure encrypted "Signalling b1" channel providing the channel number it has chosen to initiate a secure channel to **share internet data** through, as well as the BSSID or SSID and the password to use such channel and so forth. This last channel, referred to in above system drawing as "payload internet b1" is a medium power consumption wide band radio connection (for example Wi-Fi or Wi-Fi Direct or similar) to ensure sufficient bandwidth is available to share internet. With this last info received by the Smartphone WDb "SID SDK" aims to automatically disconnect and power down the signalling level, to reduce power consumption, and intended to automatically connect to the "payload internet b1" channel connecting with the decrypted credentials as password, channel number, frequency band and so forth.

At this point all internet petitions from Smartphone WDb are all channelled through the "SID SDK", using a Proxy or VPN function strictly between smartphones BUT IN NO CASE DOES SID USE ANY VPN CLOUD-SERVER AT ALL IN ITS CURRENT PRODUCT. The Smartphone WDb "SID SDK" passes its internet petitions to the Smartphone WDa "SID SDK" who passes those petitions on individual multiplexed threads to the direct internet connection and every internet response content is de-multiplexed and put on the corresponding thread that made such original petition and send back encrypted with a 128 AES encryption to Smartphone WDb "SID SDK" and decrypts such internet responses.

Similar case for the User of Smartphone WDc to WDn 4 aims to receive internet shared by the same source WDa through their corresponding “SID SDKs”. Although the technical capability of the hardware is quite high, meaning capable of connecting around 7 simultaneous smartphones by a BLE signalling channel or connecting around 10 smartphones by Wi-Fi, the SID system limits the maximum number of smartphones that are allowed to connect to a single ***internet host (WDa)*** to two (2) and in future possibly up to four (4) when connected to the charger, in order to reduce power consumption. Also, the power of the wide band channel is aimed to be managed in future products to be limited according to the RSSI (radio signal strength), for example if RSSI received at Smartphone WDb is -50dBm which is transmitted by the Wi-Fi Direct transceiver of Smartphone WDa than the output power of such transceiver is reduced to the minimum because -50 dBm is a very strong signal reception meaning WDa and WDb are in very close proximity (5 to 10m) of each other. Similar if RSSI at WDb side is less than -80 dBm then the output power of Wi-Fi transceiver is set to the maximum output power because any value less than -80 dBm is approaching a very weak signal reception meaning WDa and WDb are indoors with interfering walls or floors (10 to 70m) or simply not in close proximity of each other.

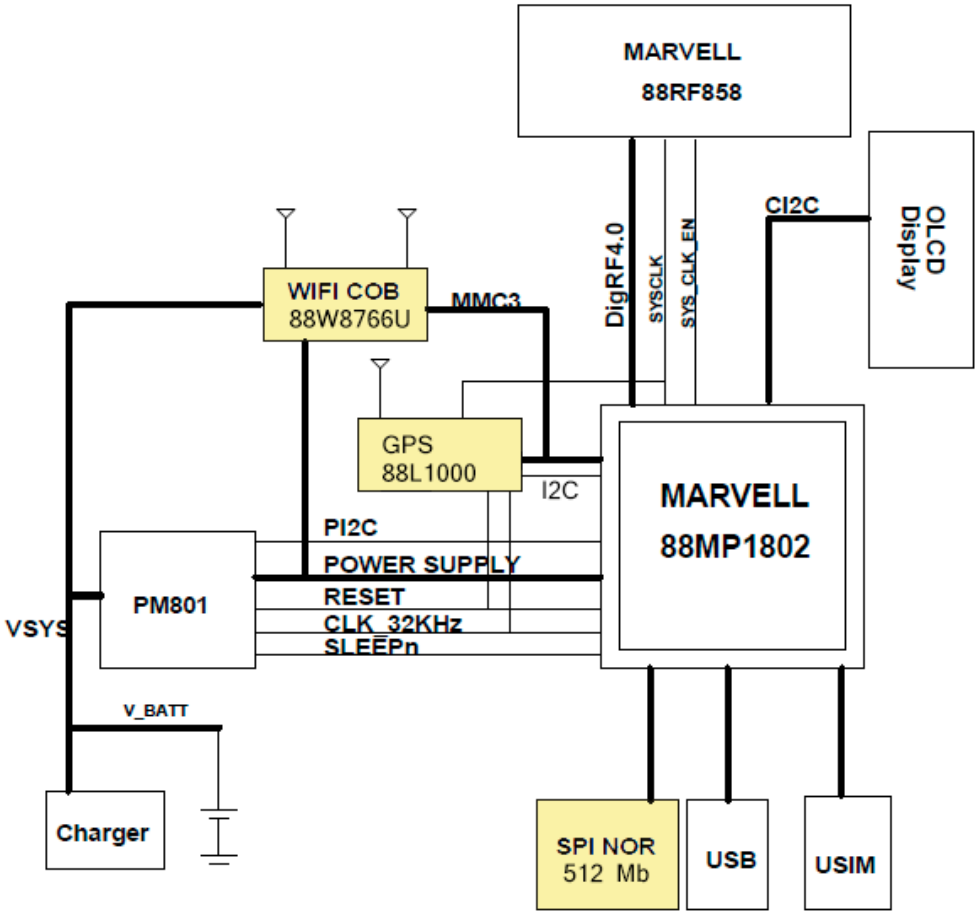
The SID SDK is aimed to be adapted in future versions to auto reconfigure itself inside a Smartphone or Tablet from a configuration as a **direct internet source** or a configuration as **no direct internet source** into a different configuration such as these two:

- Configuration as an **indirect internet host**, meaning no direct internet connection but has however an indirect internet connection and thus can function as an indirect internet host to other Smartphones with a SID SDK inside
- Configuration as a **no internet host**, meaning no direct internet connection but has however an indirect internet connection from an indirect internet host and thus cannot offer any internet to any other nearby Smartphones with a SID SDK inside. This is done to ensure reasonable internet performance to the shared devices.

And lastly but not less important is the specific case when WDa is not a Smartphone or Tablet but is an adapted MiFi Device User. Then the adapted MiFi Device with a “SID SDK” inside, is aimed to automatically share his internet with the Smartphone WDb “SID SDK”. Again, the MiFi Device (SID SDK” is aimed to limit the number of simultaneous Smartphones “SID SDKs” it shares internet with to 4, meaning these devices do not require any password from the MiFi Device and intended to share

automatically sharing internet in exchange for Tokens (Voucher credit points). This specific case has been illustrated last because to allow Users of the "**SHARE INTERNET DATA**" (SID) system to benefit from the automated internet sharing, it require the development of a modified hardware of a MiFi device to allow the Share Internet Data (SID) SDKs to operate as intended in the most recent filed pending provisional patent. Such hardware is aimed be development if sufficient funds are available from SID´s 2018 advance turnover (token sale) or from other revenues through Licensing or other funding ways through the MiFi manufacturer(s) themselves as to allow the completion of such development and hardware production, likely in co-operation with an Asian MiFi firm. In this way the supply is aimed to be more likely to be guaranteed to Users and prices are aimed to be competitive simply because the Asian or any such other firm is intended to be allowed to sell it globally.

A block diagram of the parts of a standard MiFi showing the additions on the hardware to accommodate the SID SDKs is shown here:



Single chip Wi-Fi – BLE, we recommend Marvell's: **88W8766U**

http://www.marvell.com/wireless/assets/Marvell_Avastar_88W8766U_SoC-001_PB.pdf

Single chip memory: Increase Memory by a minimum extra 128MB but we recommend an extra 256MB SID memory to be future proof, thus showing the SPI NOR 512 Mb.

Single chip GPS, we recommend Marvel's: **88L1000**

http://www.marvell.com//wireless/assets/Marvell_88L1000_product_brief_r4.pdf

Although the development of the MiFi with SID SDK inside would aim to open up a potential future revenue stream, the number of added Wi-Fi access points is negligible at a global scale and thus is of a lower priority to the key target of scaling the SID system Users. That can only be achieved by focusing on Smartphone's as the number 1 priority in the short term.

If going forward at a certain stage the revenue becomes critical to the future survival of SID, then we may reconsider, because the MiFi devices can be offered to SID Users together with a SID roaming SIM where only SID with its patent pending technology has the technical capability and novelty to share the internet from the MiFi with other smartphone Users in exchange for Tokens (Vouchers) BUT more importantly it is this next technical matter that affects the profitability:

The MiFi of SID would connect in priority to Wi-Fi access points of the SID network, where the passwords are stored on a SID network server. A regional number of passwords would be downloaded strictly through https command TLS encrypted and on top of that the payload would be extra protected with an additional 256 or 128-bit AES encryption of the payload.

By connecting in priority to a Wi-Fi when available rather than to a Mobile Network of the SIM, it reduces the cost of acquiring internet data from the traditional Mobile Operator whilst still charging for the internet shared with devices connected to the MiFi at the same rate as if the internet was originated by a Mobile Network. This means that of the percentage of internet megabytes consumed in any given month through the SID-MiFi device was say 20% Wi-Fi and 80% was from Mobile data then even if the price charged by SID to those who received 100% of that internet was at actual cost paid by SID to the Mobile Operator, still the margin to SID would be 20%. Actually, the margin is linear to the percentage of internet data crowd-sourced by the SID-MiFi directly through quality internet sources as a proportion of the total internet consumed. That margin can then be used mostly to pay for marketing vs. cost of organization. Such marketing would be to fund the online cost of acquisition to grow the SID system User base.

5.2 More detailed technical functionality explained

Furthermore, the SID SDK technology is designed such as to comply mainly with most recent pending patent, namely NOT to use a VPN Cloud-server and NOT to use the Smartphone tethering or hotspot function at all. Additionally, the security aspect when sharing internet aims always be high on our technical priority list. A top-priority as described in the embodiments and claims of the recent pending patent is to reduce power consumption to acceptable levels, such as a negligible power consumption of the SID SDK whilst not being nearby other smartphones with the SID SDK or when connected itself to an internet source. Actually, the consumption of the SID SDK as part of the Smartphone overall consumption when connected to an internet source and not nearby smartphones that request for any internet is described in such pending patent and tested to be negligible as it doesn't even show up in the smartphones consumption calculator feature.

Why are these so important?

Well to start, it was our Chairman´s view, that using a VPN Cloud—Based-Server (a server on the internet) could become an issue for certain countries, and so right he was because not so long ago at least 2 countries banned the use of VPN Cloud-servers which hide the actual internet resource accessed (website or internet address) by the PC or smartphone, namely from Russia and China.

Furthermore, as the SID Chairman has been in Telecoms all his life and wrote more than 15 patents in his career, it was clear that Mobile Network Operators would defend their traditional business model of selling as many different subscriptions as possible, even multiple SIMs per users. Again, spot on, as Mobile Operators try to sell users a different SIM for every single device, for example a SIM for each Smartphone (WDa to WDn), another different SIM with a different number for Tablet, another different SIM for a 3G/4G Watch with mobile connectivity (3G Pebble Smart Watch, Motorola Watch, Apple Watch ...). Not only that, but Mobile Network Operators also have the means to disable the tethering or hotspot functionality in the device where their SIM is inserted into. Here is a quote from Wikipedia "**On some mobile network operators, this feature is contractually unavailable by default, and may only be activated by paying to add a tethering package to a data plan or choosing a data plan that includes tethering, …** "un-quote. Here is the Wikipedia URL link and a few other ones for those who want to read a bit more about this.
https://en.wikipedia.org/wiki/Tethering

https://android.stackexchange.com/questions/47819/how-can-phone-companies-detect-tethering-incl-wifi-hotspot

file:///C:/Users/josem/Downloads/Procera_SB_Mobile_Tethering.pdf

In the SID app however, we opted for a higher transparency than the current status quo. Up and till today when a user activates the tethering or hotspot function inherent in each smartphone and tablet hardware, the user is not asked any question if the Mobile Operator or internet service provider allows such internet sharing. So, most users simply assume since the tethering function is available is there for their use at their discretion, whilst small prints of some operators specifically only allow the internet only for personal consumption. This of course has never been challenged and no precedent court case is known to us where any Mobile Operator challenged the use of the tethering function to share by users their own mobile internet with their friends and family and sometimes even with strangers. The same for home Wi-Fi where users simply give their home password to visitor's friends and family and even stranger.

However even going a step further multinational companies as Google, Facebook and a long list of many others actually make profit using the internet from users´ own mobile data and from users´ private home Wi-Fi and through their PCs, simply through massive advertising income, gaming income, etc.

SID has taken the internet service providers and mobile operators contracts serious and has implemented one more protection to those mobile operators and service providers, which they themselves do not implement in the smartphones and any such other hardware they sell to their own users.

- SID APP setting of sharing mobile data is default off
- **When a user activates that setting it is prompted to confirm it has such rights because only the User itself can check with the Mobile Operator or internet service provider (home Wi-Fi, etc.) if it is allowed to share internet through his own tethering function from the device supplied by his own Operator and consequently thus through SID providing the same function namely sharing internet.**
- If multinationals are allowed to create revenue and profits from internet paid by end-users to mobile operators and service providers than the same precedent applies to any other firm as a principle of law, which has been challenged in numerous occasions by mobile operators specifically in Europe BUT no precedent case where this was not allowed. The simple fact is even most employees and shareholders of mobile operators and internet service providers use at least one or more of the APPs

of those companies profiting from internet paid by end-users, in this case themselves, when using Google search, Facebook, Instagram, Alibaba, Amazon, WeChat and so many others.

Finally, the security of User data is even more important than battery consumption as that has to be protected at all cost. The SID SDK has been provisioned with quite a few security protections which we aim to explain herein after in more detail.

However, once the security matter is resolved than the power consumption becomes the next highest priority item as Users are very likely not tolerate high consuming APPs. Even less lately when Android operating system flags high consuming APPs and Users simply would uninstall an APP that consumes to much in their view, especially when they are not using the APP service themselves.

Having established that above points are absolute critical to SID and its Users now we can proceed with further explanation of more details on how our proprietary implementation resolves these issues or technical shortcomings.

5.2.1 VPN Cloud-server is not used anywhere in our SID system.

The simple explanation is this one. None of the SID system servers use any VPN Cloud-server, VPN remote server on the internet, as that is forbidden in certain countries. Instead we have developed a proprietary data communication on top of existing standard radio standards such as on top of Wi-Fi-direct, Bluetooth or BLE (Bluetooth Low Energy). The proprietary nature of the secure links between Smartphone's and Tablets is what allows us to ensure we comply with the following points, namely to:

- Limit the power consumption of those User's Smartphone devices that have internet to share.
- Maximize the security of any data exchanged between User's Smartphone devices.
- Comply with global laws, by not using any forbidden features as the use of VPN Cloud-servers.

The last point again is easy, Share Internet Data (SID) system does not use VPN Cloud-servers anywhere, whereas the other two points are resolved and explained in the following two paragraphs.

5.2.2 Tethering/hotspot functions of Smartphone are not used in any SID SDK.

This is very important in order to ensure our SID-system can't be tampered or interfered with by SIM providers in the smartphones or tablets. It has been achieved by the proprietary nature of the **secure links** or also known as secure channels that we developed in-house between Smartphone's and between Tablets. The proprietary protocol is technology independent as its mapped on-top-of existing radio technologies such as Wi-Fi-Direct, Bluetooth or BLE (Bluetooth Low Energy). This is important in that any future new radio technologies that may come along, the SID-system proprietary technology can be easily adapted and laid on-top-of those new radio technologies.

For the avoidance of doubt, the Share Internet Data (SID) SDKs and the "SHARE INTERNET DATA" SID platform, or also referred to herein as the SID system, is NOT a mesh system and has no relationship to Mesh at all.

One of the key aspects of the proprietary implementation of the SID SDK is that the Smartphone that has internet is basically NOT transmitting at all when it is not nearby another SID SDK that requests internet. Why? Well to solve the point mentioned in previous paragraph namely to "Limit the power consumption of those User's Smartphone devices that have internet data to share". This is critical as to incentivize Users to share internet with others on the same SID system, as that can only be achieved by limiting to an absolute minimum the power consumption of those Users that are so kind as to share their internet data, be it Mobile Internet data or Wi-Fi internet data, regardless if additionally, being incentivized by receiving Tokens (vouchers) for the actual internet Megabytes used. This is in fact completely the opposite of what the tethering / hotspot function in a Smartphone does, actually the Smartphone User with Mobile internet or Wi-Fi internet has to activate his tethering or hotspot with the corresponding massive amount of power consumption for the Smartphone User that is so kind to share his internet and consumes even if nobody is connected and even if nobody is nearby. Of course, that previous mentioned User has to verbally or in writing give his tethering / hotspot password to those he shares internet with, but that is unlikely to happen to all the people they don't know 24h a day and every day.

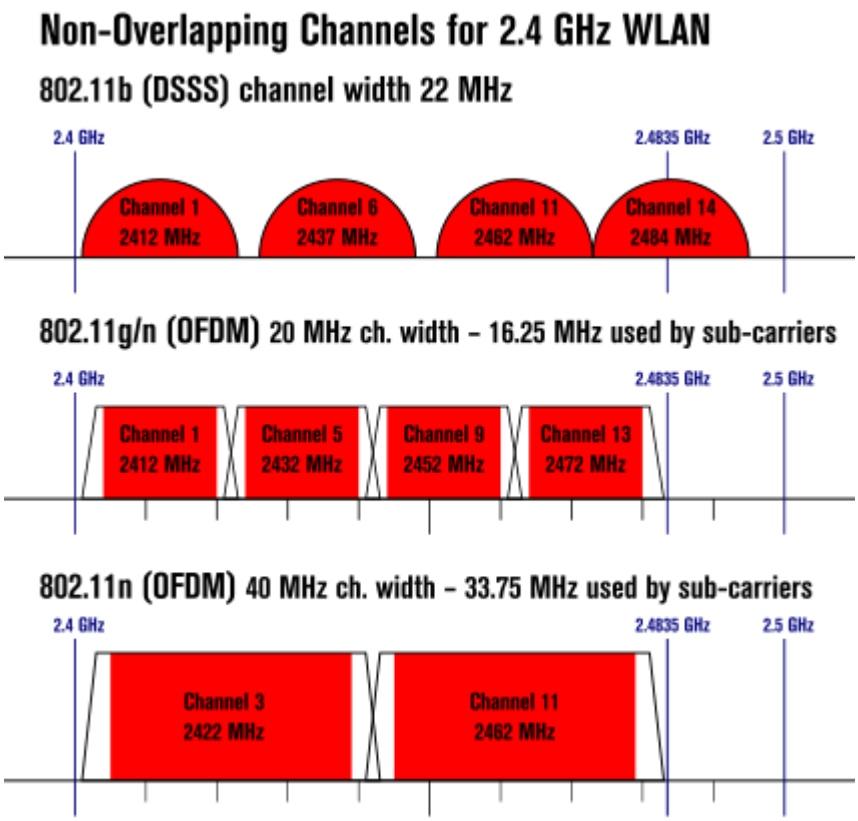
In short, nothing but negatives when using a Smartphone tethering / hotspot function from a user-friendly perspective: and to make it even worse, SIM providers have control to limit the use, disable or completely remove that tethering/hotspot function. With tethering the power consumption of the Smartphone that has internet source is continuous and thus unacceptably high, and last but not least: the security has been compromised by sharing his tethering / hotspot password with other people

that he may not even know well or not at all. All in all, tethering / hotspot features in Smartphone's are not the way to build a reliable SHARE INTERNET DATA system on, actually it is the worst one.

In our SHARE INTERNET DATA system, the **SID SDK** uses its own secure channel protocol with the necessary additional security measure and mapping the internet petition and content responses as payload within our secure channel. By doing it our proprietary way, **SID SDK assigns a super low power transmitter only to those Smartphone devices that have no internet,** regardless of the reason why they don't have internet. Such reason of not having internet could be, but are not limited to, having no SIM, yes having a SIM but no Mobile Operator coverage in some regions or certain indoor locations, no Wi-Fi password of nearby access points, yes Wi-Fi password but just at border or outside its coverage radius, etc.

In this way a SID SDK of Smartphone with internet when it doesn't receive any radio requests for internet transmitted from any other SID SDK of a Smartphone with no internet, then his power consumption is limited to the bare minimum power consumption as it is only in receive mode. This last is in real life the status most of the time in an average day. If however a SID SDK of a Smartphone with internet receives an internet access request from a SID SDK from a Smartphone with no internet, then both SID SDK initiate a proprietary exchange of authentication (**Signalling**) and select the available radio on both sides to SHARE INTERNET DATA through a different secure channel using a different radio technology with more power consumption to achieve radio range but also with a wide band transceiver such as Wi-Fi-Direct or potentially in future Bluetooth 5..

A typical order of events would be performing Signalling over a low power consumption narrow band transceiver on BLE (Bluetooth Low Energy) and once authenticated and encrypted exchange of the free radio channels, next radio password and the next channel encryption key would be shared encrypted and then both sides would exchange internet through a higher power wide band transceiver on Wi-Fi Direct or potentially in future Bluetooth 5. Another technical issue to resolve in crowded places is to ensure the least interference or free radio channels are used, in particular on the extremely crowded and most used 2.4GHz band devices.



This is particularly true on 2.4 GHz where Bluetooth, BLE and Wi-Fi and Wi-Fi Direct all operate on. However, that frequency band only has for US region 3 non-overlapping frequency channels, namely 1, 6 and 11 whilst most other regions in the world have 4 non-overlapping frequency channels, namely 1, 5, 9 and 13. Although these 3 channels are the worst case for the US, in real life those are the ones used by most hotspots globally. Those 3 channels (1, 6 and 11) are defined as non-overlapping channels, many Wi-Fi hotspots use every other channel in between, channel 2 to 5, channel 7 to 10, creating interference and degradation of quality on the neighbouring channels as they overlap. That doesn't give much flexibility when in crowded areas as the choice of which radio technology to use is dependent on the environment.

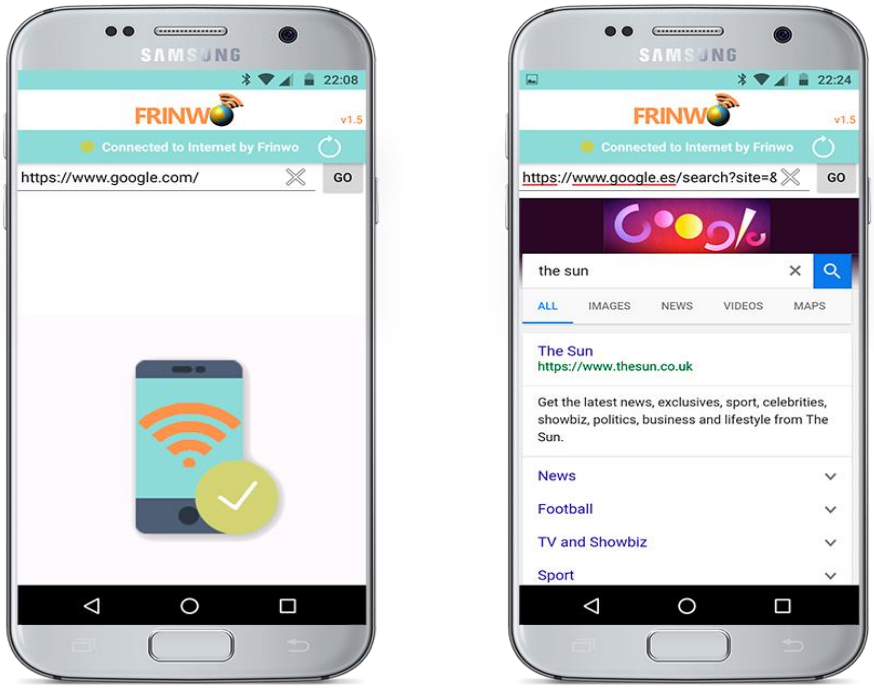
Channel	Frequency (MHz)	North America [6]	Japan[6]	[hide]Most of world [6][7][8][9][10][11][12]
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes

Channel	Frequency (MHz)	North America [6]	Japan[6]	[hide]Most of world [6][7][8][9][10][11][12]
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No	Yes	Yes
13	2472	No	Yes	Yes
14	2484	No	11b only	No

In the more recent 5GHz band there are a lot more non-overlapping channels; close to hundred actually (typically channel 36 to 165 depending of the region). Additionally, Bluetooth and BLE don't operate yet in this frequency band leaving all these non-overlapping channels available to be used for Wi-Fi or Wi-Fi Direct ensuring high quality of service even in dense areas where many

Smartphone's and/or Wi-Fi hotspots would be sharing the same coverage area but not the same channels. This is why Wi-Fi Direct is the preferred option to share the internet payload to nearby Users simply because Bluetooth 5 is not yet allowed on the 5GHz band. The SID SDK aims to select a free 5 GHz channel if available on both sides as established during the Signalling exchange (takes typically 10 to 15 sec) and then once connected the power consumption is tan intended in future also be managed mainly in the 5GHz band between SID SDKs reducing it down to such a level where the quality is still sufficient. If the first 2 devices that connect don't both have 5GHz transceivers then the SID SDK aims to reconfigure the Smartphone automatically to use the 2.4 GHz as that one is always available on all smartphones. The transceiver output power in future is aimed not only to be checked against the RSSI (radio signal strength indication) received on the other side but also aims to use the checksums, as when those fail then the power is put a notch higher. The overhead needed to ensure the secure connection is mandatory as to ensure the communication channel between SID SDKs through the Smartphone is secure BUT additionally the payload, meaning the actual shared internet data is submitted through several extra security checks;

- When integrating the SID SDK in our own SIDAPP or in a 3rd party LICENSEE App, the future update of the SID SDK can be put in debug mode and detects in that mode any non https communications originated by the APP where it is integrated in. This was done to ensure during design all the non-secure communications are replaced by secure https ones.
- The SID in-App browser ***always aims to send any command out in https*** regardless if the users enters it in the URL or not.
- The internet data passed as payload through the proprietary secure channel of the SID SDK between nearby smartphones can be filtered at the petition level and additionally protected by encrypting it with an additional 128 bit AES encryption.



An example of the previous mention of the filtered internet data can be understood as follows. Any internet access by a User of a Smartphone is filtered and checked against pre-set criteria. For example, does it have a valid Licensee of the SID SDK and which 3rd party APPs are allowed to receive internet because our SID SDK may allow ALL Users certain minimum internet access without exchanging those megabytes for any Tokens, be only through the SID SDK in-App browser. In this way even in emergencies any User with no internet access nearby another User with internet access could in future be able to browse the web, be it at a limited speed and only through the in-App browser. There are no restrictions whatsoever of which websites can be accessed through our in-app browser other than that they are performed in https and other then any network restrictions in certain countries in line with local legislation, but not any different then as if accessing the internet not through the SID SDK if the devices had direct internet access.

5.2.3 Protecting Users' data and payload.

The utmost care has been taken on securing the protection of all Users' data, accessed data on the internet (payload) and our own companies' data and intellectual property.

In this respect let's go step by step; firstly, the User's data is treated identical to the companies' data, meaning the same protection levels are applied on a multiple level. Firstly, all communications into and out of the SID SDK are only done in the secure protected method https already today in the released SID APP, whenever possible also TLS is recommended to be applied by websites themselves as an additional encryption level by any 3rd party accesses attempt. The SID SDK encrypts all communications between smartphones BUT on top of that also the payload that contains the internet petitions and internet responses are encrypted with an additional 128 bit AES encryption. This means that all Users' data and company data has a minimum of 2 and in some cases 3 protection levels, one on top of the other.

As for the Company data stored remotely, in a secure server or on a Blockchain custodian, such as the Wi-Fi network passwords get the same protection treatment when communicating with remote secure servers. Those data may include, but are not limited to, Wi-Fi network passwords, country, precise location, altitude etc. And those are stored encrypted BUT more importantly they are protected even when any part thereof is transported outside our secure servers or outside our secure SDK, again applying the same protection levels: https only and TLS when possible and mandatory minimum 128 (or 256) AES encryption of the payload on top of the previous.

Next is the protection of data and payload exchanged between nearby Smartphone's or Tablets through the SDKs. Here it is important to notice that there is already an inherent security layer in the underlying technology of the radio transport medium, for example;

. BLE (Bluetooth) uses as per their standard the 128 AES encryption with counter mode CBC-MAC with adaptive frequency hopping, Lazy acknowledgement protection method, 24 bit CRC, and 32 bit message integrity check.

Wi-Fi Direct (Wi-Fi) uses as per their standard the 128 bit WPS / WPA2 security and encryption standard (AES) – CCMP as cipher & TKIP and a randomly generated pre-shared key (PSK) for mutual authentication. Some newer hardware models already start using the next generation WPA3 which is a lot more secure than WPA2.

Regardless of all the above protections inherent in the transport medium standard, SID adds additional protection layers on top. In this respect any data exchange between Smartphone's through:

- BLE (between nearby devices) is coded at transmission points and decoded at receiving points thus creating a proprietary secure channel. Coding/Decoding is then complemented by on top of that

adding a 256 bit AES encryption, likely to be updated 128 bit AES to reduce power consumption, of the payload (the actual valid data info exchanged is called the payload).

- Wi-Fi Direct (Wi-Fi between nearby devices) is coded proprietary based on TCP-IP, and could have in future a triple protection of which the last is optional (as to allow the Licensee to decide trade-off between extreme increased security and power consumption increase per extra security addition). Only https when possible recommend TLS at servers side, and an extra 128 AES encryption of the payload (the internet requests and responses are considered payload with some overhead data), and an optional extra third protection in the form of a proprietary firewall at Smartphone device with internet source. This means that even if the internet source is compromised, still the data to and from the SID SDK accessing the internet between smartphones is fully secured.

Let's analyse this previous statement for a brief moment, "even if the internet source is compromised", really? Well the internet source is typically one of these two, mobile internet from a Mobile Network Operator or a Wi-Fi access point. The Mobile Network Operator transport mediums are too many to list, but just to mention a few, GSM 3G/4G/5G, PCS, WCDMA, etc. And none of the Wi-Fi standards encryptions and authentication methods used have been known to have been compromised or hacked since its inception. So, encrypting the payload when we communicate through shared internet from mobile network internet source seems like overkill but as we say better be safe than sorry. The Wi-Fi transport mediums are a smaller list, but to mention the most relevant, IEEE 802.11, 802.11a, 802.11b/g/n, and 802.11ac, and very latest hottest new Wi-Fi standard 802.11ax. Again, none of the Wi-Fi standards encryptions used have been known to have been compromised or hacked since its inception BUT during early 2017 the authentication method was compromised by a Belgium hacker Researcher of the University of Leuven. For those interested in more about that specific hack here one of the many articles on that subject: https://www.forbes.com/sites/thomasbrewster/2017/10/16/krack-attack-breaks-wifi-encryption/#19cb0e302ba9

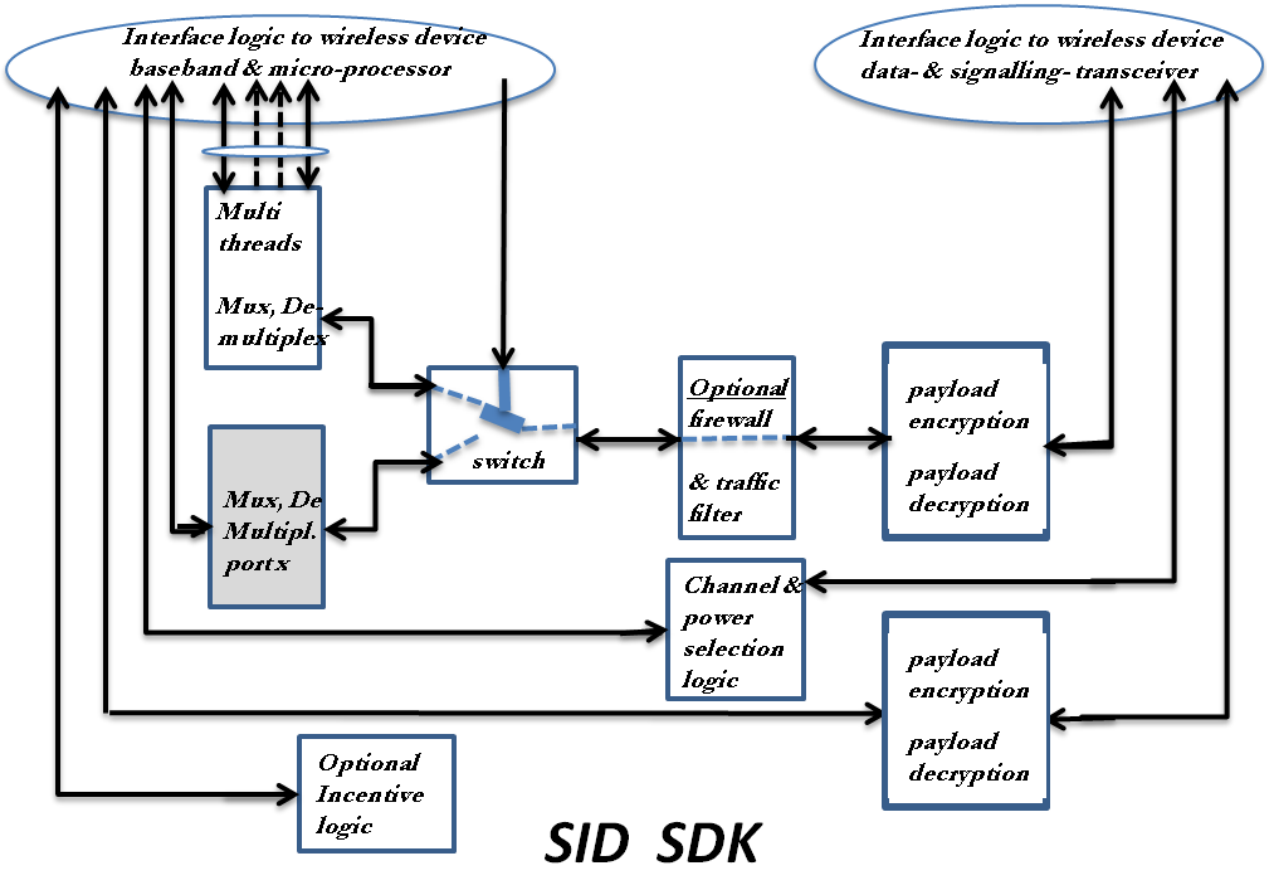
The vulnerability exploited was an inherent weakness in the actual standard on the handshake method where a key that should never be re-used is allowed and thus allowing to enter onto the Wi-Fi network without even having entered the password of that Wi-Fi. This is very disturbing and most dangerous because once a hacker is on the Wi-Fi network, he or she can sniff all the information that passes through that Wi-Fi and more worrying is that it could access sensitive information connected to that internal Wi-Fi network. According to certain news releases this hack method was affecting

around 60% of total global Wi-Fi access points / hotspots at that time and most Android Wi-Fi Smartphone's and Tablet. In reality the Wi-Fi access points are the ones to worry about because those can only be made secure again by installing a firmware / software patch closing this security loophole. This vulnerability is likely to remain at a very high number of global Wi-Fi access points simply because most don't have remote auto-update software feature and thus requires a person connecting a PC and manually installing a patch update. That, we know will most likely never happen on all global hotspots, so that security breach will remain there in installed base models for years to come until they are replaced by a newer model. As for Google's Android a vulnerability like that is quickly resolved and provided as a security system update of their operating system for which users don't have to do anything, simply it auto-updates smartphones and tablets alike, so problem resolved reasonably quickly. The same applies for mobile APPs they are simply updated quickly with fixes. So, encrypting the payload when we communicate through shared internet Wi-Fi network internet source seemed like an overkill when we started but right now we are glad we introduced the extra safety precautions, as we say "better be safe than sorry".

5.3 Provisional patent protected implementation charts explained.

The following block-diagrams and flow-chart forms part of our Chairman´s provisional patent protected representation of the implementation of the SID system. The key part of the "Share Internet Data (SID) top-level system" as shown in previous point 4.1 is actually the Smartphone software module referred to therein as "Proprietary Module". That software module is actually the integration of one or more of our SDKs inside that "Proprietary Module", as described before in "SID project overview". The core of the technology is in the **autoWiFi SDK** and **SID SDK**; however, the more novel technology is actually in the SID SDK.

In the following diagram, we show the actual embodiment implementation that we have software coded in our released SID APP, following the registration of the provisional USPTO patent Application Number 62588951. The individual parts of the diagram have already been coded and tested on their individual functionality and full integration of all parts as a single SDK is completed and implemented in the 1st commercial SID APP release of 6 February 2018.



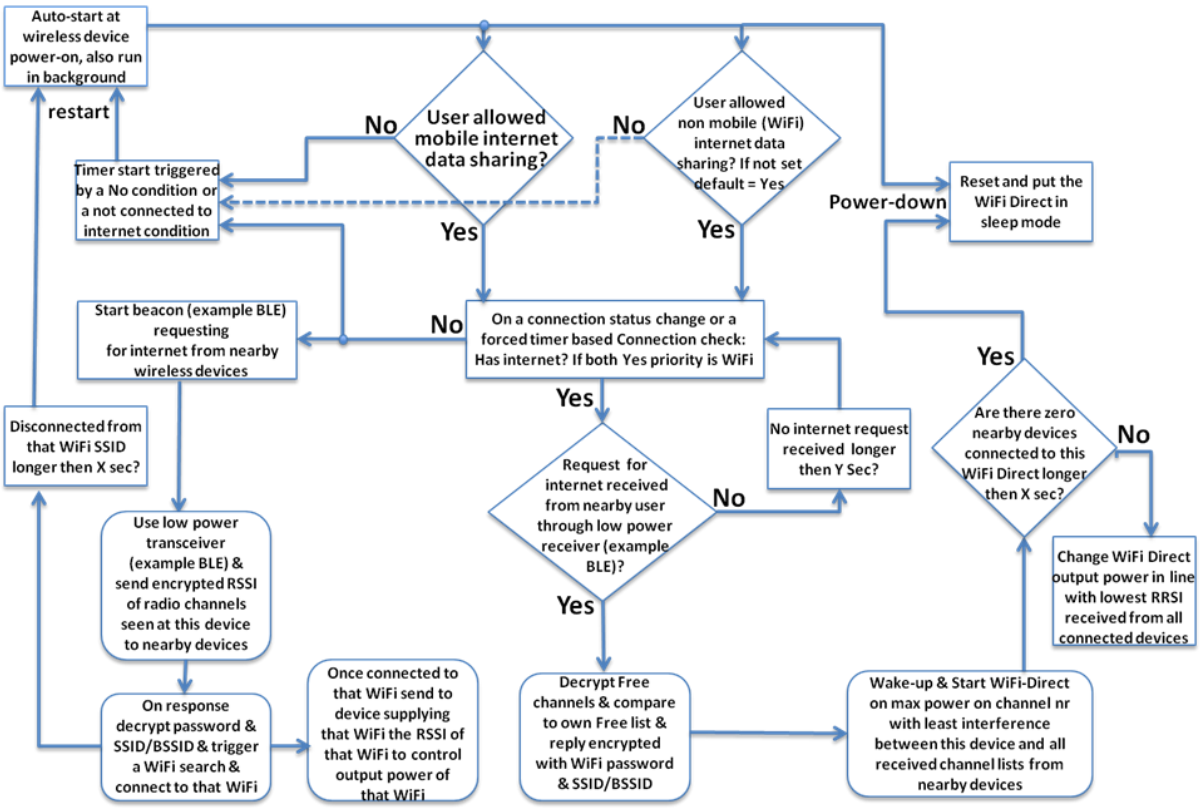
The SID SDK, handles the core function of activating or de-activating a signalling channel or an internet payload data channel. A particular novelty is that in the above SID SDK by monitoring the past historical internet domain searches for certain domains, after a power on of the device or after an exit of flight mode of the Smartphone with our SID SDK inside. When a domain such as **google.com/** is detected than that URL redirect response is used to determine the country or region of the actual current or last used internet connection. If such past domain response was not available or not recent enough than the SID SDK with a direct internet connection requests for example an https://google.com/ internet petition and the response analysed as to extract the country/region from an internal table mapping. As a matter of illustration, if the response has in the redirected received URL address (uniform resource locator) somewhere the following content "google.co.jp/" than the country where the Smartphone connects to the internet is Japan, but if the response includes "google.be/" than the country is Belgium in Europe. However, if "google.com/" detected by the SID SDK is in the response URL than that is considered as an internet access through a USA internet connexion or any such regional/countries domain owned by Google Inc.

A real life different example that we tested with the SID SDK, was making an internet request to https://www.google.com/ and receiving this real test response

https://www.google.com.gi/?gws_rd=cr&dcr=0&ei=ahsPWqCdCIKla-XkmpAN and when the SID SDK compares all the Google Inc. owned domains and corresponding country table, finds only one match with “google.com.gi/” meaning the country from where the internet was accessed was Gibraltar.
This is the complete list of all domains owned by Google Inc. as extracted on 17th November 2017 from the internet from this URL:
https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/List_of_Google_domains.html
With the country or region now fully resolved, our invention in this embodiment when the region/country detected is the USA, limits the number of channels used by any of the Smartphones’ non-cellular or non-mobile transceivers, for example Bluetooth, BLE, Wi-Fi, Wi-Fi-Direct, aims to be channel 1 to including channel 11 when in the condition that the Smartphone is configured by the SID SDK to operating in the 2.4Ghz band. If, however the region/country detected is Japan then channels used on the 2.4 GHz aims be channel 1 to including channel 13 whilst in the event of Wi-Fi 802.11b additionally channel 14 could be allowed. If, however the region/country detected is not USA and not Japan then channels used on the 2.4 GHz aims to be channel 1 to including channel 13.

Alternatively, in a different embodiment, if the region/country detected is not USA, meaning not detecting “google.com” nor “google.com/”, excluding any URL response with “google.com.” where the extra dot refers to other countries different then the USA, such as “google.com.ar” for Argentina or “google.com.au” for Australia and so forth, then channels used on the 2.4Ghz aims to be channel 1 to including channel 13. This last improves outside of the USA, for the rest of the world, the radio interference robustness of our SID SDK compared to competitors in the amount of 13:11= 1.18 times (an increase of 18% more robust to radio interference) and the same amount 1.18 times increasing the statistical limit before saturation of all the channels would be reached and consequently the same 1.18 times increase of the number of Smartphones that can operate in the same 2.4Ghz band before saturation or too much interference of all channels is reached.

The next drawing is a software flow chart that we are following as guideline as it worked quite well during our individual parts testing of our SID SDK and currently under coding and integration with the rest of the parts that make up the SID system.

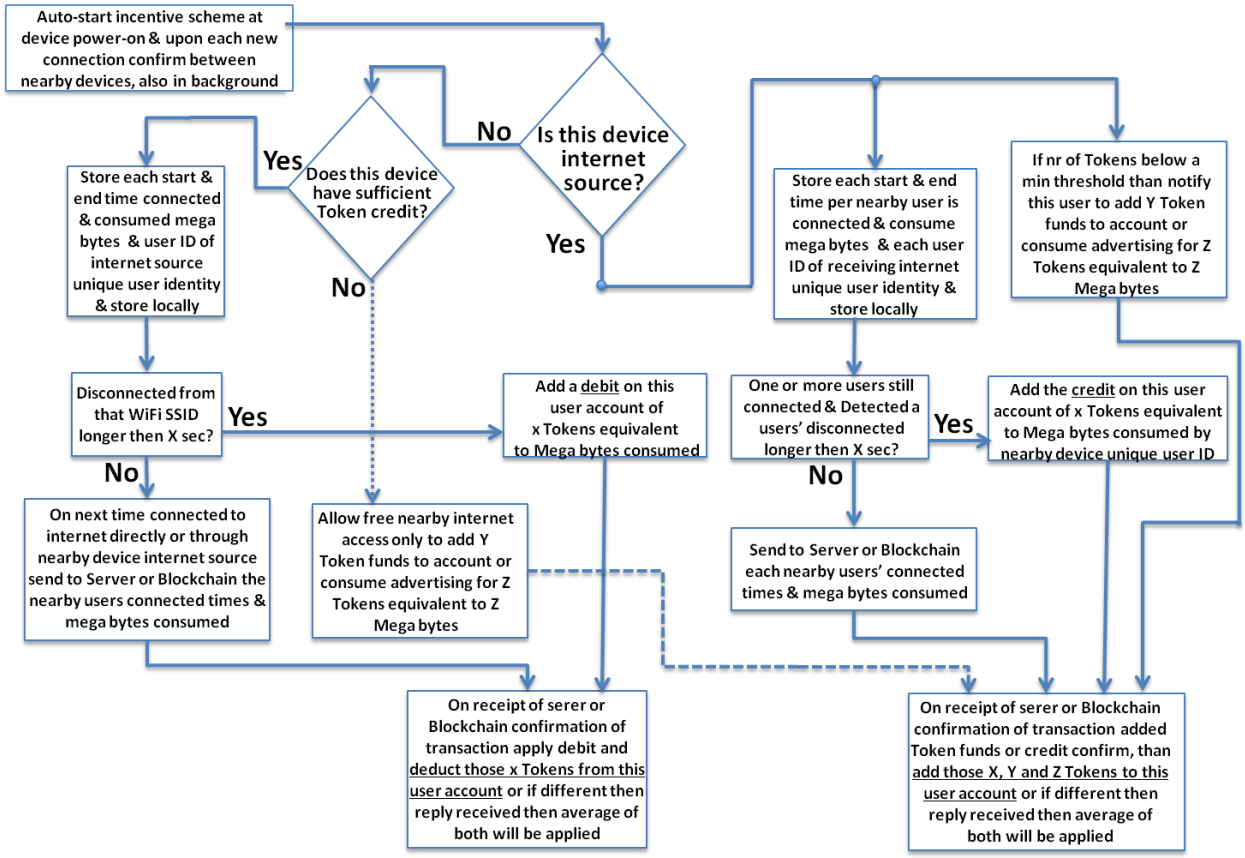


SID SDK software flow chart

The software flow chart is self-explanatory however it is important to draw the attention that for Smartphone or tablet power consumption considerations, the flow chart used in the SID SDK uses at least 3 different radios (transceivers). A first radio is the one connected to the internet source, which can be a Mobile radio transceiver (3G/4G/5G WCDMA etc.) or a Wi-Fi transceiver connected to a Wi-Fi hotspot. A second radio is used for signalling channel (low power narrow band transceiver as a BLE) to keep power consumption at the device with internet when nobody is connected to virtually negligible as is only in receive mode and at the side of device who needs internet at ultra-low around 0.1% or less battery power consumption per hour to send internet requests until a nearby Smartphone responds. A third radio that only activates after signalling is in range at the Smartphone that responds he can share internet and that device switches to 2.4Ghz if both have 2.4GHz only, a Bluetooth or a Wi-Fi Direct which are higher power and wide band transceivers. However, if the Smartphones sharing have 5GHz band available to both than only the Wi-Fi Direct transceiver is activated to share internet at 5GHz by encrypting all internet petitions and responses between Smartphones. To reduce the power consumption to an acceptable level during the time period devices are sharing internet, the smartphones with no internet , and which had send prior through the second radio signalling (BLE) the free radio channels list, the RSSI (radio level) it receives the

transmission of the Smartphone with internet and with that and other parameters the Smartphone with internet reduces the output power level of his transceiver radio (i.e. Wi-Fi Direct) to the minimum needed to still ensure a good reception and data quality at the other smartphones connected to it. With this previous mentioned embodiment, it means that the power consumption of our SID SDK invention, compared to competitors, SID can in future updates reduce further battery power consumption during internet sharing period according to our testing results between 20% and 80% depending if the nearby smartphones are far away (10 to 70m indoor/outdoor) or close by (1 to 10m).

The below is a software flow chart of the SID system incentive scheme. The SID system is formed by the SID SDK in Smartphones and the incentive scheme implemented between the SID SDKs and the SID Servers and the Blockchain custodian.



SID system Voucher/Token incentive scheme flow chart

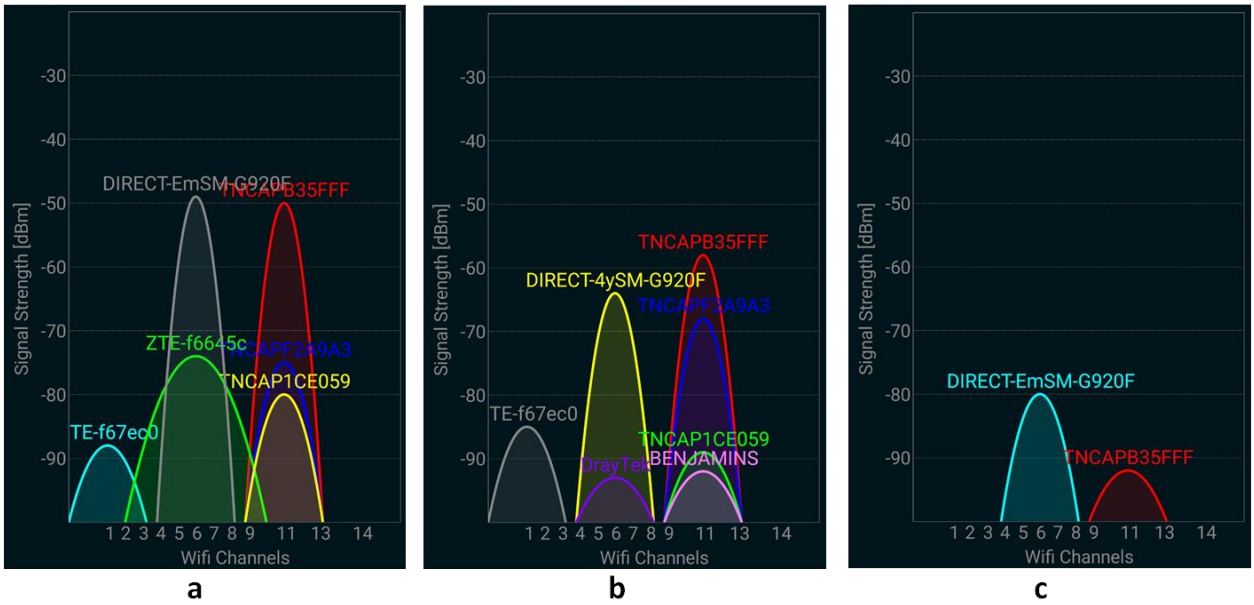
The above software flow chart describes a different embodiment of the "optional incentive logic" of previous block diagram of the SID SDK, showing our preferred implementation in the form of a flow chart "SID system Voucher or Token incentive scheme flow chart". The flow chart is self-explaining

with the text inside each box when following the diagram from the starting function “Auto start” at the top left and following the direction of each arrow. In our software coding work, the incentive logic of paragraph 4.1 and shown as a flow chart here just above is an integral part in the Proprietary Module or in other words in the SID SDK and the SID server.

The incentive logic is restarted at least at each of the power-on of the Smartphone or tablet and at each connection confirmation between SID SDKs of nearby Smartphones. Than the logic follows one set of the logic if the SID SDK detects that it has a direct internet connection or a different set of logic if no direct internet access is available. The rest is quite self-explanatory.

5.4 Provisional patent wide band transceiver (Wi-Fi-Direct) test results

There is no better way to understand this specific implementation part of one block of the SID SDK other than looking at the actual test results of the measured radio signals received from a frequency analyser monitor device during the time whilst two smartphones share internet.



The previous measurements correspond to this test set-up: Smartphone 1 with direct internet and a nearby Smartphone 2 without direct internet. After Smartphone 1 receives signalling request asking for internet from Smartphone 2 and Smartphone 2 sends back that he has no 5Ghz band transceiver so only 2.4GHz is possible and the list of least interfering channels in order of most free to least free.

In the screenshot (a) the free channels send by Smartphone 2 to Smartphone 1 were in this order: 6, 1 and not 13 as we were simulating USA region. Also, the RSSI signal of the BLE signalling level received by Smartphone 1.

Smartphone 1 has internet from Wi-Fi hotspot with SSID “TNCAPB35FFF”, such hotspot transmitting on channel 11 of the 2.4GHz band AND Smartphone 2 does not have the password of that Wi-Fi hotspot. With that, Smartphone 1 responds to Smartphone 2 with the BSSID or SSID of the Wi-Fi Direct and the password in encrypted form. Then Smartphone 1 starts the Wi-Fi Direct transmissions, with SSID “DIRECT-4ySM-G920F” at radio channel 6 because that one is the common denominator least interfering channels on 2.4GHz band and then Smartphone 2 connects to that Wi-Fi called “DIRECT-4ySM-G920F” with the password he decrypted and sends the RSSI level of that Wi-Fi (DIRECT-4ySM-G920F) to Smartphone 1 at regular times to adjust the output power lower because the RSSI received is very strong, see screenshot (a) RSSI higher than -50dBm.

In above test screenshot (b) Smartphone 2 you can see the output power of Smartphone 1 Wi-Fi (DIRECT-4ySM-G920F) is lower because now the RSSI received by Smartphone 2 is below -75 dBm.

Now we move Smartphone 2 away from Smartphone 1 indoors to a next room 10 meter away with a door and a wall in between such that the RSSI drops to below -95dBm and the output power of Smartphone 1 is set to maximum such that now the RSSI received at Smartphone 2 is at -80 dBm and sufficient good enough to still receive good quality internet. Remember that at this point Smartphone 2 even if it had the password of that Wi-Fi hotspot “TNCAPB35FFF” it would not work properly because at – 95 dBm the internet quality is being degraded quite a lot but through the internet sharing by Smartphone 1 who is between Smartphone 2 and that Wi-Fi hotspot “TNCAPB35FFF” the internet quality is acceptable.

6 SCALING THE BUSINESS

6.1 Overview of the business scaling model

The Share Internet Data (SID) business beyond a Token sale, is summarised herein this section of this Whitepaper. Whereas the crypto & fiat monies received from the Token sale of the up and coming ITO (Initial Token Offering) is intended and to be understood as payment received from SID Users as advance payment or pre-pay on a Token (Voucher) for consumption of internet sharing through the SID system, so basically its turnover even if the consumption by the User on the SID platform is at a later date. The consumption by the SID users is aimed to be allowed to tart a few months post ITO coinciding with the moment the SID app interface to the blockchain to trade Tokens for shared internet Megabytes is activated and consolidated at each SID user Wallet.

As in any other normal business, turnover is here used in the same way namely to cover the cost of the service provided as well as for the overall costs for the running of the business.

Actually, the percentage to cover the costs of organisation is a relatively smaller portion of the overall spend compared to the bigger spend being the marketing spend, defined mainly as the CoA (cost of acquisition of new SID Users).

Coming back to the essence, the scaling of the business is aimed to be done in phases. An alpha test has already been performed at a small scale in 2017, with several tenths of thousands of real end-users. We did it in two ways, by using an old chat APP that we had acquired from a third party who discontinued their APP-Server service and replacing it with our own alpha test APP with both the very first ever **autoWiFi SDK** inside without any chat function. The original old discontinued 3rd party chat app had over 300,000 (three hundred thousand downloads but less than 40 thousand active end-users but very skewed to the Asia region and many in Philippines. As such we didn't use absolutely anything from such 3rd party discontinued app other than the app re-naming for the alpha test only, no code whatsoever as the only interest was in using the existing customer base for an initial alpha test of our own autoWiFI SDK wrapped with a user interface around.

This was expected to very likely upset initially all those existing users, but since the chat service was going to be stopped by that 3rd party anyway there was nothing to lose by trying something new in an aggressive way. Namely the "discontinued 3rd party App" was updated in June 2017 as the "discontinued 3rd party App name adding Frinwo behind" App where inside was no chat function at all but rather the auto connection to Wi-Fi access points and sharing internet with nearby Smartphone's at a very early experimental code phase. As expected over the weeks following the updated over half un-installed the APP but some small percentage of new end-users downloaded the APP and we got an amazing amount of incredibly valuable feedback from the remaining end-users. This was accompanied by small social media campaigns to drive some uptake to that alpha autoWiFI App in order to also test the reactions on social media BUT more importantly to get the initial figures on Cost of Download (those who simply downloaded the app) and Cost of Install (those who interacted at least once with the app and accounted for as an install). The Cost of Acquisition (CoA) was obtained as different figures depending on the online marketing social medium used, for example paid banners adds on Facebook, Twitter, Snapchat, Google Adds, etc.

Than we started with a different Beta test with a different APP called "**Frinwo**" still leaving the previous alpha test App called "discontinued 3rd party App with Frinwo name behind" APP active but updated to exactly the same code as the "Frinwo" APP. The combination of both APPs has provided for just over 20,000 (twenty thousand) alpha plus beta test end-users for which we had concluded the testing and data recollection phase after the summer of 2017. Several small new online marketing campaigns were executed, only for "Frinwo APP" over a few months period to test out different marketing messages, different banners, etc., different channels in Facebook, Twitter, Snapchat, Google and direct email marketing contents to verify or update the assumptions in this Whitepaper to grow and scale the business. For this last beta test, an **"iOS autoWiFI App"** was also released with the **autoWiFi SDK** inside as we had no time to complete development of the core SDK at that time after the summer of 2017.

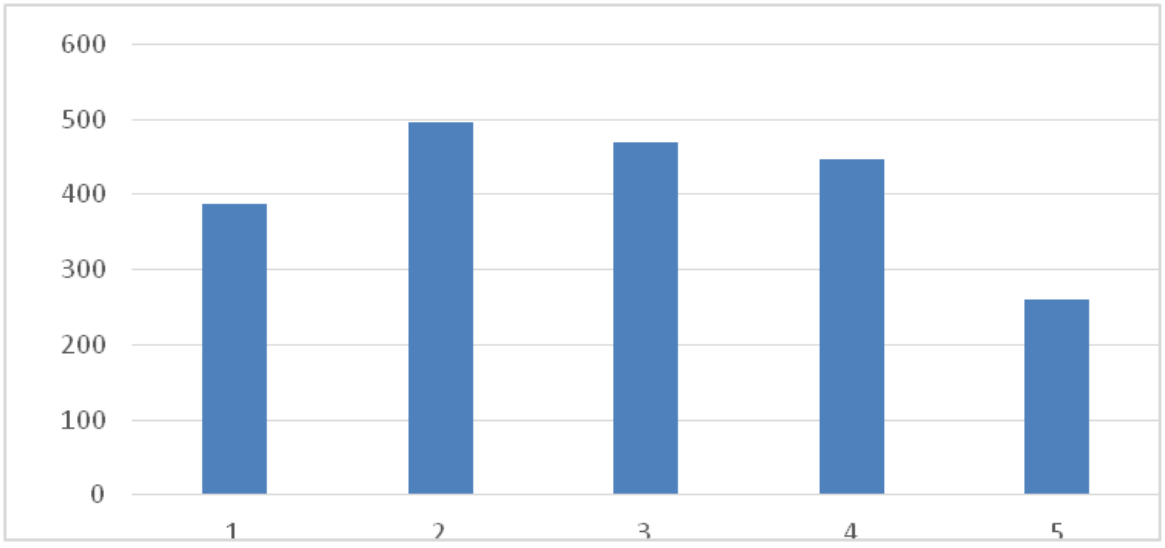
The initial results were as follows:

. Just over 4 thousand new downloads on Frinwo APP with just over 2 thousand active end-users whilst without targeting the other APP "discontinued 3rd party App with Frinwo name behind" it grew almost with the same amount to just over 25 thousand end-users. We believe it to be due to the appearance of the word Frinwo in the app name of both and to the fact that Google has an App called "Google Allo" with over 10 million downloads and again the word "Allo" that was

also in the alpha test app name is common so it is likely it drew some unintended but welcome new end-users to our alpha and beta app “discontinued 3rd party App with Frinwo name behind”.

By 30th December 2017, the test APPs were re-named in preparation for the official commercial product release version, due by the end of January 2018, as follows:
“Frinwo” APP was removed from the stores to avoid confusion of having more than 1 app with the same function and identical look inside.
“discontinued 3rd party App with Frinwo name behind” was renamed to “SID” on PlayStore and newly created as “Share Internet Data” (SID) on AppStore.

The commercial release versions of SID were uploaded to the stores on 20th January 2018, pending approval by Google and Apple respectively to be published on their stores. Although the formally announced release date with the initial early failure bugs fixed was 6th February 2018.



. Google - Frinwo Play Store visitors, over a 5 day period during the post summer 2017 Alpha test.

Marketing Campaign			**Platform**	**Impressions**	**Clicks**	**Cost per click**	**Cost per impression**
Brand Awareness			Instagram	123 245	119	0.13 €	0.001
			Facebook	36 877	33	0.48€	
				Total: 160 122	Total: 152		
Page post engagement			Instagram	267	66	0.28€	**0.002**
			Facebook	12 323	30	0.30€	
				Total: 12 590	Total: 96		

. Marketing campaigns performance, over a 5 weeks period in our Alpha test.

Instagram, in our particular marketing messages used, offered a better visibility in terms of impressions and better user interaction than Facebook.

Cost per visit	Cost per conversion
0.35€	**4.37 €**

. Marketing campaigns conversion rate, during a 5 day period in the Alpha test in Europe.

The alpha test marketing campaigns were focused to generate traffic only to Google Play Store as the Android version of the app was the only one available by the time the first campaign started and only during the campaign was the iOS version uploaded. We aim to account for an average online cost of acquisition per User starting at 1.14 EUR (1.37 USD, 1.03 GBP).

The visitors in the Google Play Store during the above shown specific 5 day Marketing Campaign are roughly 18% of the total amount of visitors in the alpha testing period of 5 weeks. With this very small marketing exercise we have generated insights about which markets have better response to the

Frinwo test APP at the time (basically the SDKs). The main goal of this exercise was to find the issues early on to streamline the R&D work to resolve those marketing and product issues in order to reduce the cost per visits and consequent CoA by targeting only those markets initially in which we appreciate an appropriate end-user's engagement. Once the CoA has been identified, then it becomes crucial to add the improvements to the product and marketability issues inside the Beta version APP and server design as to accommodate these things that contributed to a negative impact such that the next commercial runs smooth.

With the app improvement with the identified fixes for both Android and iOS the future updates are to consider to minimize the current difference between the cost per visit and the cost per conversion. As Instagram is owned by Facebook, the spending in advertisement through both social networks is intended to be considered as the same marketing medium. Twitter however is a totally different social network which functions, in our case, only to extend the brand awareness and its online presence as the advertising on Twitter tends to be more expensive and it resulted during our alpha and beta testing in lower conversion rates, so the marketing spend in this platform going forward is aimed to be the lower percentage of the overall marketing spend.

The email marketing is a medium which was tested only at a lower volume scale and thus is not really representative at this moment during the alpha and beta tests, so the conversion rate can't be calculated based on facts for this medium. In any case, according to Mailchimp figures published on 1 February 2017, in the Software and Web App "Business and Finance" Industry the Open Rate (impressions) is about 20.97% and the Click Through Rate is about 2.73%. (https://mailchimp.com/resources/research/email-marketing-benchmarks/). The average cost for sending 100.000 emails per month was about 30 € which results in 0.01 € cost per click.

However, an amazing thing happened during our initial alpha testing where one of the marketing data collected with end-user permission is the emails of the contacts in order to use for future marketing campaigns. These resulted so far, as of the end of the marketing campaign, in a database of several hundred thousand of emails which can be used to test the direct email marketing medium in our next large scale commercial test post commercial release. We expect in the coming months the number of our email database to grow slower because in a commercial release we only collect the user google account email and not all his contacts emails as for that we need a feature as chat to justify it in the future. Once chat is included in the future we expect quickly to collect over 2 million emails, mainly due to the Dunkin Coffee APP and our own SID APP users, once we jointly find a reason

to extract the contacts emails, assuming the average emails per downloaded APP to contribute to be avg. 8 X 250,000 = 2 million plus the few hundred thousand we already have of our alpha and beta tests.

Also, the different marketing channel efforts focused on direct marketing and influencer marketing is more controllable in that it provides almost real-time cost of acquisition and the conversion rate can be measured on the go, taking into consideration the results which are aimed to show their effectiveness.

It is our intention, provided the EUR 80 million is obtained to fund the first three years of our Business as advanced turnover during a Token sale, to scale the business to around 40 million downloaded app users' installs in aggregate by the end of the 3rd year post ITO.

6.2 Monetisation Models considered for the SID business scaling

(i) SIS Advertising Model

Traditional business advertising models, before the blockchain tokenisation era, were based on two parameters: ARPU (Average Revenue Per User) and ARPDAU (Average Revenue Per Daily Active User). The main objective, back then, was to get a high enough ARPDAU to account for as business revenue as the sole value creation method.

Our SID business model however is a "sharing economy model", as a matter of speaking like UBER with sharing taxis but SID with sharing internet data, where Share Internet Data (SID) value creation is aimed to be obtained by the following three things:

. A percentage of the revenue to those SID users who shared their internet Megabytes

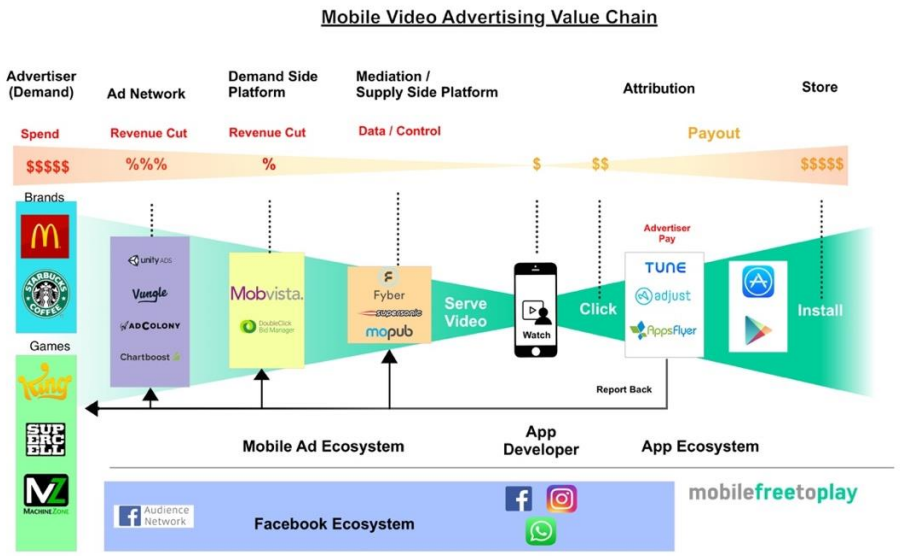
. A percentage of the transaction on the SID eco-system (SID platform).

- Company valuation is aimed to be defined in future, in our view after a critical mass of 100 million active yearly users has passed, as the average of the two previous points = sharing economy ARPU per SID user per year multiplied by the number of different active yearly users.

(ii) Advertising Value Chain

Advertisers pay APP owners to show ads to users that drive revenue for the advertiser's´ clients. Therefore, the more ads our SID users consume the bigger our revenue.

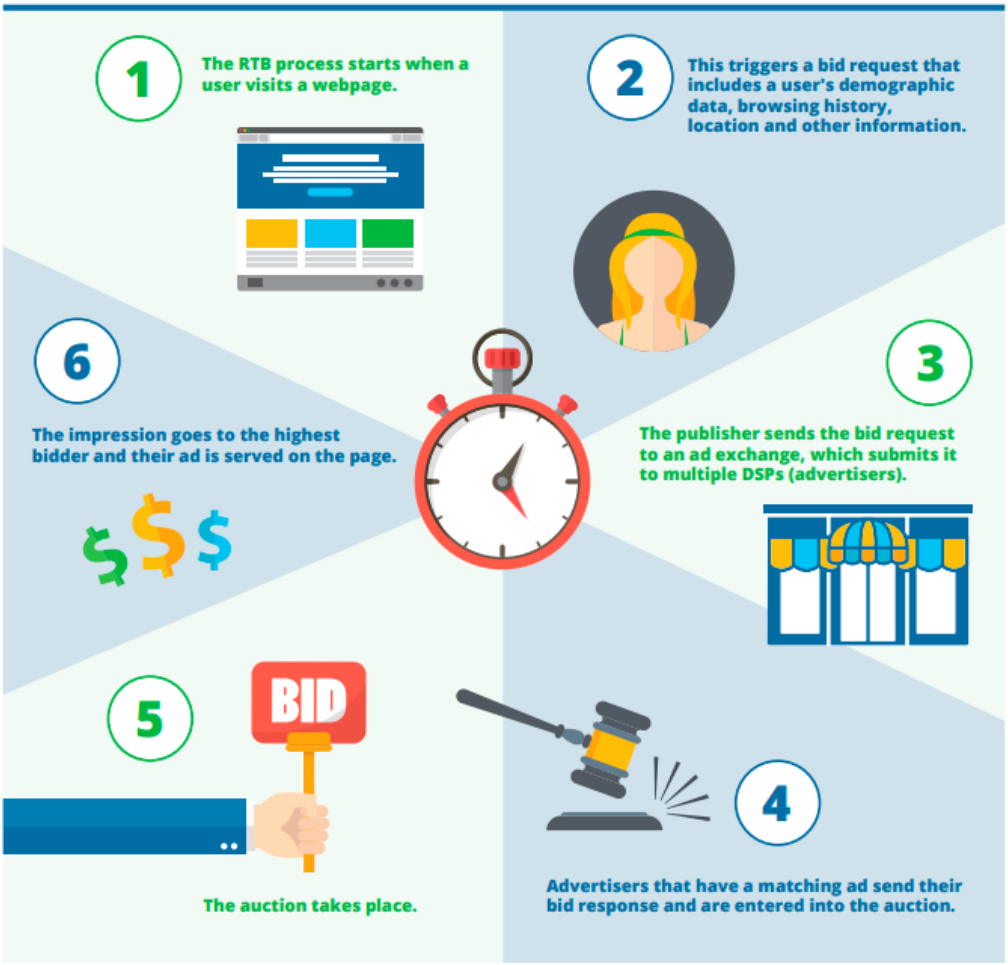
However, every view does not always equate to revenue. The reason for this is that an advertiser wants to pay for valuable actions, for example, an Ad that results in an install of a 3rd party app of the Advertisers' client. As developers, we only get revenue from SID users who ultimately watch the full ad, click, then install the advertised app or watched the full ad video ad right till the end.



Source: https://mobilefreetoplay.com/2017/03/09/video-ad-value-chain/#the-mobile-video-ads-value-chain

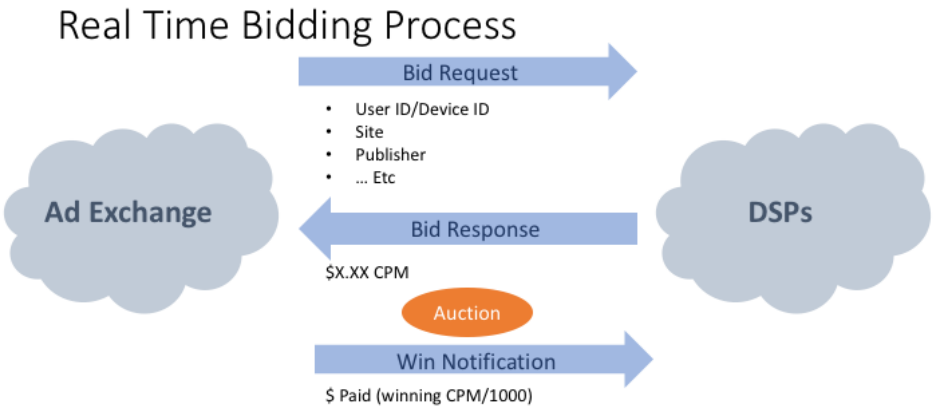
As we are unable to control a SID user's behaviour after they have watched an ad, we should focus on what we can control, the display and timing of the ad. It is to be noted that the revenue per same ad is not always the same over time. It depends on the type of advertising, country, advertising platform, time of the year and placement of the ad.

Here's what happens in a 200 millisecond real-time bid:



Source: http://www.nanigans.com/blog/cross/usu/real-time-bidding-what-happens-in-200-milliseconds-infographic/

That means that, in the exact moment we request an ad to show up to our SID users, a real-time auction occurs, and at that specific moment only the revenue is actually set.



Source: http://www.nanigans.com/blog/cross/usu/real-time-bidding-an-overview-of-auction-types/

As we stated before, the actual country where the SID users are consuming an ad is an important parameter to define the absolute value of revenue per ad consumed. We have therefore defined 5 different groups of countries, depending on revenue per ads ratio.

For example, we consider Tier 1 countries those like Australia, Canada, Denmark, France, Germany, Netherlands, Norway, Sweden, United Kingdom and United States.

Countries like Spain, Japan or Italy are Tier 2, and countries like Indonesia and India are Tier 3 or Tier 4, respectively.

Source: http://www.brusmedia.com/country-tier-targeting/

(iii) Ad Revenues

SID´s ad revenues are generated by our SID users viewing in-app ads. Such revenue is susceptible to the variability of real time auctions results and usually measured as “eCPM” (effective cost per mile). This eCPM is the result of a calculation of the ad revenue generated by a banner or campaign, divided by the number of ad impressions of that banner or campaign expressed in units of 1,000.

At this point, we have 4 different possibilities for our SID in-app Ads:

- Banner: Still the most popular mobile ad format, the banner ad uses an unobtrusive “banner”, typically at the top or bottom of the screen which features relevant text and graphics. Banner ads rely heavily on brand recognition, with little space to provide detailed information. It’s a

simple and safe way for a brand to get their name and product viewed by as many people as possible. They are still alive because these became a habit of use, are the cheapest ad format, are easy to implement and ease of compatibility of implementation. (Source: https://appsamurai.com/4-leading-mobile-ad-types-of-2017-banner-ads-still-exist/)

- Interstitial: Interstitial ads are interactive ads that display across the entire screen, often while an app is loading, during certain specific interactions in the App or after an app is closed. Interstitials offer users a chance to take part in high-level engagement with an advertiser's product, often featuring compelling and creative call-to-actions.

- Video: Video ads are simple in their concept yet complex in their execution. They are literally videos that play either while a user opens or interacts with a mobile application (App). They require a substantial budget, but offer a high level of user engagement.

- Native Ads: Native ads are ads that don't really look like ads. Rather looks like they present a banner with certain relevant information. Native ads attempt to seamlessly integrate with the publisher's App. The ad format mimics that of the original App format for optimal user experience.

As would be expected, the eCPM is quite different for each of the previous different ad options, so we must decide what kind of ad we are going to use, when, where and how.
The average eCPM can be estimated as follows:

- Videos $6.27
- Native ads $1.56
- Interstitials $5.14
- Banners $1.01
- Standard banners $0.35

Source:
http://ecpm.adtapsy.com/
https://www.appodeal.com/reports

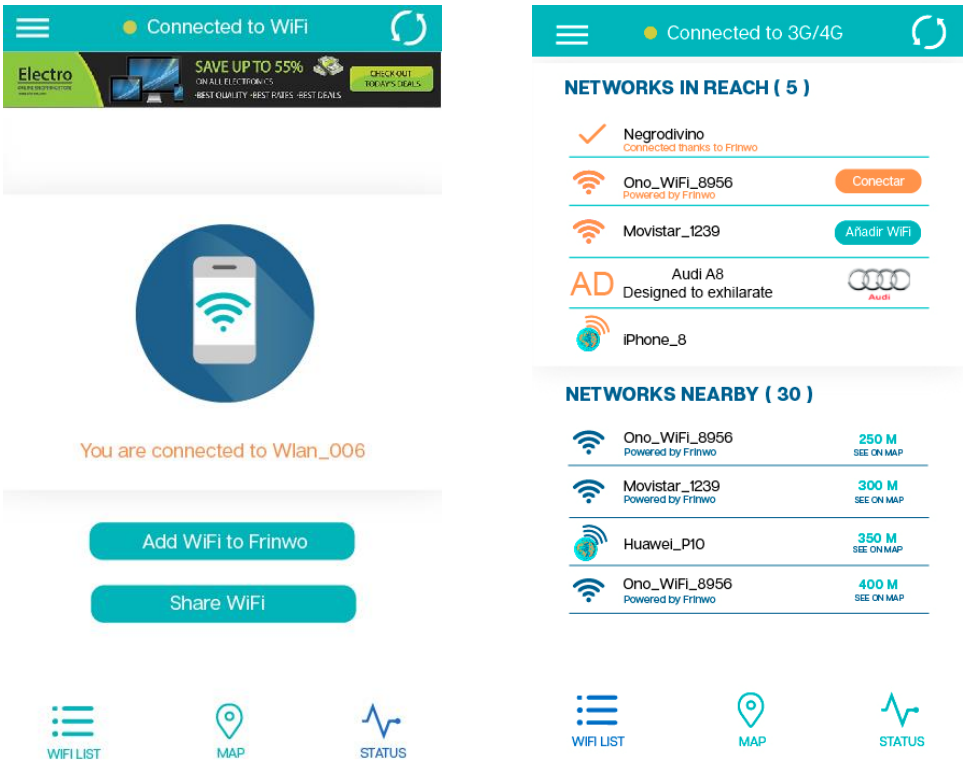
We must however keep in mind, for our specific SID business model, that most of the ad platforms transfer the money 30 to 60 days after the ads, whereas our SID users are aimed to receive instantly Tokens (Vouchers) or fractions thereof for consumed ads.

(iv) Advertising Strategy & Tactics

With all this previous information, our future revenue strategy is aimed to be designed such that ad revenue shared with our SID users, intended where possible to be on the basis of non-intrusive ads which most likely lead to a lower potential revenue but to a more stable basis of revenue.

For those SID users who wish to acquire Tokens (Vouchers) to pay for consumed Megabytes (MB), we must offer a high-eCPM solution that gives us a just sufficiently high enough incoming per Ads or in worse case a few ads at best to allow the SID user to obtain the number of Tokens (Vouchers) required to pay for at least a few tenths of Megabytes of internet data in an easy way.

In a first instance, a more suitable option is to make use of banner and/or native ads.



Going forward however we believe that a mix of the previous with presenting our SID users at specific times and countries with Native advertising is becoming a stronger option as that Ad delivery method

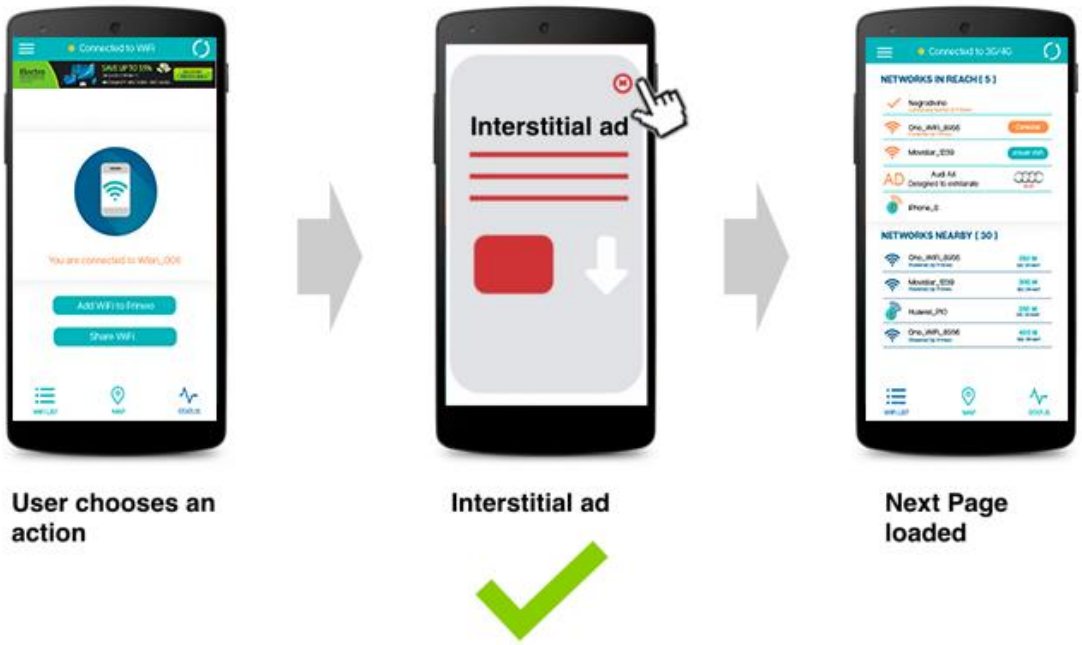
is becoming more mature and reliable, so maybe it's a good alternative way of creating a higher eCPM with our SID users.

Source: http://www.businessinsider.com/the-native-ad-report-forecasts-2016-5

https://nativeadvertisinginstitute.com/blog/native-ad-revenue/

https://nativeadvertisinginstitute.com/blog/native-advertising-trends-2017/

For those SID users who actively engage themselves in acquiring in-App Tokens (Vouchers), probably video advertising and interstitial ads are more suitable in our view.



We can give those specific future SID users with a high propensity of in-App engagement, the opportunity of watching a complete 30 sec. video, or a carousel of 6 interstitial ads, with a locking period of 5 sec. each, depending on the country and Ad platform. This aims to result in potentially higher revenue per ad in one way or another.

As a conclusion, the previous clearly shows that there is not just one ad solution that fits all but rather we aim to implement a mix of all the previous ad delivery methods and keep adapting those regularly as the SID user base grows. Adaptation can be for example to adjust ad methods to the countries or regions with high SID user´s concentration making more local ad agreements in those regions to maximum revenue or adjust the actual ads per SID user´s groups that would stand out more than others such as for example to promote ads in the language(s) to those actual high concentration of SID users.

A key aspect to consider in the advertising monetisation to Tokenization model, as mentioned before is the typical 30-day gap between the company receiving actual Fiat payment for consumed SID user´s ads and the instant Tokens acquisition for the SID user from another SID user or from a SID Token Exchange, so the company aims to maintain a cash reserve to pre-fund the purchasing of these Tokens. However, in the event there are no Tokens for sale at the precise moment as a user consumes an Ad and is due his Tokens instantly, then the Tokens provided could be from the company Tokens reserve pool. The Company Token pool or also known as the company reserve Tokens which are suggested to be increased yearly by new generated Tokens equal to the % of each prior year's global inflation rate as published by the World Bank starting one year after the completion of a successful ITO. This will be reviewed and is subject to change by the Company going forward at any time.

(v) Monetization of Payment Transactions

SID could in future also partner with or add its own eWallets to the SID App enabling digital currency transactions whenever a user is within range of another SID enabled user with an internet connection.

SID aims to receive a small share of transaction fees, only if and when working with remittance 3rd party businesses, thus potentially creating an additional future revenue stream.

(vi) Night Mining.

SID could also add the capability to allow users to install light mining software on their smartphones. This can enable users to participate in crypto-mining networks by enabling their smartphones to earn mining fees paid in SIDs for example while the users are sleeping and their devices are plugged in to the mains and have a data connection. This need exploring further as to its technical viability.

7 The Token Sale

Funding the Business is aimed to be through a Token Sale of SID Tokens (SIDT), our Utility Token. SID is preparing for a Token Sale to obtain funds in the form of advancing revenue by Tokens sale to implement additional incentive scheme to the existing ones and scale the existing system of the SHARE INETRNET DATA (SID) system to accommodate the expected Users growth and to interface the SID system to the Stellar blockchain aimed for automatic mass scale settlements of payments by SID Tokens on the SID system. This advance turn-over received from selling of Tokens to our Users for them to consume internet sharing on our SID network aimed to be used as follows:

- Development of bigger scale infrastructure to accommodate mass Users exchanging Tokens for Internet shared on the SID system or between SID users
- Integration expansion to allow mass settlements of SID Token transactions through the Stellar Blockchain
- Increasing Brand Awareness on social & main stream media
- Engaging with and integrating to a global network of distributors for new SID Users acquisition.
- Development & deployment of the Licensee's Apps with our SDK inside
- Traditional online Marketing & Distribution Costs
- Cost of organization, initially only R&D followed increase by project management and post-commercial launch costs of SID heavily skewed towards Marketing spend,
- The lower part of the overall for Legal & Administration & Management & Board/Advisers.

The **SID Token** has been created on the Stellar platform suitable for high volume micro-transactions at practically negligible transaction cost to users. The best candidate for SID was the Stellar blockchain.

The advantages of using a fast, low cost blockchain like Stellar for which we already created the SID Tokens, for the SID users are as follows:

Transaction costs on Stellar are negligible (approximately 100,000 transactions cost less than $0.01). This compares favourably with $0.16 cents per transaction currently on Ethereum. The lower the transaction costs, the easier it is for us to process transactions in SIDT and the less costly it is for trading shared internet Megabytes for SID Tokens.

Faster Transaction Speeds.

The Stellar blockchain can already process up to 30,000 transactions per second with a median confirmation time of only 4-5 seconds.

This compares favourably with other blockchains such as Ethereum, likely because despite this last being considered a far broader engineering language so far still only handles 15-20 transactions per second with confirmations taking around 3.5 minutes (when the Crypto Kitties are not awake).

Furthermore. Stellar has Stellar Term, its own decentralised exchange (a "DEX"). In effect the Stellar blockchain is an exchange in its own right, meaning that any SID user all they would need to do in future is to create their own Stellar account/wallet to be able to receive SID Tokens and transfer between SID users is as simple as a transfer between two different Stellar accounts/wallets.

Participants interested to support the SHARE INTERNET DATA project (SID project) can do so already by signing up through our website https://ShareInternetData.io where today they can Register and soon will be able to contribute towards SIDTs using BTC, BCH, BTG, ETH, LTC and of course our underlying blockchain coin XLM (Stellar Lumens) or one of the many supported FIAT currencies.

To facilitate adoption by users in less affluent economies, the SIDTs are aimed to be launched at the price of 100 SIDT per €1 i.e. €0.01 for each SIDT, with bonus or discount as published on the SID website (www.ShareInternetData.io) in due course and updated or amended from time to time. Nevertheless, users are aimed to still be able to transact in fractions of SIDTs, in future, if required.

Maximum cap (max. limit) at See www.ShareInternetData.io

Unsold Tokens after each deadline are put in Company Pool for another future Token sale.

Token name	SIDT
Hard Cap: Maximum amount to be collected (if this maximum target is reached then the token sales ends)	See www.ShareInternetData.io
Total maximum pre-mined Token supply created	25 Billion (BN) [100%]
Maximum number of tokens (SIDT) generated to token sale participants. Number of tokens for each phase as well as the price per token for each phase and the bonus or discount will be announced through our website: www.ShareInternetData.io	10.25 Billion (BN) [41%]
Maximum number of SIDT generated to Bounty, Referrals & ITO Brokers (Brokers estimated to be 2 to 6% of total) at ITO or if paid from ITO revenue crypto currencies or fiat then these Tokens will go to the **Company Token pool**.	1.991 BN [8%]
Maximum number of SIDT generated for Whitelisted users, as free tokens for certain user tasks & Air-Drop tokens giveaway programs for certain users´ actions during private sale and all through the ITO phase.	0.884 BN [4%]
Maximum number of SIDT tokens generated to **Founders & others pool** founders, executives & other individual contributors.	5 BN [20%]
Maximum number of SIDT tokens generated to **Board Advisors pool**	1.25 BN [5%]
Maximum number of SIDT tokens generated to **Company Token pool**	5.625 BN [23%]

* Sid Ltd has not imposed a minimum aggregate contribution target. SID Ltd reserves the right at any time to impose a different minimum aggregate contribution target.

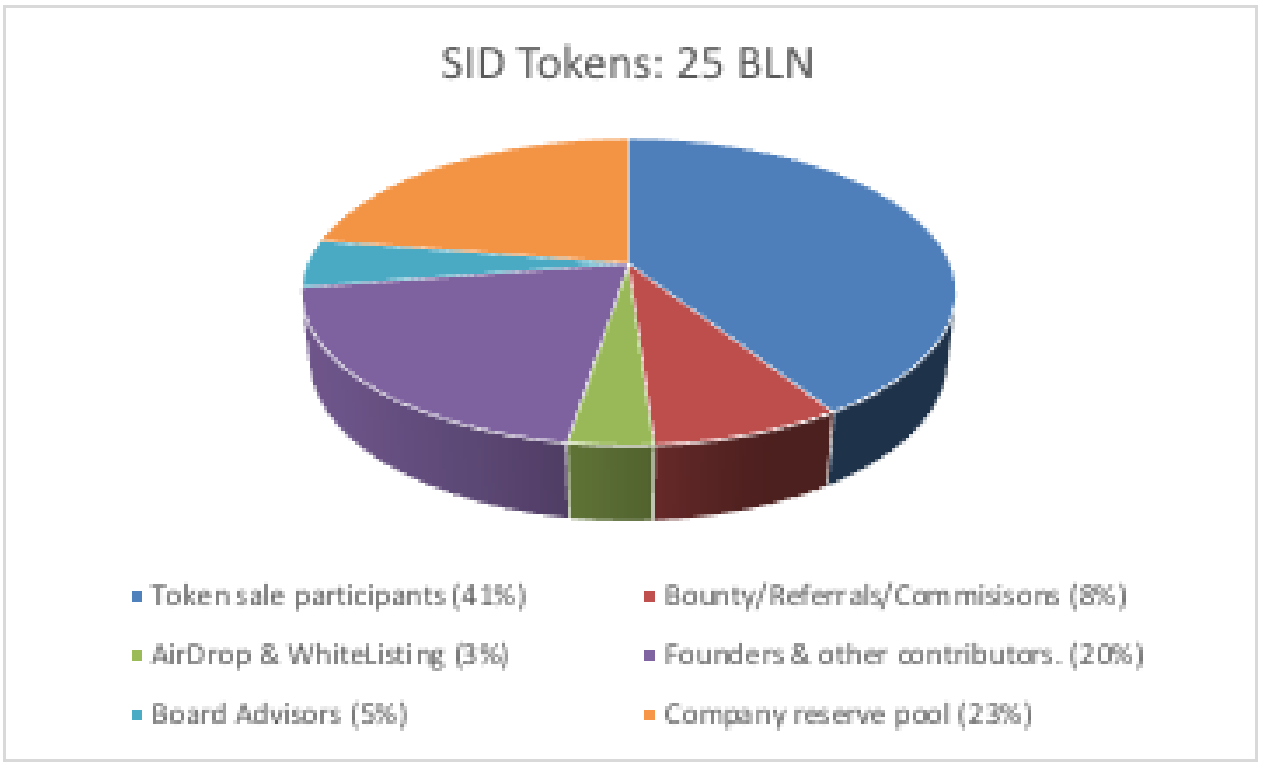
* All time maximum tokens is now capped at 150BN. The future SID Tokens other than the 25BN herein, called mined tokens aim to fund future expansion (users growth) and aimed to be released when 90% of the current 40million users target is reached, namely at 36million (meaning the 3rd party SID-SDK & SID APPs) users App downloads combined AND 50% unmined are locked for two and a half years from 1st June 2018 onwards and the remaining 50% (62.5BN) are locked for three and a half years from 1st June 2018 onwards and released if 90% the next 100million users target is reached, namely at 90million extra users or total in aggregate 40+90= 130million (meaning the 3rd party SID-SDK & SID APPs) users App downloads combined.

The minded locked Tokens aim to fund 80% each of the next 100m users App download increment growth and 20% cost of organisation. Since the first 40m users = 25B SID Tokens. So, the next 100m SID users are aimed to be funded by mined (25:40)X100=62.5BN Tokens per each of the two 100m users App download tranches.

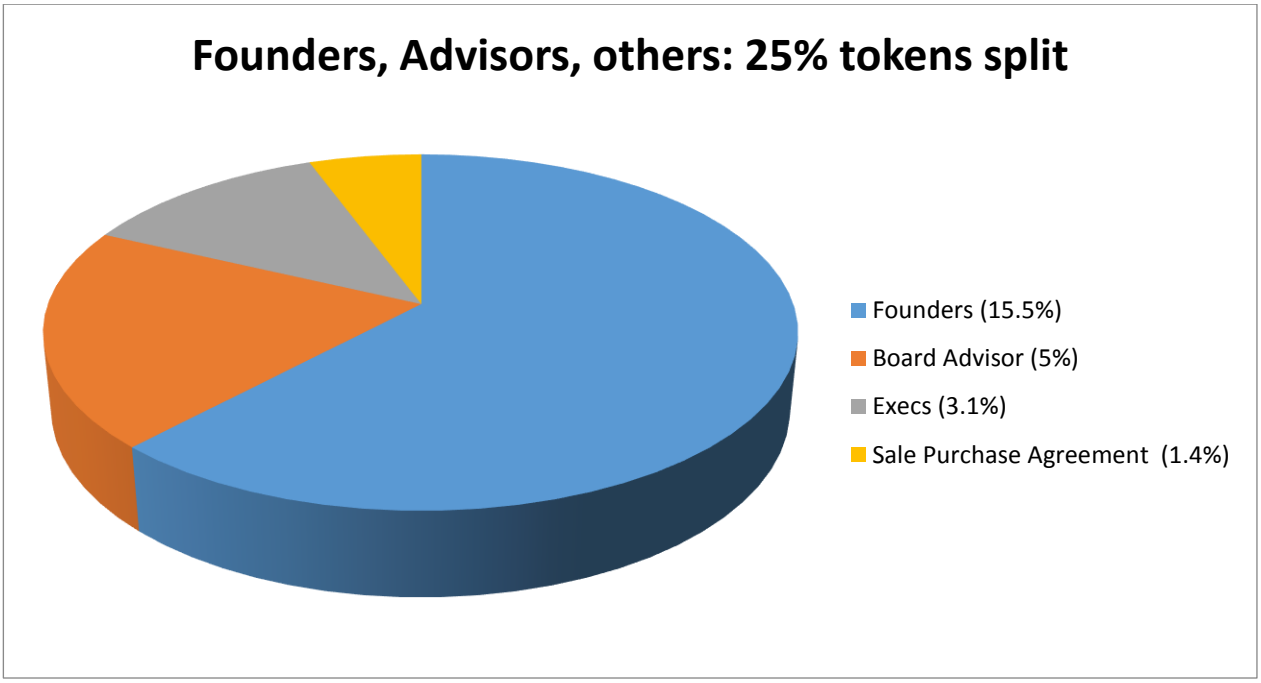
For the latest version applicable at any given time on DISCLOSURES, TERMS AND CONDITIONS OF TOKEN SALES, PRIVACY POLICY, visit our website at **www.ShareInternetData.io**

Graphical representation of the Tokens split at the Initial Token Offering.

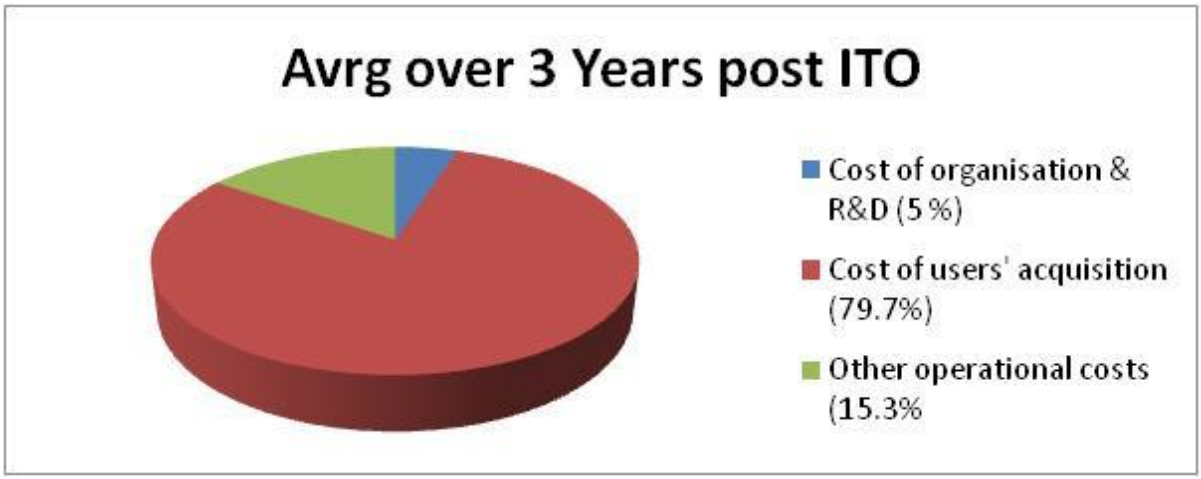
As an example only, 1 EURO = 100 SID tokens. Price/token may be different during ITO or after.



The % of total tokens for new Advisors, new Execs or others may be vary slightly up or down.

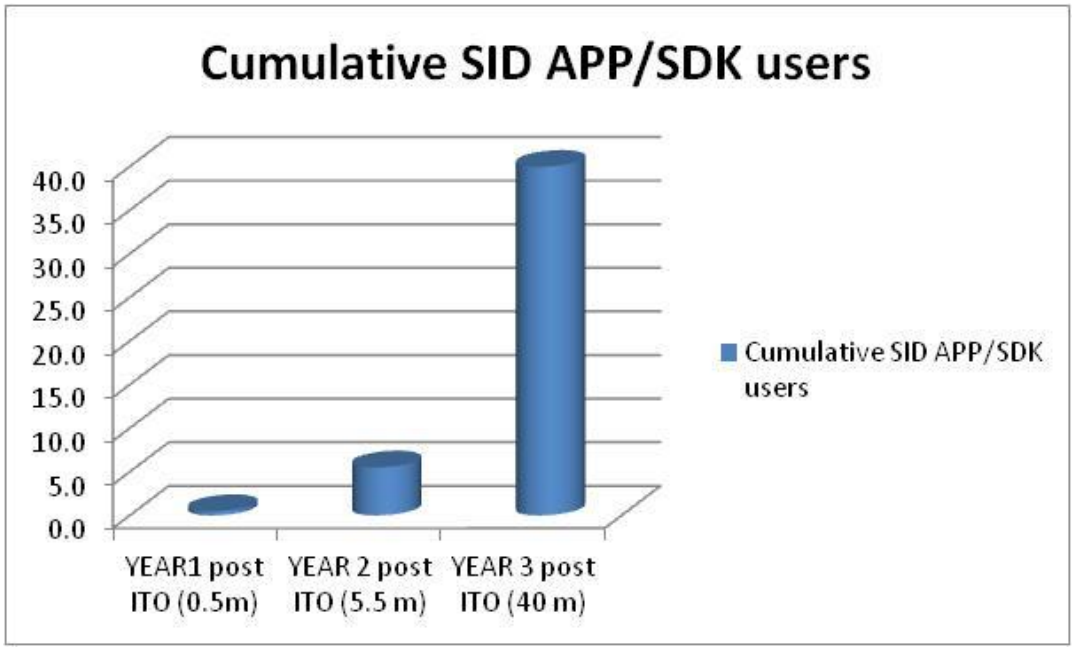


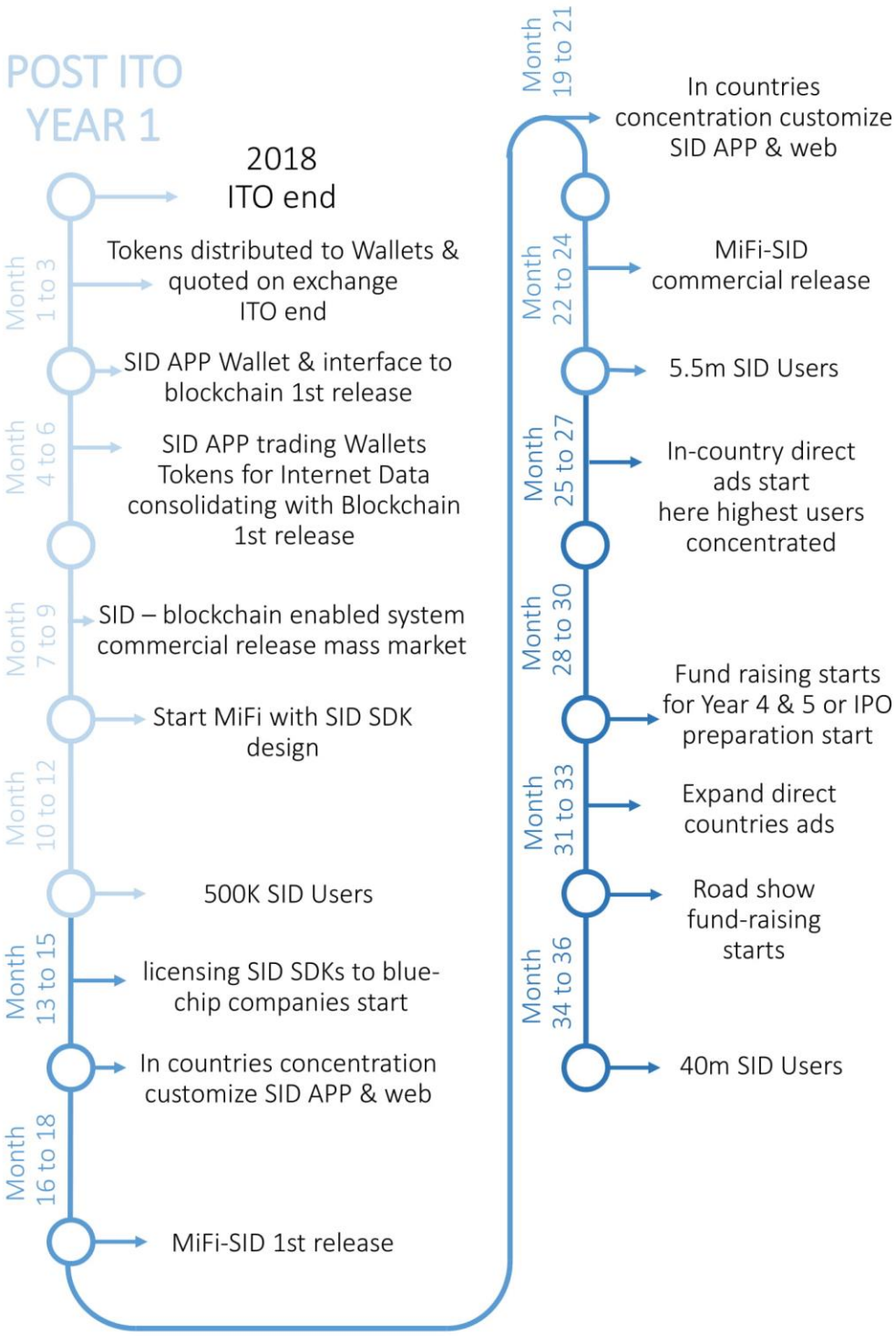
Graphical representation of funds spending split over the three years' post ITO



Graphical representation, number of SID users APPs & SDK over the three years' post ITO

These figures over 3 years post ITO are assuming the € 80 million max. cap is reached, otherwise the figures of number of total cumulative SID users aimed to be achieved is aimed be proportioned to the actual available net funds at the end of the ITO process or at the start of each of the three years post ITO. Meaning year 1 requires 3m, year 2 requires 14m and remainder 63m is required for year 3.

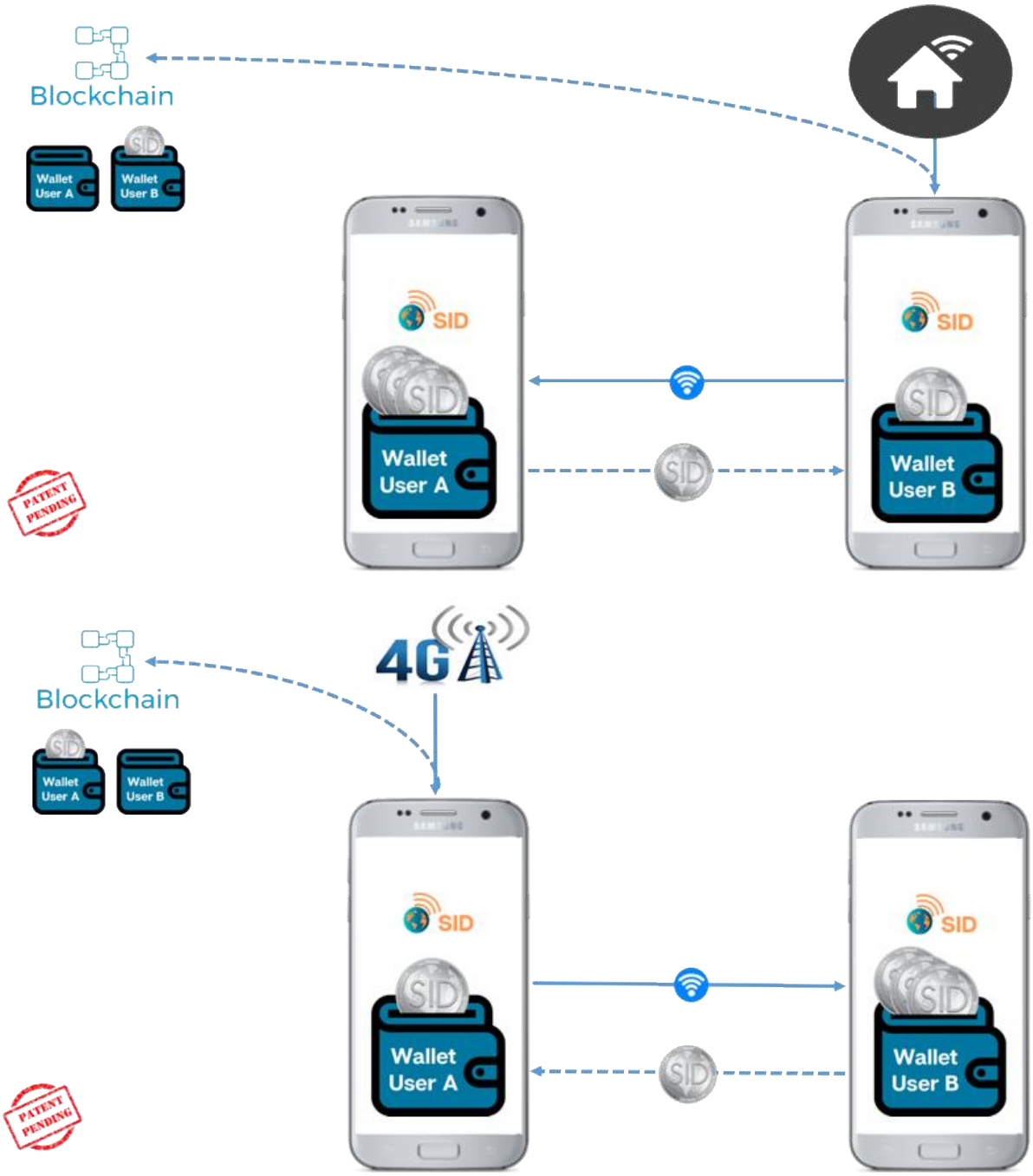




8 The role of SID Token in the SHARE INTERNET DATA Ecosystem

The SID Tokens (aimed to use the ticker symbol “SIDT” if available) have the following functions:

- The SID Tokens accounts are aimed to pay all of their administration & custody fees in SIDTs whenever possible, or in other crypto currencies, bought from the open market.
- To encourage sharing economy, SID Users sharing their connections are aimed to have their accounts credited with SID tokens (SIDT) as defined by the company from time to time on our website.
- The amounts of SIDTs credited to users, are aimed to be calculated by algorithms based upon estimated share of revenues from advertising when consuming future Ads or the amount of internet data and source home-WiFi, mobile data, country etc..) received from another SID user.



9 Reasons to Participate in the Token Sale

Although the product already was released, part of the Token Sale aims also to support the future development of the commercial large-scale expansion of the SID system following the activation of the interface to the Stellar blockchain interface and updating user's wallets when using the Tokens as trade for consumed internet on the "SHARE INTERNET DATA" (SID) de-centralized system. Prior to any token sale payment collection, the SID system already supports the obtaining of SID future Tokens on their account (same account as the Whitelist account (private user area) which was available through our website since the 23rd April 2018, or through our SID Android APP since 31st May 2018, for each new WIFI added by SID users to the SID network.

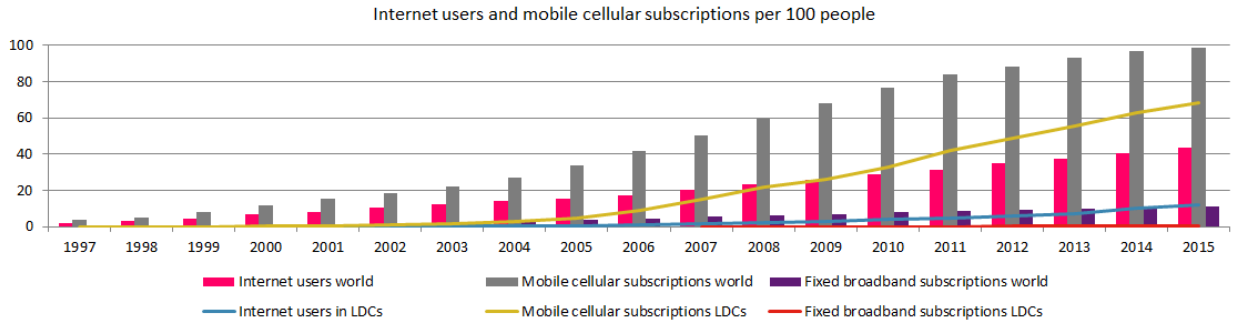
The SIDT aims to offer Smartphone Users the possibility to access crowd-sourced internet shared by other Users of our "SHARE INTERNET DATA" ecosystem, SID eco-system, when they have no coverage or no data credit or simply no internet access at a given location but hey are nearby other SID smartphones who do have internet access or nearby a WiFi on the SID network added by a SID user. By accessing internet from nearby Users' Smartphone's' this SID Token (voucher) sale could possibly be the trigger to unleashing a vast amount of people coming out of poverty simply by the fact that they would have finally a means to access the internet, as published by the world economic forum. See the following URLs:

This of 2015

https://www.weforum.org/agenda/2015/02/how-to-lift-160-million-people-out-of-poverty/

And this one of 2017:

https://www.weforum.org/agenda/2017/07/digital-least-developed-countries-inequality/



Although in the developed world we may take for granted the things we access on the internet, it's not the case in many developing countries where less fortunate people can't do the things depicted in the follow article and shown in a graph as "what is accessed in 1 minute internet time" BUT that's one of the things what SID is also trying to improve with its SHARE INTERNET DATA system: https://medium.com/world-economic-forum/what-happens-in-an-internet-minute-in-2017-91288d95bc7d

A misconception needs to be addressed in our view, the notion of "less fortunate people" or "poor people" are not terms specific to Developing Countries but those are generic terms to be understood globally because there are also a scary amount in the two digit millions of "less fortunate people" or "poor people" in the developed economies like the USA and Europe who in the 21st century have no internet access or can´t afford it never or not every month. Therefor it has to be taken in the global context and not just to Developing Countries.

See this article with title "70% of poor people on broadband subsidy will lose their connections thanks to Trump's FCC": https://boingboing.net/2017/11/17/internet-access-is-a-human-rig.html

10 The Team

SID Ltd. (Share Internet Data limited liability company): https://shareinternetdata.io/#team

Jose Merino (Co-Founder)

Co-Founder & Chairman & Company Director of Share Internet Data (SID). Serial Entrepreneur with experience in telecoms, mobile, bleu-chip executive experience, Start-ups trade sale. Ex Vice President of Operations of Philips consumer communications in US, ex-Founder of Sensei Ltd in UK sold to Vtech Holdings of Hong Kong. Past world prestigious engineering magazine IEEE article contributor and author of 15 granted telecoms patents and several pending patents in the pipeline.

Susan Howard (Co-Founder)

Occupies SID's position of supervising current R&D team expenses and future employees´ expenses and in future all expenses above a certain figure, as decided by the board, aims to be approved by an executive and then by her or anything that may result in financial liability in the future or could result in a future invoice to SID Limited needs her a 2nd approval before incurring such liability. Susan was in the UK a former Director of ToyStore LTD and in Spain a former General Manager Benalclaf S.L.

Kiss Lajos

Highly experienced Manager with more than 25 years know-how in multinationals companies as Alcatel and Nokia. Background in communications chipsets design, commodities and management.

Marcin Zduniack

Technical blockchain software developer on behalf of SID & potentially to become Blockchain lead software developer of Share Internet Data (SID LTD) after ITO, provided an employment agreement can be reached. Former Senior Java Software Developer Engineer, Software Architect and since 2015 an Experienced blockchain Software Developer specialised on Crypto-currency Software projects.

Michael Camilleri

Currently Regional expansion Canada & US on behalf of SID, pending employment agreement can be reached post ITO. Serial Entrepreneur with experience in telecoms, mobile, bleu-chip executive experience, Start-ups trade sale. Ex Director EMEA of Philips consumer communications in Europe, co-Founder of Bizzby currently operating in UK, Ex-Founder of Sensei Ltd in UK sold to Vtech Holdings.

Corey Wilton

A past Sales representative for Wyndham Worldwide, and more recent past Community Manager for Xcel Token. Currently Corey is the Telegram community manager and co-setup of the incentive programs for SID.

Dr Ibrahim Halkano, PhD

Dr Ibrahim Halkano, PhD is an expert in Blockchain micropayments and experienced in ERP Systems. With ex functions in the field in companies like MTN Bharti Airtel and MTN through Oracle.

Ericl Pardio

Founder at Pardio Networks Blockchain Enthusiast - Privacy Advocate - Network Design Specialist - Consultant SID Mexico and Latin America growth manager at SID-Frinwo You can reach me on the usual channels and projects https://t.me/epardio In medium for research ATM https://medium.com/

Gaurav Areng

A skilled Digital Marketing specialist with 10+ years of work experience. I am adept in Market Analysis, Strategy Development, Global Marketing strategy, Channel management, Search Engine Optimization(SEO), Search Engine Marketing (SEM), Social Media Marketing (SMM), Influencer Marketing.

Santosh Yellajosula

Currently Chief Tokenisation Officer at SID. Decentralization activist, Policy maker with Skillset in Blockchain tech and tokenization, sub-tokenizing, Sees himself as a Crypto Economist, Marketing for tokens specialist, ICOs Investor, Advisor to ICOs and Blockchain projects.
A firm believer in the decentralised world and peer to peer exchange of value. Real-world experience of working with Innovation ecosystem including Large corporates, VC firms, Government bodies and communities to Blockchain/Crypto world.
A member of the Kairos society. Participated in Start-up India in Portugal, f6s, Digital blockchain foundation, and SingularChain.

Paul Mears

Passionate tech, bio and innovation investor with experience of working in a variety of finance and operational roles in UK, Amsterdam, Hong Kong, USA, Canada and Monaco in a range of companies from start up to multinationals including hedge fund, telco, constriction, software. Angel investor with portfolio of Biotech, Med Devices , Apps, Payments and since 2016 active in crypto as an investor and advisor to Initial Coin Offerings including Humaniq, Modex, Varcrypt, Howdoo, Autobay, Jointo.

SID Strategic Advisors:

Christian Solli Nyborg

Serial entrepreneur. Ex Ericsson's Global executive management program member. Ex-Member of the Board of the Spanish- Norwegian Chamber of Commerce, taking part of improving networking business relationships between Spain and Norway. Former Co-Founder, Board member and C.O.O. of Masmovil an MVNO that did a successful IPO on Madrid stock Exchange and currently grew to become the 4th biggest Network operator expanding from mobile to own optical fibre fixed network, currently passed a market cap of more than 1.5 Billion EUR as of January 2018.

Kerry Ritz

Former CEO of Great River Ventures Ltd, Ex-CEO at Great River Ventures Ltd. Former Chief Commercial Officer at ACN, CEO at Palringo Founded in 2006, Palringo had over 27 million users across 350,000 user created groups enabling people to come together and communicate through text, voice, pictures and games. Ex-President of Vonage UK Ltd, during his term achieved 24 consecutive months of double-digit subscriber growth; Developed innovative approach to media buying, customer analysis and customer segmentation; Developed B2B sales strategy that increased Vonage sales 3x, including outbound telesales; negotiated retail listings of hardware in largest UK retailers of consumer electronics.

SID Board Advisors:

Simon Cocking

Simon Cocking is Senior Editor at Irish Tech News - now getting 500,000 unique monthly views, Editor in Chief at CryptoCoin.News, and freelances for Sunday Business Post, Irish Times, Southern Star, IBM, G+D, and others. He is a top ranked member of the 'People of Blockchain' (currently as of 15th March 2018, ranked at #1 / 18,000).

He is also a business mentor and advisor working with 80+ successful ICOs to date. He also been named many global Twitter influencer lists in the last 12 months. He is an accomplished public speaker at events including TEDx, Web Summit, Dublin Tech Summit, and overseas in Dubai, Singapore, Moscow, Tel Aviv, Madrid, Tbilisi, Riga, Porto, Dublin and Helsinki in the last 12 months.

He has been based in Ireland for over 22 years and has cofounded or founded seven successful companies."

David Drake

Currently Board Advisor of SID Ltd (Share Internet Data Limited). Mr. Drake through his family office manages and co-invests in alternative assets with the top 30 family offices out of his 5000 - family office & institutional investor reach. These top 30 are 40% from Asia, 20% from Europe, 20% from the Americas, & 30% from the Middle East.

Mr. Drake is a digital automation advocate for private equity as he lobbied the US Congress on the JOBS Act since 2011. He represented the US Commerce Department at the EU Commission in Brussels & Rome in 2012, was invited to the White House Champions of Change ceremony in Washington, D.C., &, was a speaker at the UK Parliament in 2013. Born in Sweden & fluent in six languages, Mr. Drake has an MBA in Finance & an MA in International Law & Economics from George Washington University in DC where he was awarded the Wallenberg Scholarship for academic merit. As of 15th March 2018, ranked at #2 on icoBench.com

Vladimir Nikitin

Co-founder of Top ICO Advisor, an accomplished legal consultant, ICO advisor, Blockchain cryptocurrency specialist and a member of several Board of Directors.

A renown member of the crypto community and an active advocate of Blockchain over the last few years, where he has gained an extensive community of contacts, as well as over 30,000 network connections on LinkedIn. With a Masters degree in both Law and Economics (Finance and Credit), Vladimir has over 10 years of Civil law, finance, Internet technologies experience in various industries such as retail consulting, hospitality and information technology.

A listed Blockchain Expert on ICObench.com (TOP-6 on March 15, 2018).

Amarpreet Singh, MBA

Currently also a Board Advisor of SID. He holds three Masters degrees and has lived/worked/studied in India, Singapore, France, China, South Africa, Korea, Canada etc. He has worked with tier 1 firms like Microsoft, The World Bank, Airbus. His work with The World Bank has given him key macro insights and taught him valuable lessons about how multi-lateral international banks work. His many awards, certifications and recognitions are a testimony to his character and quality work.

Nikolay Shkilev

Firstly, an experienced entrepreneur, Co-Founder "Top ICO Advisors", rated TOP 5 in People of Blockchain, owner and co-owner of dozens of successful business projects, an ICO advisor and ICObench.com expert. Nikolay has 20 years of experience of being involved in large-scale projects, and has many awards and titles in an area of IT technologies.

Some of his awards include: Self-Made Russia award, Tech guru, and Super TOP award. Founder and CEO of the "Private Business Club" - a private club for successful entrepreneurs. His Holding received the "Enterprise of the Year" award in Kremlin. A devoted Crypto enthusiast and mentor.

Frinwo S.L. is currently the exclusive R&D centre of SID Ltd:

All below are Frinwo S.L. founders and are also **Co-founders of SID Limited**

Jesus Ruiz

Co-Founder & Managing Director, Frinwo S.L. Spain. Experience in banking at BBVA.

Daniel Urbano

Co-Founder & R&D Director, Frinwo S.L. Spain. Ex blue-chip experience at IBM and Vodafone.

Mihaela Dimitrova Mihaylova

Co-Founder & Marketing Manager, Frinwo S.L. Spain

Alberto Carlos Avilles Jimenez

Co-Founder & Android Software Manager, Frinwo S.L. Spain

Jesus Leon Canca

Co-Founder & iOS Software Manager, Frinwo S.L. Spain

For the latest version applicable at any given time on DISCLOSURES, TERMS AND CONDITIONS RELATING TO TOKEN SALES, PRIVACY POLICY, visit our website at www.ShareInternetData.io

If any discrepancy between any mention in this Whitepaper and the "Disclosures", "T&Cs relating to Token Sales" or the "Privacy Policy" or any such other more recent document as published from time to time on our website then those on the website, www.ShareInternetData.io at any given time always prevail.

Appendix 1:

The currently accessible domains to the public:

shareinternetdata.io	(active primary domain for the SID ITO)
shareinternetdata.com	redirected to **shareinternetdata.io**
sharedinternetdata.com	redirected to **shareinternetdata.io**
frinwo.com	
frinwo.es	(This domain is not owned by SID Ltd but legal owner is Frinwo S.L.)

Other SID LTD owned domains:

frinwo.io

frinwo.net

frinwo.org

frinwo.info

frinwoico.com

frinwocoin.com

frinwotoken.com

frinwoblockchain.com

freeinternetworld.net

freeinternet4all.com

freeinternetforall.com

shareinternetdataico.com

shareinternetdatacoin.com

shareinternetdatatoken.com

shareinternetdatacurrency.com

shareinternetdatacryptocurrency.com

shareinternetdatabitcoin.com

shareinternetdataethereum.com

shareinternetdatablockchain.com

shareinternetdatacustodian.com

shareinternetdataledger.com