SIRIN LABS

FINNEY™

SECURE OPEN SOURCE CONSUMER ELECTRONICS FOR THE BLOCKCHAIN ERA

White Paper

Prepared by: SIRIN LABS Team

DISCLAIMER: This white paper represents work in progress and illustrates the intent of SIRIN LABS to develop, launch and market certain products. The implementations of these products are built on new technologies, and it is expected that significant changes will be continually required to meet the evolving requirements of the market's and customer's demands.

CONTENT

1. OVERVIEW

SIRIN LABS - the developer of SOLARIN, an ultra-secure mobile phone - is holding a crowdsale event of SIRIN LABS tokens (SRN Tokens). Funds raised will support the development of FINNEY™, the first open source blockchain smartphone and all-in-one PC. Alongside the support of the SOLARIN mobile phone. Customers will be able to purchase all SIRIN LABS products (SOLARIN and FINNEY™) and services with SRN Tokens.

The current generation of smart devices compromises on user security. The focus is overwhelmingly on user experience, at a huge cost in fraud and cybercrime. We believe the digital economy of the future cannot tolerate this trade-off: device architecture demands a paradigm shift that enables true security, while maintaining excellent user experience.

FINNEY™ devices are the first cyber-protected, blockchain-enabled mobile phone and PC. They enjoy the functionality of Android™ OS, plus a suite of cyber security technologies, giving users safe, reliable access to the blockchain.

FINNEY™ devices form an independent blockchain network, a distributed ledger both scalable and lightweight, powered by IOTA's Tangle technology and SIRIN LABS' security ecosystem. FINNEY™ is free from centralized backbones and mining centers, capable of providing fast, fee-less and secure transactions.

FINNEY™ devices will run on SIRIN LABS' open-source operating system, SIRIN OS™. This is designed to support inherent blockchain applications, such as a cold storage crypto wallet, secure exchange access, encrypted communications and a P2P resource sharing ecosystem for payment (not by means of SRN Tokens)The SRN is the exclusive way to acquire SIRIN LABS full line of products and services.

SIRIN LABS will partner with consumer electronics OEMs to promote the adoption of FINNEY™ architecture and SIRIN OS™. Both will be released under open source licenses.

2. BACKGROUND

2.1 About SIRIN LABS - Past, Present, Future

SIRIN LABS was founded in 2014 with the mission to develop the world's most secure phone. SOLARIN – our flagship product – was launched in May 2016 to high acclaim, after an intensive research and development process.

SOLARIN incorporates state-of-the-art hardware and software security technology, 24/7 cyber protection, and includes a private zone for encrypted calling and messaging.

At SIRIN LABS, innovative technologies meet impeccable design and uncompromising quality. Our passion for excellence drives us to create the world's foremost technologies. Pioneering design and immaculate service, enables SIRIN LABS to deliver high-end, exclusive products to consumers worldwide.

SOLARIN was launched in May 2016 making a splash global media and until today is still considered as the world's secure phone in the world.

SOLARIN is sold via our london store in Burton place, and is leading in sales at Harrods luxury technology department.

Since SOLARIN was launched we learned -

- We have an incredible professional team and useful assets: Know how in creating hardware, IP for the most secure OS and services
- There is a "tectonic shift" in the world of digital economies and blockchain technologies
- There is an immediate and growing community that believes in blockchain based products and services and with a real need for privacy and cyber protection

These insights were melded into a new device family: FINNEY™. Naming is an homagé to bitcoin pioneer, Hal Finney, who passed away in 2014: https://en.wikipedia.org/wiki/Hal_Finney_(computer_scientist)

SOLARIN – ultra secured high-end smart phone

2.2 Our Vision

SIRIN LABS' vision is to become the world's leader in secure open source consumer electronics, bridging the gap between the mass market and the blockchain economy.

3. PROBLEM DOMAIN

We plan to solve these main challenges:

3.1 Securing the Blockchain Ecosystem

Smartphones and PCs were never designed with security or privacy as a major factor, though these are essential to ensure the trust of the blockchain network. As technologies such as cryptocurrency mining, trading, and online payments become available for these devices, they turn into even more valuable targets for malicious actors.

Many apps that we download, harvest data by asking for more permission types than are really needed (for example, flashlight apps that need access to your contacts) and so jeopardize our privacy. Nowadays, smartphones are just as vulnerable to hackers and malware as PCs but are even harder to protect.
Another problem with modern smartphones is that they have so many capabilities. Thanks to a hypercompetitive marketplace, there is a constant race to add more and more features. This has two implications: 1) security often lags behind, and 2) the potential attack surface is enormous. It is relatively easy for a determined attacker to hack a device, access it and obtain data. There have been several attempts to tighten up smartphone security - like the introduction of end-to-end encryption on some widely-used messaging apps such as WhatsApp and WeChat. But unfortunately, this is not enough. While an app may be secure, this does not help if you have already been tricked into downloading a piece of malware that sends screen captures of your messages or records your calls.

To prevent such attacks, smartphones must be secured not only against external intrusions, but also at the hardware low-level of the phone itself. This can only be done through tightening the operating system itself, which means that a phone must be developed in its entirety, as the necessary level of protection cannot be achieved through app development alone. These considerations have forced manufacturers of secure mobile phones to develop phones, which are both expensive to produce and provide limited usability in favor of security, and therefore leave no room for advanced features.

We plan to tackle and solve these security and privacy challenges while maintaining full uncompromised usability.

3.2 Using cryptocurrencies is not trivial

A major barrier to mass-market adoption of cryptocurrencies is the technical complexity of their use. While the actual sending of funds is simple as any other means of payment, applying reasonable protection of one's wallet from being lost or stolen is very complicated.

With an operating system designed to be inherently secure, combined with hardware that can essentially implement a cold storage wallet, software can automatically provide the best practice handling of cryptocurrencies: store keys in the cold storage wallet; separate frequently-used wallets from rarely-used ones; direct the user to delegate recovery tools when their wallets accrue high balances, etc.

3.3 Monetization of Secured and Trusted P2P Sharing of Resources

The spread of stationary and mobile consumer electronics during the 21st century - smartphone, laptop, tablet, PC, etc.- places a wide range of both opportunities and hazards.

On the one hand, each person owns various types of digital resources, such as data connectivity, energy, computational power, environmental information, embedded in his private consumer electronics device's software and hardware. Some of these resources are available to one person and in short supply to the others. On the other hand, there is no widespread technology that enables resource sharing of such needed means, pro bono or for profit, and even if such technology existed, the current day-to-day cyber-attacks, threats, and the limited trust between persons, acquaintances and strangers, would prevent such resource sharing.

Imagine a tourist or a businessman, landing in San-Francisco, while his smartphone has almost no battery power and his roaming data plan doesn't work properly. A stranger nearby might give him 20% percent of battery power and provide him with access to his local mobile data plan. This resource sharing exchange would take place while maintaining three key qualities:

- **Trust** - the two strangers can totally trust each other for sharing the agreed upon resources and fee
- **Security** - the resource sharing is conducted between ultra-secured cyber protection devices, that prevents aimed or deceive cyber-attacks between the devices, and without compromising the security of the parties and the resources, while conducting the mobile data tethering process
- **Monetization support** - in the future, SIRIN LABS intends on supporting the monetization of each resource owner, allowing him or her to gain micro payment fees for his or her contribution (not by means of SRN Tokens), based on the trust of the blockchain infrastructure (see section 9).

SIRIN LABS's ecosystem and SIRIN OS™, its products deliversand services deliver the opportunity to execute a widespread, trusted and cyber protected, peer-to-peer resource sharing, from one consumer electronic device to others. This ecosystem gives the community of Blockchainblockchain developers the opportunity to create a diverse domain of trusted and secured resource sharing applications and services, per micro payment, (not by means of SRN Tokens), for example:

- **Resources** - data connectivity, energy, computational power
- **Data** - local weather, traffic status
- And the sky is the limit

3.4 Need for Fair, Decentralized App-Store

Most users retrieve the apps they use through an app store, managed by the OS vendor of their device. These stores provide users with little value, mostly in the form of auditing and reviewing apps ensuring better protection of the users from malware, at a high cost: store charge roughly 30% of the developer's proceeds, including most forms of in-app payments, out of developers' pockets. Most estimates put the combined revenues of Apple and Google from operating their app stores in recent years at between 50b$-100b$ annually.

But the damage to users is even higher. The operators of the app stores use their monopolistic power to impose censorship on the app offering: from barring apps that contain unapproved contents (such as gambling or adult content apps), to bolder limitations on apps that pose a risk to the operator's business (for example, Apple blocked all blockchain wallets for the lion's part of 2014).

SIRIN's D-App Store is a decentralized store for any type of app, in which users pay developers 100% of their subscription fees directly. Auditing services providing security protection, parental control etc. may be provided by trusted 3rd parties and sold directly to the subscriber.

4. PRODUCT

SIRIN LABS' Unique Proposition

Decentralized networks introduce tremendous challenges starting with network scalability, payment speed, security and privacy. Based on SIRIN LABS' legacy in developing and launching the SOLARIN smartphone, we plan a new distributed OS (SIRIN OS™) which is used by the FINNEY™ smartphone and PC connected devices, to address these upcoming challenges.

4.1 State-of-the Art, Secure & Blockchain Smart Devices

SIRIN LABS is developing its second-generation of products – the FINNEY™ smartphone and FINNEY™ 'allin-one' PC. These devices will operate using the SIRIN LABS' open-source SIRIN OS™, an Android™ based operating system with an ultra-secure cryptography core. SOLARIN, the SIRINLABS legacy products will be available as well to be purchased using the SRN Token (with a discount of 10% from retail maximum price).

4.1.1 SOLARIN ™ Smartphone

SOLARIN, the ultra-secured, Android-based, smartphone, features SIRIN LABS's Security Shield, and a complete suite of security features

High-level Specification:

Features:

- SIRIN LABS Cyber Protection suite:
- Behavioral based Intrusion Prevention System (IPS)
- Physical security switch (for secure call and massage)
- Secured communications (VoIP, text, email)
- Two factor authentications – Biometric (Finger, Lock Pattern)

Hardware Specifications:

- Display 5.5'' QHD
- 128GB of internal memory storage
- 8GB RAM
- Wi-Fi 802.11ac / WiGig
- BT 4.0
- 24MP Main camera
- 8MP Wide-Angle selfie camera

4.1.2 Secure calls and massages app & services

SOLARIN, the ultra-secured, Android-based, smartphone, features SIRIN LABS's Security Shield, and a complete suite of security features.

Communications application which applies multiple layers of security to assure that all communications are protected end-to-end; from special hardware in the SOLARIN, and authentication of the communication parties, to 256bit AES end-to-end encryption (FIPS 140-2 certified).

The SRN tokens can be used for purchase and expansion of the secure calls and messages bundles from SIRIN LABS. The application is compatible with all common Android and iOS devices.

4.1.3 FINNEY™ Smartphone

The SIRIN LABS product line will include the first smartphone for the blockchain community. FINNEY™ Smartphone is an affordable (~$999) ultra-secure and impeccably-designed smartphone, that will incorporate advanced blockchain and cryptocurrency trading algorithms to ensure the transactions integrity.

High-level Specification:

Target price range: ~$999

Blockchain features:

SIRIN OS™:

- Secure P2P resource sharing
- Built-in hardware "cold storage" crypto wallet
- Distributed Ledger Consensus

SIRIN LABS Cyber Protection suite:

- Behavioral based Intrusion Prevention System (IPS)
- Blockchain based full tampering proof
- Physical security switch (for wallet protection)
- Secured communications (VoIP, text, email)
- Three-factor authentications: Biometric (Iris & Finger), Lock Pattern, Behavioral

Hardware Specifications:

- Display 5.2'' QHD
- 256GB of internal memory storage
- 8GB RAM
- Wi-Fi 802.11ac
- BT 5.0
- 16MP Main camera
- 12MP Wide-Angle selfie camera

4.1.4 FINNEY™ PC

SIRIN LABS' product line will include an affordable (~$799) ultra-secure and impeccably-designed all-in-one PC, the FINNEY™ PC.It is built on "thin client" practices with additional computational power, such as (GPU/ CPU/RAM) that can be added based on SIRIN LABS P2P resource sharing protocol or cloud base service.

High-level Specification:

Target price range: ~$799

Blockchain features:

SIRIN OS™:

- Secure P2P resource sharing
- Built-in hardware "cold storage" crypto wallet
- Distributed Ledger Consensus

SIRIN LABS Cyber Protection suite:

- Behavioral based Intrusion Prevention System (IPS)
- Blockchain based full tampering proof
- Physical security switch (for wallet protection)
- Secured communications (VoIP, text, email)
- Three-factor authentications:
  Biometric (Iris & Finger), Lock Pattern, Behavioral

Hardware Specifications:

- 24” 2K Display
- Biometric security
- 8GB Memory
- 256GB storage
- Wi-Fi 802.11ac

*specifications are for local “thin client”. Additional computation power can be added based on SIRIN LABS cloud base service.

4.2 SIRIN OS™

The FINNEY™ Smartphone and FINNEY™ PC devices will use the SIRIN LABS’ open source SIRIN OS™, an Android™ based operating system with an ultra-secure cryptography core. At the center of the SIRIN OS™ there is a distributed, scalable, light-weight, and ASIC-resistant ledger. SIRIN OS™ is designed and ready to run on millions of smart electronic devices around the globe. SIRIN OS™ implements an ultra-secure, peer-to-peer cryptocurrency transactions mechanism with a user-friendly, hassle-free interface. Those are the enablers: feeless & fast payments (without involvement of SIRIN LABS), resource sharing, and service offering. To ensure the integrity of the distributed leger transaction, SIRIN OS™ will offer multi-layered cyber protection. It makes use of innovative methods to secure the weakest link in cryptocurrency transactions, which is in the interface between the wallet, the internet connection, and the blockchain network.

SIRIN OS™ is built with the following features:

4.2.1 BlockShield™

BlockShield™ is SIRINLABS’ propriety technology that ensures the integrity of transactions. BlockShield™ consists of multiple protection layers built into the devices manufactured by SIRIN LABS, Trusted Display, IP Address Hiding and MAC Address Randomization.

4.2.2 Built-in hardware "cold storage" crypto wallet

The main goal of the wallet is to safeguard the user’s private key. The wallet also displays the user’s balance, transactions history and public address. It is hardware based embedded inside the TrustCore ™, a tamper-resistant secured element, which is protected by SIRINLABS’ BlockShield™ technology - a secure area, protected by a physical switch. When the embedded wallet is not being used, it will be physically and electronically disconnected from the network.

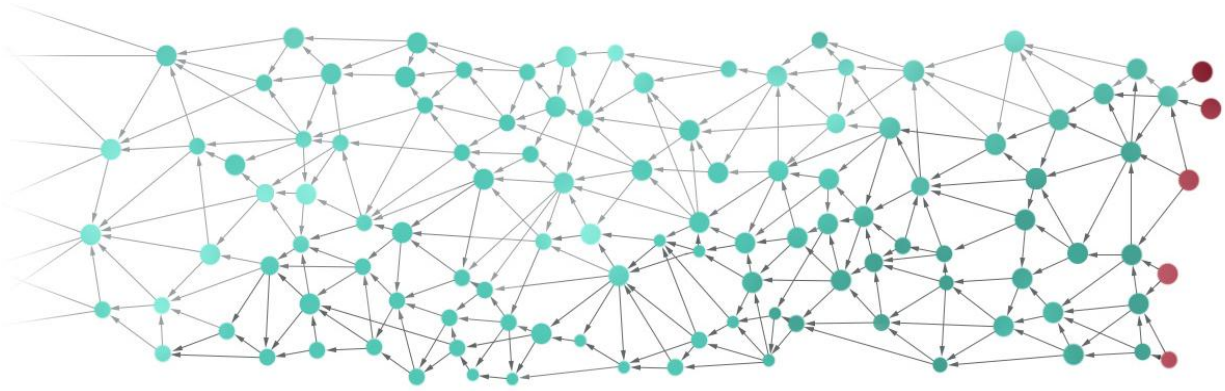
The wallet will allow holding multiple accounts and will support Bitcoin, Ether, Litecoin, Dash, Zcash, Ripple, Stratis, Dogecoin and other leading cryptocurrencies. Furthermore, it allows to hold the SRN Tokens.

4.2.3 Cyber Protection

The entire device is being multilayered cyber protected, ranging from low level OS up to the application layer. Acknowledging the dynamic nature of cyber threats, SIRIN LABS is developing a multilayer, behavioral-based and machine-learning Intrusion Prevention System (IPS).

4.2.4 Distributed Ledger Consensus (DLC) module

The DLC module enables approving transactions with a fee-less consensus mechanism, which allows fast payments between the network peers, without the need for mining. The consensus is based on a Tangle network consensus algorithm.



4.2.5 Decentralized App-Store (D-AAP)

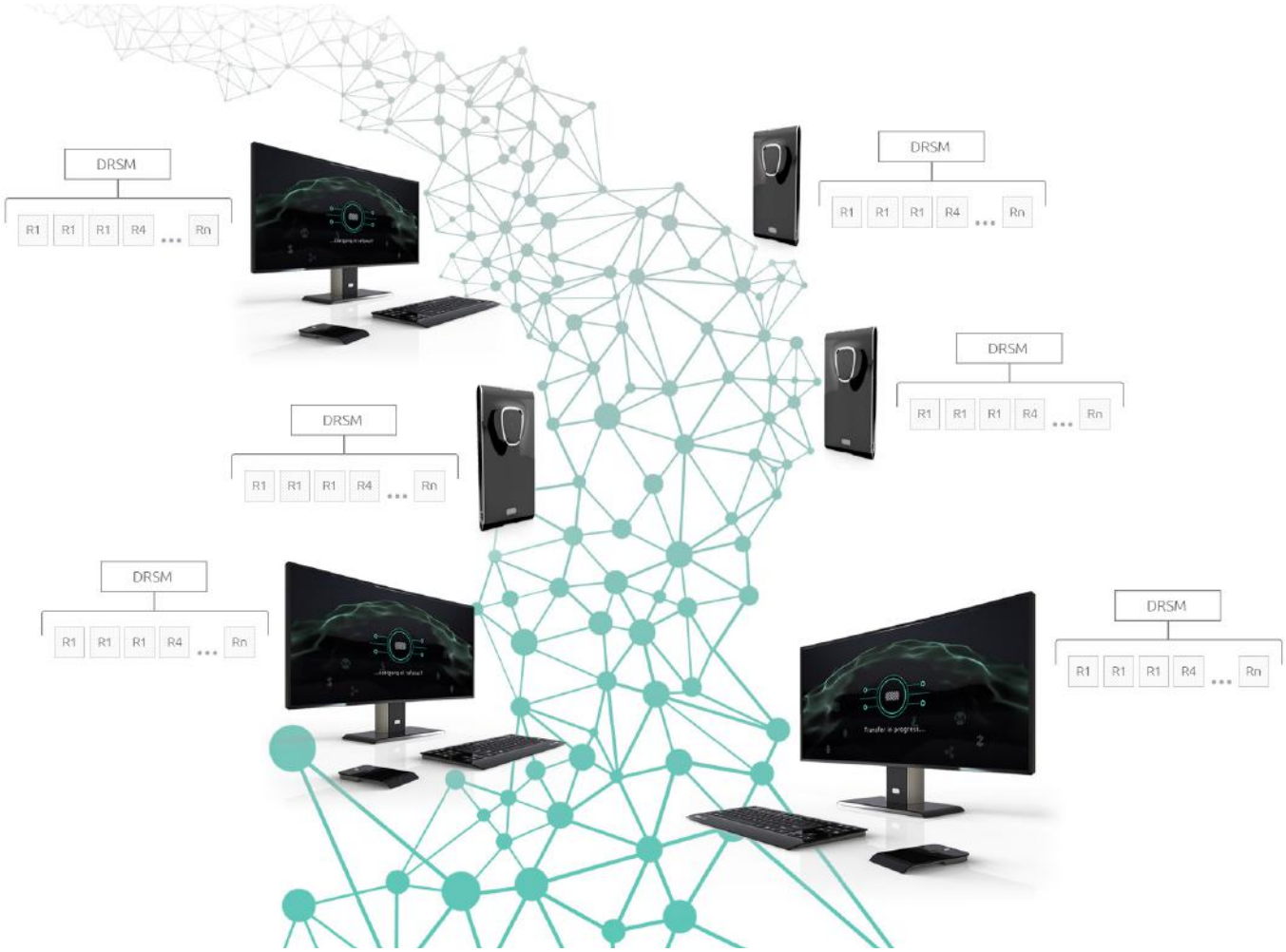
We believe that variety, collaboration and openness are key to the success of the app ecosystem on SIRIN OS™. To stimulate SIRIN OS™, SIRIN LABS will introduce the D-APP Store - an open, fee-less and censorship-free marketplace for apps. The D-APP Store is a digital distribution channel for apps and services, providing developers with distribution, subscription management and in-app payments solutions, and providing users with discovery, updates and auditing services.

Unlike conventional centralized app stores, SIRIN OS™ App Store will be managed by the community in a decentralized way: users may use the services of a trusted auditor of their choice to review, rate and/or filter the assortment of apps they see.

Paid apps and in-app payments will be based on secure peer-to-peer resource sharing which will distribute the fee between app and services developers and end users. Much like conventional app stores, users will be able to search for apps and services based on predefined categories.

4.2.6 Peer-to-Peer Resource Sharing Market Module

SIRIN OS™ offers developers a software development kit (SDK) that enables access to the OS's blockchain features and functionalities, which in turn offer sharing of digital resources and services between peers or group of users. These services can be based on the device's camera, data, storage, security, location etc.



4.2.7 SDK for Distributed Applications Development

SIRIN LABS will offer developers worldwide a Software Development Kit (SDK) that enables faster and more secure development of distributed apps for the blockchain generation, based on our network capabilities and functionalities, taking advantage of a seamless and secure peer-to-peer resource sharing and payment system (not by means of SRN Tokens).

SIRIN LABS' SDK will implement and make available all the building blocks of decentralization – gossip protocol, decentralized database, voting/polling mechanism and oracle API.

Using SIRIN LABS' SDK, developers could get directly paid for software, services and tangibles. In addition, users can make "in-app" micropayments.

5. SIRIN LABS SECURE BLOCKCHAIN TECHNOLOGY

5.1 Overview and Requirements

SIRIN OS™, the basis for FINNEY™ devices, is a freely distributed open source operating system based on Android™, designed to enable safe use of blockchain applications on mainstream devices. The SIRIN OS™ provides an enhanced blockchain features, decentralized resource sharing and a lightweight, fee-less and quantum-proof transactions of cryptocurrencies (without involvement of SIRIN LABS).

5.1.1 Security Requirements

To enable mass market adoption of blockchain technologies, cryptographic tools should be a simple and foolproof. Experience with the first generations of connected payment systems shows that any vulnerability that may exist between the moment a sensitive information is processed (on a network or storage) up to the moment it is displayed to end users (such as on display) is eventually exploited, and at large scale. Complex procedures of maintaining key pairs, protecting private keys, planning one's recovery procedures and verifying transaction data are routine for today's blockchain users, but cannot be routine for all users.

The security scheme used in SIRIN OS™ must ensure that private keys are never exposed, and can only be accessed by a limited set of "secure mode" procedures, that are included in the OS, that authenticate the user and sign transactions or method calls with the keys. Keeping the secrets out of reach is the only way to ensure that it is impossible to steal them by using malware, by exploiting a bug in an app or even by cheating the user into sharing his secrets.

Additionally, users must have a simple and foolproof way of distinguishing fake from real payment interfaces, to protect them from phishing attempts. This requires a physical indicator on the device shell of when the device is in secure mode. Such indicator can be a unique LED, a physical switch, or even a separate screen for secure mode operations. Users of the device only need to learn that the physical indicator must be set in order for them to make payments or other secure operations.

While the above requirements are mandatory to prevent wallets being compromised by theft, phishing or keylogging, one must note that the advanced features enabled by FINNEY™ create new opportunities for attackers. Specifically, we believe that resource sharing (and particularly sharing of CPU and network resources) could create a risk of eavesdropping and breach of access restrictions. To mitigate that risk, FINNEY™ will feature cybersecurity elements as a service by SIRIN LABS.

5.1.2 Blockchain Requirements

The blockchain operations provided natively by SIRIN OS™ can be used on any common blockchain technology. However, for common usages of payments and resource sharing, we find that none of the current standard blockchains is suitable for mainstream users.

The native blockchain used for payments and resource sharing must provide fast transaction confirmation, ensure extremely low transaction costs to enable micropayments, and have light clients capable of operating nodes on devices with entry-level CPU and limited network connectivity. PoW design that enables a long-state equilibrium in which user devices do most of the validations in the network, rather than centralized mining pools, is also required to ensure the long-term independence of the network.

5.1.3 Hardware Adaptation Requirements

To comply with the private-key protection schemes and anti-phishing measures required by SIRIN OS™, two security requirements must be aided by hardware elements: protection of private keys from application access, and user protection from phishing.

Naturally, special hardware requirements may add a burden on manufacturers and designers, which we must ensure will not be a barrier to widespread adoption of SIRIN OS™. To counter that, SIRIN LABS will provide a choice of hardware designs (and certify other designs if suggested by 3rd parties) that can satisfy these requirements, allowing OEMs to choose the design that can best fit their constraints.

5.1.4 Resource Sharing Requirements

Perhaps the most promising capability of a blockchain device is its ability to dynamically trade its resources with other devices, thus providing its users with better experience as they need it and better utilizing its resources when not in use.

Resource sharing must be seamless, secure and efficient for mass-market users to enjoy it. SIRIN OS™ introduces a virtualization layer between the OS interfaces and any of its shareable resources, making access to each of the resources virtualized both by the sharer and by the receiver. This ensures that partners to a shared resource (such as network or CPU) cannot undermine each other's security or privacy. The virtualized containers will also provide accurate metering of the shared resource; the sharer meters the amount of use of the shared resource at his sole discretion.

Two types of resource sharing protocols will be designed: LocalBoost™ for sharing resources with directly-connected devices, and CloudBoost™ for sharing resources over the network. SIRIN LABS will publish an RFC for both protocols. Being open protocols, any device -- not just SIRIN OS™ devices -- may contribute or use resources; this allows WiFi routers, cloud or edge-cloud computing services, public charging stations and many other devices to be also a part of the resource sharing network.

5.1.5 Development Methodology

SIRIN OS™ is developed in accordance with the SDLC (Security Development Lifecycle), and OWASP SCP including secure coding and penetration testing done by specialized 3rd parties and occasional hacker bounties.

5.2 Hardware Designs and Abstraction Workflows

Ensuring the secure use of blockchain apps by user requires hardware capable of secure execution: isolating private-key usages from other functionalities, in such way that secure code can access its own secure storage, and that its communications to the display and user input device(s) are protected from eavesdropping or manipulation by insecure code. Another required hardware capability is visual indication: there must exist a clear and simple indication for the user of when the device is in secure mode.

SIRIN LABS will provide at least two hardware designs to meet the secure execution requirement: one requiring that the main chipset be of an architecture that support secure enclaves (such as TEE - Trusted Execution Environment supporting chips), and one supporting any chipset when connected to a Secure Element (SE) chip. The former will enable OEM hardware vendors to adapt their existing board designs to use

SIRIN OS™ with little or no changes, whereas the latter may require new board designs but due to the low cost of SE chips, will have minimal effect on the overall BOM.

To meet the visual indication requirement, we recommend a physical switch requiring the user to actively move the switch for transition between secure and ultra-secure modes. Alternatively, a dedicated indicator LED that will only light up when in secure mode can be used. The indicator should be easily distinguishable from any other visual indicator on the device, making it easy for users to learn that they should only authenticate transactions when in secure mode.

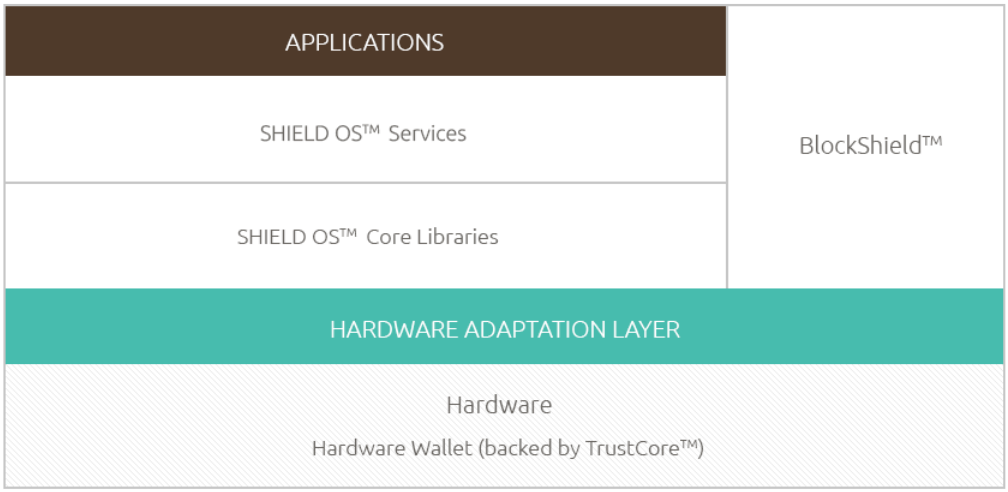
Example: Abstract Workflow

Although the design alternatives use different approaches to isolating the wallet storage and computation, and to the physical indication of secure I/O, all use the same abstract workflows for wallet operations. For example, currency transfer follows this workflow:

1. The user chooses to send currency in a supporting app, (e.g. a peer-to-peer messaging app)
2. The app creates a document containing the transaction details ("raw transaction"). Optionally, the app may attempt to acquire the destination address' owner certificate - an SSL certificate indicating that the real-world name and address of the recipient.
3. The app calls the SignTransaction() method of the "Wallet Interface Service" provided by SIRIN OS™. This call sends the raw transaction to the wallet hardware (either secure enclave or an SE chip).
4. Secure mode visual indication is turned on.
5. The hardware wallet displays (on secure display) the transaction details: amount transferred and destination address; if an owner certificate was attached to the transaction, the recipient name and address will also be shown. It then asks for user authentication for approval of the transaction.
6. If the user authenticated and approved the transaction, the secure code will sign the transaction using the private keys stored in the secured storage and send it back to the app. Next, it will exit secure mode.
7. Secure mode visual indication is turned off.
8. The messaging app is back in control, it received a signed transaction which it may send to the blockchain to commit the transaction.

5.3 Architecture

Adaptation Layer and HAL



The Adaptation Layer and the HAL (Hardware Abstraction Layer) defines a standard interface for OEMs to integrate SIRIN OS™ on top of their existing Software / Hardware platforms, in order to abstract resource access in a secured manner.

Just as the resource sharing protocols, LocalBoost™ and CloudBoost™, are not limited to a specific device -- the abstractions built into SIRIN OS™ to support hardware can be ported to any type of devices or on top of an existing Operating System.

5.4 System Services and Core Libraries

System Services are modular components exposed by the SIRIN OS™ to the Application Framework and its APIs.

The system services cooperate to provide the core functionality of the SIRIN OS™ over existing hardware devices by taking advantage of the SIRIN OS™ stack of core libraries.
The core components of the System Services layer are:

5.4.1 DLC: Decentralized Ledger Component

To best meet the requirements of the native blockchain (fast, fee-less, scalable transaction over light clients), SIRIN LABS is cooperating with IOTA Foundation with the intention of integrating a Tangle-based Ledger Technology into SIRIN OS™ (IOTA Tangle is described in [1]).

The DLC is a component that is designed to meet the implementation requirements of IOTA:

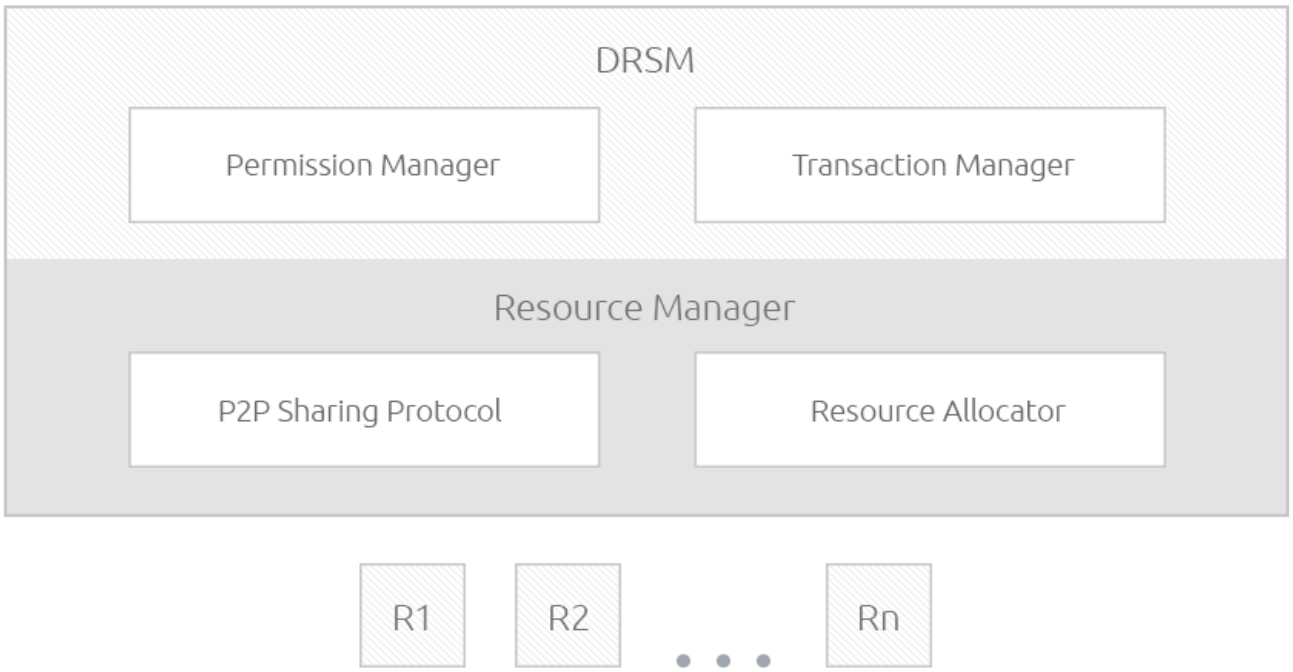
- Managing secure P2P transactions among devices over the Tangle network
- Perform the Tangle's Tip Selection algorithm as described in IOTA whitepaper.
- Performing hash calculations and verify selected previous transactions.

5.4.2 Wallet Interface Service

In SIRIN OS™ devices, access to private keys is only available for the hardware wallet module. The Wallet Interface Service provides apps with API access to the wallet, enabling them to have currency transfers and smart contract calls signed. The hardware wallet (either running on a separate chip with its own storage, or in an enclave with exclusive access to the secure storage holding the private keys) asks for user authentication and approval, and returns the signed transaction if approved.

5.4.3 DRSM: Decentralized Resource Sharing Manager

The DRSM (Decentralized Resource Sharing Manager) is responsible to allocate, authorize and share resources over a decentralized network in a secure, trusted and private fashion. A background service operated by DRSM manages payments to resource sharers according to a dynamically calculated cost-benefit protocol.



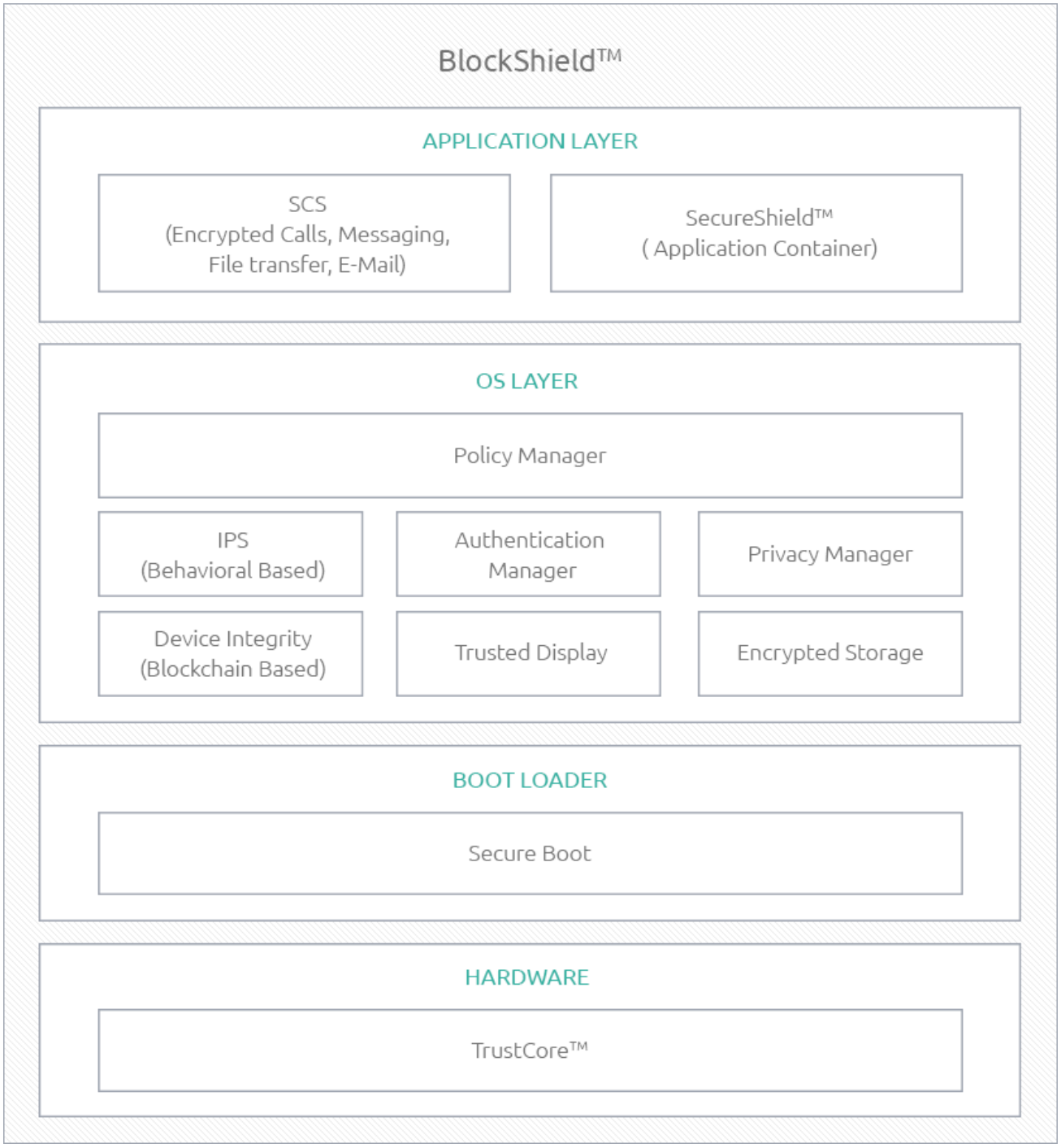
Among the resources managed by DRSM are:

- Device sensors data
- Network connections
- CPU time
- GPU time
- Device storage

  and more.

5.5 BlockShield™

As SIRIN OS™ is designed as an inherently secure architecture, in addition to providing secure blockchain operations it can provide a toolkit of security and privacy-related services. Parts of this toolkit are designed to provide security features to non-blockchain use are optional and OEM vendors may choose not to embed it in their products.



5.5.1 Application Layer

SecureShield™ (Application Container)

The SecureShield™ provides a Sandbox protection at the OS level to protect selected applications (such as Wallet apps, Encrypted VoIP/Messaging, Encrypted E-mail, etc.) The SecureShield™ provides applications with permission based isolation from accessing device and system resources such as:

- **Sensors:** Camera, Microphones, Vibrator, Speakers, Motion, GPS,
- **Communication:** Bluetooth, NFC, Cellular calls and SMS
- **Peripherals:** USB, HDMI, Serial/Parallel Ports
- **System Processes:** Audio or Video Recording, App installation, Screenshots, Factory Reset, and Debugging

Further access protection to application that are guarded by the SecureShield™ can be done through a physical security switch and two factor authentications that is managed by the Authentication Manager.

SCS: Secured Communication Suite (optional for OEMs)

The Secure Communication Suite is a set of comprehensive endpoint-to-endpoint encryption solutions that provide secure communication on connected devices to safeguard sensitive conversations against eavesdropping by malicious actors.

SCS is comprised of secure and encrypted Voice Calling, Secure Text Messaging, File Transfer, E-mail
SCS uses a PKI cryptosystem stored in a hardware-protected keystore stored on SIRIN LABS TrustCore ™. The robust encryption framework leverages 2048-bit RSA and a cryptosystem with AES 256-bit symmetric session keys.

As we expect developers and vendors to adopt SIRIN OS™ enhance the security and privacy of communications and resource sharing developments and bring SIRIN OS™ advantages to the public, so is SCS applications enhance its security and privacy by using SIRIN OS™ APIs.

SCS uses SIRIN OS™ for various use cases like:

1. Service authentication.
2. Negotiation between peers, for example: encrypted call establishment.
3. Payments and Micro payments, for example:
    - Charge users for app services.
    - Transfer payments between users
4. Security resources sharing, for example:
    - User can lease his device hardware encryption engine.
5. Post an alert to others when a threat is detected

5.5.2 OS Layer

Policy Manager

The Policy Manager aggregates data that is collected from sensors embedded in the OS kernel, as well as in the device firmware. It can execute actions and countermeasures to dynamic cyber threat policies, to contain and restrain the cyber-attacks. Example for such actions and counter measure are:

- Pausing / Blocking SW Installations
- Blocking Connections
- Terminating Suspected Processes

etc.

SIRIN LABS PROTECTOR™ backend system manages cyber threat dynamic policies, according to day-to-day changes in the worldwide landscape of cyber threats. These policies are pushed OTA to the devices upon need.

IPS: Behavioral-based Intrusion Prevention System (optional for OEMs)

Acknowledging the dynamic nature of cyber threats, SIRIN LABS is developing a multilayer, behavioral-based and machine-learning IPS, protecting against known and unknown threats (including Zero-Day

attacks). This relies on our extensive experience developing SOLARIN, the most secure smartphone in the world. ("Meet the safest smartphones in the world!" – https://bballmaster.com/meet-safest-smartphones-world/).

BlockShield™ includes a continuous on-device behavioral-based cyber-protection engine, against networks attacks, host-based (malware) attacks, and physical attacks. The IPS engine, which is in an Always-On state (including during offline and flight mode), monitors the entire device for malicious behavior and dynamically detects in real-time both known and unknown threats and attacks (including Zero-Day).
The IPS engine identifies, prevents and shields the devices against a wide range of cyber threats and attacks from diverse entry points, such as:

- WiFi Network attacks – ARP MITM (Man-in-the-Middle), traffic-tampering, SSL strip, ICMP redirect MITM, fake SSL certificate attacks, rogue WiFi Access Points, or
- Suspicious baseband behavior - Such as Silent SMS, unexpected downgrade of 3G/4G encryption, etc.
- Host-based attacks (behavioral-based and not signature-based) – suspected APK (from the Google Play store, other app stores, website, email, and FTP), EOP (Elevation of Privilege), system tampering, device jailbreaking or rooting
- Physical attacks – ROM tampering, preloaded application authenticity tampering, hardware tampering

The IPS engine is backed-up with a Cyber-Incident Response Team (CIRT), that enhances the cybersecurity level of the devices using proactive monitoring and analysis. The CIRT investigates the online cyber threats and mitigates them to assist customers with managing security issues related to usage of the devices.

Authentication Manager

Recognizing the inherent weaknesses of traditional self-determined authentication methods, such as PIN, pattern, or password, SIRIN LABS offers a range of authentication methods, integrating methods of self-determined authentication with biometric authentication.
BlockShield™ supports two sets of authentication methods, one set for each zone (the "regular" zone and the shielded zone). For each set, the customer may choose which authentication methods to use to protect their privacy and security.

Optional authentication methods include:

- Self-determined – password, PIN, pattern, swipe, or none
- Biometric – fingerprint, iris recognition and/or retina scan (on supporting devices)

The devices enable the end-user to determine the authentication protection level of the selected section:

1. None
2. Self-determined only
3. Self-determined + single biometric authentication
4. Self-determined + double biometric authentications
5. One-factor biometric authentication
6. Two biometric authentications

The self-determined and biometric prints are stored in a hardware-secured element within the smartphone and within the all-in-one computer, enhancing the security level of this sensitive data.

Device Integrity (optional for OEMs)

One ominous threat in the cyber-security landscape is that of hardware and software tampering of consumer electronic devices. The main counter-measure is to tamper-proof the hardware and software components' authenticity.

SIRIN LABS is developing an advanced, unique blockchain-based, tamper-proof mechanism, for both the hardware and software components of electronic devices. Device Integrity subsystem verifies mechanisms to verify the authenticity of firmware and hardware across devices:

Hardware Tampering Prevention (optional for OEMs)

The Device Integrity module supports the integration of secure device assembly inside factory using supply chain management that is controlled by blockchain.

Selected hardware component's authenticity verification is done throughout their lifecycle, from their assembly line by the ODMs, through shipment. Selected component's hash is stored on a distributed ledger and verified against the associated devices of SIRIN LABS' blockchain network.

Any attempt to tamper with or replace the selected hardware components of the devices is detected by the Device Integrity module and cause in IPS event which can be propagated to UI indication to the customer, and appropriate countermeasures according to the analyzed severity of the incident.

Firmware Tampering Prevention (optional for OEMs)

Similarly, any attempt to perform unauthorized software update or replacement of the device sensitive components (such as bootloader, Kernel, System Services, etc.) and other sensitive selected software components, is detected and causes an event in the IPS, with appropriate functional countermeasures.

Secure Boot (optional for OEMs)

The Secure Boot mechanism that is built into BlockShield™ guarantees the integrity of the device software starting from a hardware root of trust up to the system partition. During boot, each stage verifies the integrity and authenticity of the next stage before executing it.
Any integrity violation that is detected during boot is reported to the IPS to provide warning on the local device and the boot sequence is hold.

Encrypted Storage - (optional for OEMs, except in hardware wallet)

The Encrypted Storage subsystem support an integration of full encrypted storage that is backed by either software or hardware.

Trusted Display

The Trusted Display ensures that the information typed by the end-user is securely controlled by taking advantage of Trusted Execution Environment (such as TrustZone by ARM, QSEE by Qualcomm, etc.). Trusted Display protects and validates the input-output chain, starting from the input device (such as touch screen, fingerprint sensor, keyboard, or mouse) up to the user interface and the device’s physical display.

Whenever a user makes a transaction, the information displayed is derived from the TEE, which prevents any non-secure application, potential malware or malicious actor from tampering with or sniffing the transaction details.

Privacy Manager (optional for OEMs)

The Privacy Manager subsystem provides a togglable anonymization to protect user's privacy.

MAC Address Randomization (optional for OEMs)

Whenever a transaction is initiated on a blockchain, the client sends the necessary data to other clients, effectively broadcasting the transfer to the network. As most blockchain protocols do not encrypt their traffic, it is possible for prying eyes or a malicious actor to peek into the transactions and determine the wallet's balance with little effort. For a sophisticated third party, it is therefore entirely possible to gather data about transactions performed and reveal the identity of cryptocurrency users at large.

The Privacy Manager, also supports integration to VPN provided by 3rd parties.

5.5.3 Hardware Layer: TrustCore™ (optional for OEMs*)

SIRIN LABS TrustCore™ is a tamper resistant hardware Secure Element (SE) capable of securely hosting confidential and cryptographic data (e.g. key management) and using them for transaction authentication without exposing the secret data to the main CPU or storage.
SIRIN OS™ uses TrustCore™ to securely store:

- Encryption keys (Encrypted Storage, Encrypted Communication, etc.)
- Biometric templates (such as fingerprints, retina, iris)

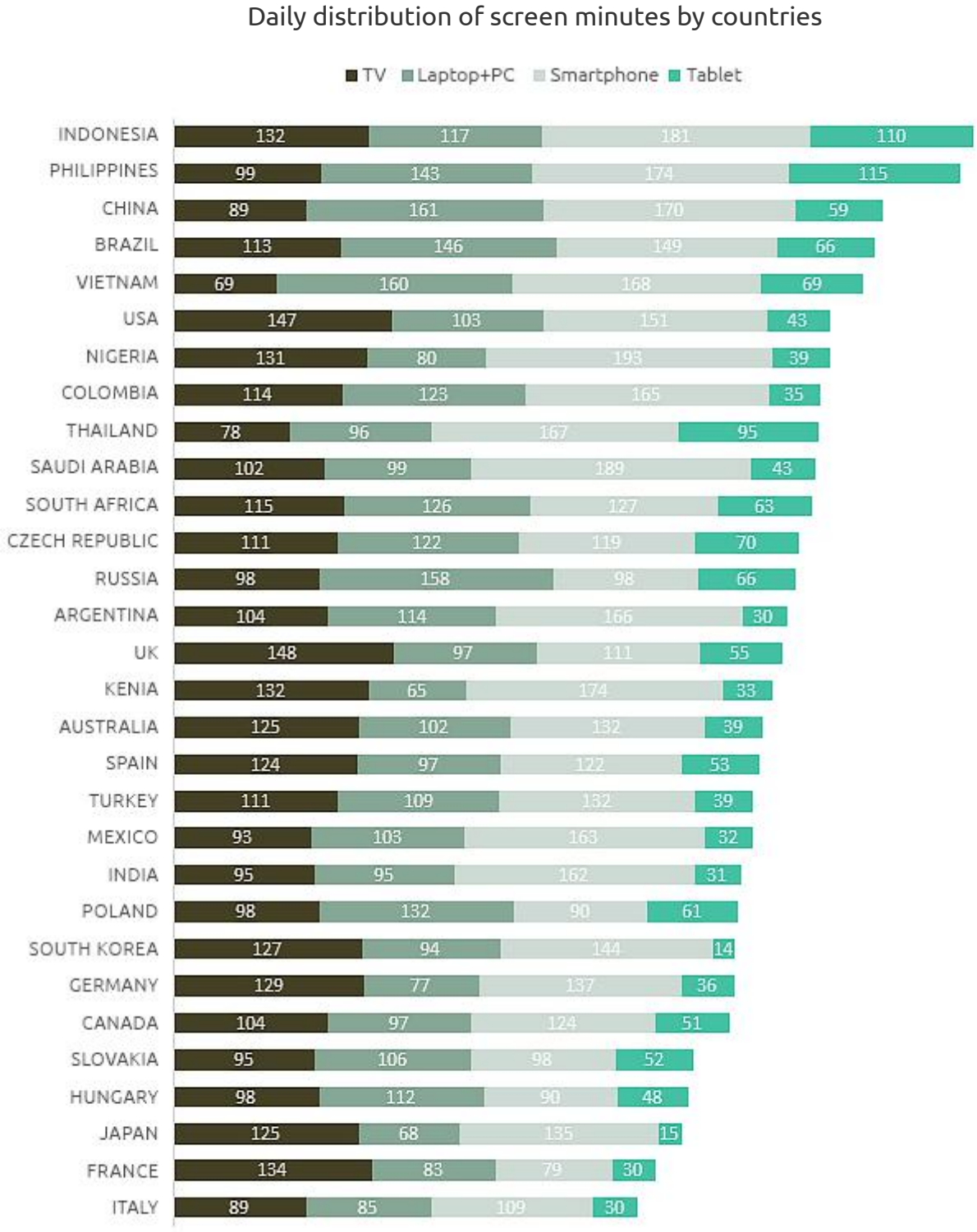
(*) OEMs adopting SIRIN OS™ may choose to use other Secure Element chips based on compliant specification.

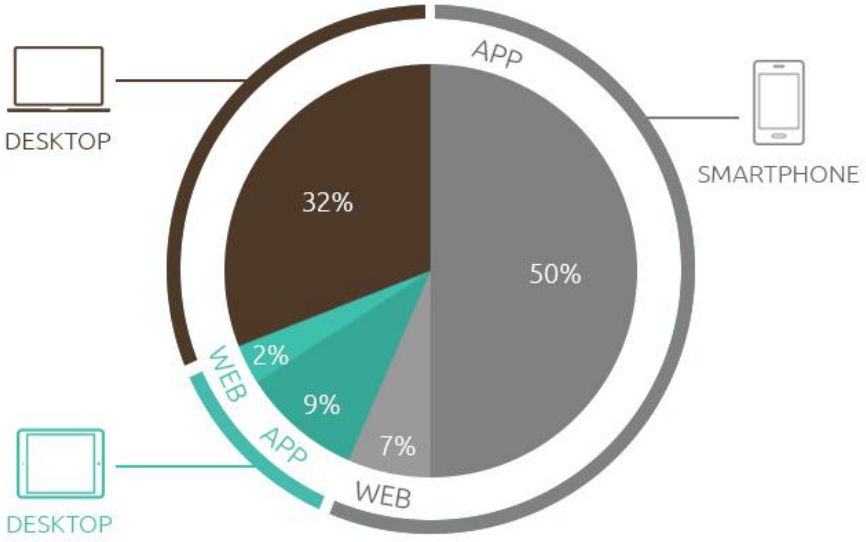
6. MARKETING PLAN

6.1 General Market Data

SIRIN LABS' blockchain solution solves key problems (security, privacy, trust) on the most used electronic devices, like mobile phones and personal computers.

In 2016, 1.6 billion mobile and PC units were sold worldwide. In addition, mobiles and PCs are used mostly for communication and screen viewing.





6.2 Security in the Blockchain Era

Data privacy has become a huge issue: cybercrime is estimated to cost individuals and companies a staggering amount. The cybersecurity market is estimated to grow from $137.5 bn in 2017 to over $232 bn by 2022.

Global expenditures on mobile and network security are growing at an estimated annual rate of $11 bn. Existing offerings in the commercial secure phone and PC market are very limited and unattractive for consumers. Examples include the GSMK Cryptophone and Blackphone2. FINNEY™ will be the first line of secure devices to incorporate the best blockchain security practices, offering a high level of usability to meet our clients' lifestyle needs.

6.3 Target Audiences (SIRIN OS™ & Featured Products)

SIRIN LABS specialty is the development of ultra-secure consumer electronics. Blockchain technologies bring a wealth of opportunities - and relieve pain in the fields of security and privacy, particularly for two key audiences:

1. **CROWDSALE participants** - mostly comprised of early adopters.

Crowdsale participants have evolved from being 'early adopters' into far more savvy traders, relying on funds and institutions. Funds obtained from a crowdsale act as a pool of capital. Due to their size these will surely play a leading role for future cryptocurrency contributors.

2. **OEM's (Original Equipment Manufacturers)** – Beside installing SIRIN OS™ on our feature products and based on early discussions with manufacturers around the world we strongly believe that our unique OS will be appealing to many of the leading consumer electronics companies who wish to enter the blockchain domain.

3. **Community of Developers** - SIRIN OS™ SDK is designed for the blockchain community of developers, who are known to be a group of passionate techies who want to help create a better world through the power of blockchain

4. **Consumers** - blockchain technologies and cryptocurrencies are considered to be too complex for 99.99% of the population. SIRIN LABS' unique consumer electronic products, FINNEY™ will offer the first real opportunity to connect give everyone access to cryptocurrencies.

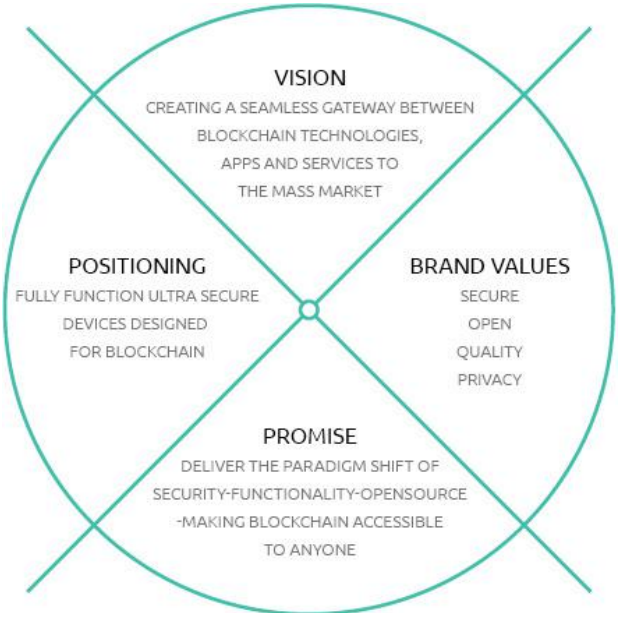
SIRIN LABS' security and privacy protocols are implemented at the core of SOLARIN and FINNEY™ products. Moreover, pricing points are set at an attractive and competitive level. The easy-to-use cold wallet and SRN economy will be user friendly and easy to use, giving access to every consumer who wishes to buy our products and become part of the blockchain revolution.

6.4 The SIRIN LABS Brand

According to Russian mythology, "sirins" are beautiful creatures that only truly happy people can hear. They are as fast and difficult to catch as human happiness, and symbolize eternal joy and heavenly happiness (Wikipedia). SIRIN LABS first product was SOLARIN, the world's most secure mobile phone, with the underlying brand values of **Security, Technology, Design and Quality**.

SIRIN LABS recognizes the importance of brand building, as we continue to develop consumer electronic goods. Looking forward we intend to make our products accessible to the mass markets, while maintaining our high standards and values.

Brand Compass

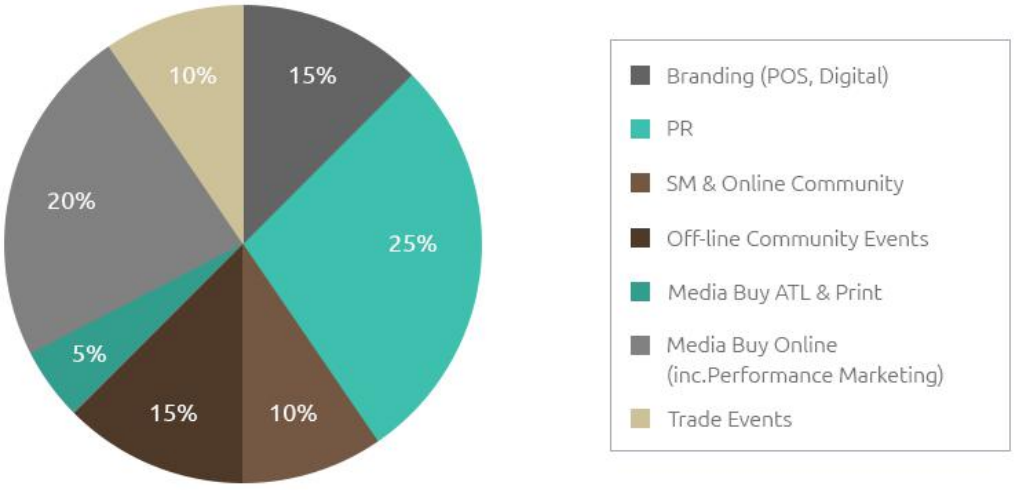


6.5 Go-To-Market (General)

CHANNEL	DESCRIPTION
Brand and branding	Establish a unique and distinct brand and product perception - vision, name, look and feel, values, messages and language
PR	Communicate the products and values via mass market and targeted media – such as trade publications and press conferences
Social media (Community management)	Delivering the products and values by creating 'stories' like news, insights, features, partnerships, and releases, via social media channels – such as Telegram, Facebook, Twitter, LinkedIn, YouTube, Medium

Media buy	Using paid channels to achieve marketing and sales objectives: the bulk of the budget will be allocated for online campaigns (SEM, PPC, FB ads, IG). Print and TV will be considered depending on the available marketing budget and online results
Affiliates	Use "pay per success" online channels (performance-based marketing)
Events	Attending trade events to showcase our products to establish awareness, sales, partnerships, and positioning
BTL (Below the line)	Deploy "brand enhancers" at points of sale to include staff training, branding elements and collaterals
E-commerce	Using e-commerce best practices. Enabling users, resellers and partners to engage with SIRIN LABS
CROWDSALE	Creating pre-launch buzz to support awareness and presales

Allocation of Marketing Budget



6.6 Sales & Business development

CHANNEL	SIRIN OS™	FINNEY™ Smartphone	FINNEY™ PC
OEM's	V	X	X
Wholesalers (distributors)	X	V	V
Consumer electronic retail chains	X	V	V
Online	TBD	V	V

7. SRN TOKEN SYSTEM & CROWDSALE DETAILS

7.1 The SIRIN LABS Token (SRN)

The symbol of the SIRIN Token is SRN. During the token sale, the SRN Token is implemented as an ERC-20 compatible token over the public Ethereum blockchain, and will be converted to a coin on the IOTA network towards the launch.

7.2 Purpose and Usage of the SRN Token

SRN Token will be available for usage and purchasing of SIRINLABS existing products and services, as well as for pre-order of future products.

7.2.1 Usage right after crowd-sale event ends

SRN tokens have the following usability that includes:

- Purchasing of the SOLARIN line products; SOLARIN smartphone, Beryllium earphone, international charger, with a discount of 10% from retail maximum price
- Purchasing of apps and services provided and operated by SIRINLABSSIRIN LABS, such as encrypted calls and messages, cyber security suite
- Pre-order of Purchase of SIRIN LABS FINNEY™ smartphone, and FINNEY™ all-in-one PC and other future hardware products, with a discount of 20% from retail maximum price

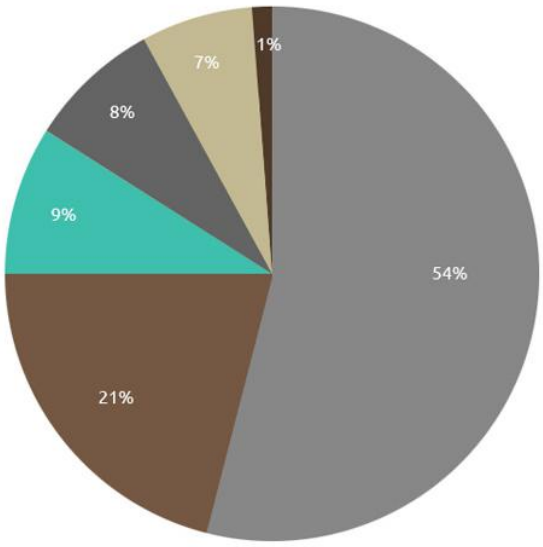
7.2.2 Upon releasing of FINNEY blockchain

- Purchasing of the FINNEY line products; FINNEY smartphone, FINNEY PC from SIRIN LABS
- Purchasing of apps and services provided and operated by SIRIN LABS through the D-App store, such as P2P resource sharing, encrypted calls and messages, cyber security suite
- Warranty, repair and other service packages from SIRIN LABS

7.2.3 Buying SOLARIN products and services using SRN

- The SRN Token can be used for purchasing SIRIN LABS's products, applications and services from the moment the SRN tokens are issued and distributed to crowdsale participants (24hr. after crowdsale ends). Moreover, special discounts will be given to SRN Token holders who pre-order or purchase products from SIRIN LABS using their SRN tokens.
- The SOLARIN is available for purchase at SIRIN LABS flagship store at 34 Bruton place, London, UK as well as online at www.solarin.com.
- The SECURE CALL AND MESSAGES application and services can be purchased from a SIRIN LABS representative, via any mean of communication as displayed at https://www.solarin.com/contact.

7.3 Use of Proceeds



USE OF PROCEEDS

COGS (Inc. Purchase of Inventory)	54%
R&D	21%
Operations	9%
Marketing	8%
G&A	7%
Others	1%
Total	100%

*** subject for change – based on management decisions ***

7.4 Token Issuance

To finance SIRIN LABS' roadmap and activities in the foreseeable future, the company plans to conduct a token sale of an initial supply of SRN tokens.
The sale event will last 14 days, with an uncapped amount of contribution. SRN tokens will be sold at a fixed price denominated in ETH and the initial supply will be dependent on the quantity of SRN tokens sold.

The allocation of total SRN tokens will be as follows:

- 40% of the total number of SRN tokens will be allocated to contributors during the token sale.
- 10% of the total number of SRN tokens will be allocated to the team and will be gradually vested over a 12-months period
- 10% of the total number of SRN tokens will be allocated to OEM's, Operating System implementation, SDK developers and rebate to device and SIRIN OS™ users.
- 5% of the total number of SRN tokens will be allocated to professional fees and Bounties.
- 35% of the total number of SRN tokens will be allocated to SIRIN LABS, to be used for future strategic plans for the created ecosystem, and as a reserve for the company.

During the Token sale event, there will be a pricing program to the contributors as following:

Duration from token Crowdsale event start	First 24 hours	2nd day	3rd day	4th day	5th day	6th day	7th day	8th day	9th day	10th day	11th day	12th day	13th day	14th day
SRN/ETH	1,000	950	900	855	810	770	730	690	650	615	580	550	525	500

8. ROADMAP

Our roadmap is based on three scenarios based of the level of contribution:

- $25M – we will develop and release the SIRIN OS™ for phone OEMs
- $50M – In addition to above, we will develop and launch the FINNEY™ smartphone
- $75M – in addition to phone, we plan to develop and launch the FINNEY™ PC

2014

2015

2016

2017

LEGACY

- 2014 - SIRIN LABS established
- 2015 - First SOLARIN prototype
- 2016 - SOLARIN Launch event

CROWDSALE

2018

- FINNEY™ phone concept study
- SIRIN OS™ concept exploration
- Crowdsale preparation & launch

H1'2018

FINNEY™ DEVELOPMENT

- FINNEY™ devices development
- SIRIN OS™ beta release to OEMs
- Release SDK for D-Apps developers
- Establishment of production line

H2'2018

FINNEY™ LAUNCH

- FINNEY™ Launch event

H1'2019

- Launch of open source SIRIN OS™
- Development of distribution channels

9. SUSTAINABLE ECONOMY – OUTLOOK FOR SIRIN OS™

SIRIN LABS is aiming to maximize the adoption of SIRIN OS™ by its users and the blockchain community as a whole. SIRIN LABS will work together with OEM vendors to increase global distribution and demand of SIRIN OS™.

Subject to the permissibility under applicable law, in the future, in order to further grow the economy around SIRIN OS™, SIRIN LABS in its sole discretion will examine the need for a new supporting tokens (Future Token) with the functionality as payment means that may be exchanged against SRN Tokens. Such exchange (if any), however, is subject to the SRN Token holder's willingness to provide sufficient proof of identity, information about the source of funds and other documentation or other information that SIRIN LABS may require in connection with SIRIN LABS's obligations under, and compliance with, applicable laws and regulations, including but not limited to anti-money laundering legislation and regulations.

Subject to the reservations of the previous paragraph, SIRIN LABS plans to implement the Future Tokens as a smart token, which uses the Bancor protocol to maintain liquidity (see section 10.2).

For the sake of clarity, this white paper and the upcoming crowdsale is limited to SRN Tokens. Future Tokens are only mentioned in connection with a potential outlook for SIRIN OS™ and are not part of the crowdsale described this white paper by SIRIN LABS. The reader of this white paper acknowledges and agrees that it has no claim (independent of legal theory or jurisdiction) under this white paper for Future Tokens.

10. APPENDIX

10.1 Risk Disclosure Statement

The following are the risk factors in relation to SIRIN LABS business in general and SRN Token Sale event in particular:

- The SIRIN LABS token may be significantly influenced by digital currency market trends and SRN value may be severely depreciated due to non-SRN related events in the digital currency markets, although SRN are not digital currency.
- SIRIN LABS is developing a complex hardware and software project and its launch may be delayed due to unforeseen development barriers.
- The use of SRN tokens may come under the scrutiny of governmental institutions.
- The ownership of SRN tokens may fall under new and unpredicted taxation laws that will erode SRN benefits.
- The positions and plans outlined in this Whitepaper may be altered as the project progresses.
- SIRIN Token sales and CROWDSALEs have been known to come under malicious attacks from hackers and/or other parties resulting in theft of tokens. Such events may inflict massive losses on buyers and the company.
- Allowing the peer-to-peer secured payment through the SIRIN LABS' devices and ecosystem is subject to applicable regulation, in particular – the applicable financial markets regulation that may require SIRIN LABS to obtain regulatory approvals

10.2 Bancor as a Token Platform

Bancor is an ERC20-compatible token template, which offers continuous liquidity via an on-chain market maker. Bancor raised over $150 million during Q2 2017 in an initial token offering, making it one of the largest fundraising campaigns in the blockchain industry.

More information about Bancor can be found on the Bancor website and in the Bancor Whitepaper.

10.3 References

http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/

10.4 Abbreviations

BT	Bluetooth
CIRT	Cyber-Incident Response Team
EOP	Elevation of Privilege
ETH	Ethereum
IPS	Intrusion Protection System
MitM	Man-in-the-Middle
NFC	Near Field Communication

OS	Operating System
OTA	Over The Air
SDLC	Security Development Life Cycle
SRN	SIRIN LABS token
TEE	Trusted Execution Environment