SIRIN LABS

ブロックチェーン時代のための
安全なオープンソースの消費者向け電子機器

Whitepaper

Prepared by: SIRIN LABS Team

CONTENT

1. 概要

高度なセキュリティ機能を備えたモバイルフォン「SOLARIN」の開発者SIRIN LABSはクラウドセールイベントを開催している。 調達資金は初のオープンソースブロックチェーンモバイルフォン、そしてオールインワンPCであるFINNEY™の開発およびモバイルフォンSOLARINのサポートに使用される。ユーザーはSIRIN LABSトークンであるSRNトークンを使用することにより、全てのSIRIN LABS製品（SOLARINおよびFINNEY™の商品）を購入することができる。

現世代のスマートデバイスはユーザーのセキュリティレベルを犠牲にしている。 最も焦点を当てているのは詐欺やサイバー犯罪対策に巨額なコストがかかっているユーザーエクスペリエンスである。 将来のデジタル経済ではこのような妥協は容認できない。デバイスアーキテクチャは優れたユーザーエクスペリエンスを保持する一方で、真のセキュリティを実現するパラダイムシフト（当然のことと考えられていた価値観などが劇的に変化すること）を求めている。

FINNEY™デバイスは初のサイバー保護型ブロックチェーン対応モバイルフォン&PCであり、 Android™のOSの機能性、そしてユーザーによる安全で信頼性の高いアクセスを可能にするサイバーセキュリティ技術を兼ね備えている。

FINNEY™デバイスはIOTAのTangleテクノロジーとSIRIN LABSのセキュリティエコシステムによりを活用し独立したブロックチェーンネットワークを形成するスケーリング可能で軽量な分散型台帳である。 FINNEY™は集中型バックボーン（ネットワーク）やマイニングセンターと繋がっていないため、迅速かつ手数料がかからない安全な取引の提供が可能である。

FINNEY™のデバイスはSIRIN LABSのオープンソースオペレーティングシステムであるShield OS™上で動作する。 この機能はSRNトークンによりサポートされることによって、コールドストレージウォレット、安全な取引所へのアクセス、コミュニケーションの暗号化、支払いとアプリのエコシステムを共有するP2Pリソースのような固有のブロックチェーンアプリケーションをサポートする。FINNEY™ネットワークのネイティブトークンであるSRNトークンを使用することにより、SIRIN LABSのラインアップ製品およびサービスを取得することができる。

SIRIN LABSは一般電子製品のOEMと提携し、FINNEY™アーキテクチャ、ソフトウェアプラットフォームおよびSRNトークンの適用を促進する。 オープンソースのハードウェアおよびソフトウェアのプラットフォームを公開予定。

2. 会社概要

2.1 SIRIN LABSについて - 過去、現在、そして未来

SIRIN LABS は世界で最も安全な電話機を開発するという使命をもって 2014 年に設立された。徹底した研究開発を経て 2016 年 5 月にリリースされた当社の主力製品である SOLARIN は高い評価を受けた。

最先端のハードウェアとソフトウェアのセキュリティ技術、24 時間 365 日のサイバープロテクションが組み込まれた SOLARIN は、暗号化された通話やメッセージのプライベートゾーンを備えている。

革新的な技術に最高のデザインと妥協のない品質を融合させた SIRIN LABS。「最高のものを生み出したい」という情熱が世界をリードするテクノロジーを創り出す原動力となっている。先駆的なデザインと完璧なサービスにより、SIRIN LABS は独自のハイエンド製品を世界中のユーザーに提供する。

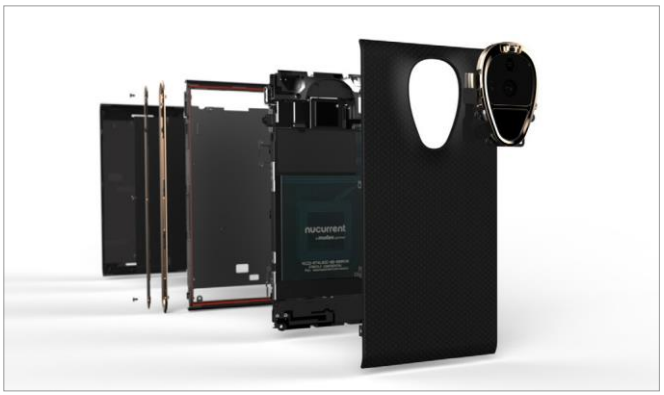
2016 年 5 月に発売された SOLARIN は世界中のメディアに旋風を巻き起こし、今日でも世界レベルにおいて高セキュリティのスマートフォンであるとされている。

SOLARIN はバートン地方のロンドン店で販売されており、ハロッズの高級品テクノロジー売場で最も売れている商品である。

SOLARIN のリリース以降学んだこと：

- 非常に素晴らしいプロフェッショナルなチームと利便性の高いアセット（ハードウェアの開発方法や高セキュリティ OS とサービスの IP/知的財産）を有しているということ
- デジタル経済とブロックチェーン技術の分野において「構造的転換」があること
- 暗号通貨製品およびサービスを信頼するコミュニティが急速に拡大しており、プライバシーとサイバー攻撃に対する保護が切に必要であること

これらの見識は新しいデバイスファミリーである FINNEY™に盛り込まれている。2014 年に亡くなられた Bitcoin のパイオニアであるハル・フィニー（Hal Finney：https://en.wikipedia.org/wiki/Hal_Finney_(computer_scientist)）に敬意を示して FINNEY™と名付けた。



SOLARIN - 高セキュリティハイエンドスマートフォン

2.2 ビジョン

SIRIN LABS のビジョンはマスマーケットとブロックチェーン経済間のギャップを埋め、安全なオープンソース家電製品の世界的リーダーとなることである。

3. 問題領域

SIRIN LABSは次の課題を解決する：

3.1 ブロックチェーンエコシステムのセキュリティの向上

スマートフォンと PC はセキュリティやプライバシーを主要素として設計されたことはないが、これらはブロックチェーンネットワークの信頼性を確保するために不可欠な要素である。 暗号通貨マイニング、取引、そしてオンライン決済などがこれらのデバイス上で利用可能になると、悪意のあるアクターにとっては格好のターゲットとなるだろう。

現代のスマートフォンのもう一つの問題は、非常に多くの機能を持っていることである。競争の激しい市場のおかげで、更に多くの機能を追加するという競争が繰り返されている。これは二つの問題を示しており、一つはセキュリティが遅れを取っていること、もう一つは攻撃の対象となりえる領域が非常に大きいことだ。強い意図を持った攻撃者がデバイスをハッキングしてアクセスし、データを取得するのは比較的簡単なことである。 WhatsApp や WeChat のように広く使われているチャットアプリへのエンドツーエンド（端末相互間）暗号化の導入など、これまでもスマートフォンのセキュリティを強化する試みはいくつか行われてきたが、残念ながらこういった対策では不十分である。アプリの安全性は保証されていても、ユーザーがメッセージ画面コピーを送信、または通話を録音するマルウェア（有害なソフトウェア）を既に騙されてダウンロードしてしまっている場合は役に立たないのである。

このような攻撃を防ぐためには、スマートフォンを外部からの侵入だけでなく端末自体、つまりハードウェアを保護する必要がある。 これはオペレーティングシステム自体を強化することによってのみ行うことができる。つまり、アプリ開発だけでは十分なセキュリティレベルまで達成できないため、スマートフォン端末自体を作り変える必要がある。 こういった考えにより安全性の高い携帯電話の製造業者は端末の開発を余儀なくされるが、携帯電話の開発は製造、そして制限された利便性（セキュリティに重点を置くため）の提供どちらにおいても高いコストがかかり、高度な機能を開発する余裕がないのが現状だ。

SIRIN LABS は利便性の追求を妥協することなく、セキュリティやプライバシーにおける課題に取り組み解決する。

3.2 暗号通貨の使用は容易ではない

マスマーケットによる暗号通貨の適用において立ちはだかる主な障壁はその技術が複雑で使用が簡単ではないことだ。 実際の送金は他の支払い手段と同じくらい簡単だが、紛失や盗難を防ぐためにウォレットを十分に保護することは非常に難しい。コールドストレージウォレットを実装できるハードウェアと組み合わせた本質的に安全なオペレーティング システムを設計することにより、ソフトウェアは自動的に次のような最善の暗号通貨の管理を行うことができる：コールドストレージウォレットへのキー保管、頻繁に使用するウォレットとめったに使用しないウォレットとの分別、ウォレットの残高が大きくなった際にユーザーにリカバリツールを委託するよう案内する等。

3.3 安全で信頼できるP2P共有リソースの収益化

スマートフォン、ラップトップ、タブレット、PCなど、21世紀に定着したモバイル家電製品の普及は様々な好機と危機をもたらした。一方で私たちは皆、データ接続、エネルギー、計算力、環境情報といった様々なタイプのデジタルリソースを所有しており、

これらは個人のデバイスのソフトウェアやハードウェアに埋め込まれている。これらのリソースの中には、シングルユーザー向けでマルチユーザー向けでないものがある。また一方で、無償であれ有償であれ、必要な手段のリソースの共有を可能にする一般的な技術はなく、もしこのような技術が存在したとしても現在の日常的なサイバー攻撃、脅威、そして個人、知人、他人間の限られた信頼関係はリソースの共有を妨げることになるだろう。

サンフランシスコに到着しようとしているある旅行者またはビジネスマンがいたとして、彼のスマートフォンにはバッテリーがほとんどなく、ローミングデータプランが正しく機能していない。すると近くにいた見知らぬ人が彼に 20%のバッテリー電池を与え、ローカルモバイルデータプランへのアクセスの提供を提案してくれた。 このリソース共有・交換は、次の 3 つの特性を持つ：

- **信頼** - この 2 人はリソースと費用について同意するために完全に信頼し合うことができる。
- **セキュリティ** - リソース共有は非常に高セキュリティのサイバープロテクションデバイス間で行われる。これはデバイスの間を標的にするサイバー攻撃を防ぎ、当事者やリソースのセキュリティレベルを下げることなくモバイルデータの変更作業を行うことができる。
- **収益化のサポート** - リソース所有者はブロックチェーンのインフラストラクチャなしに、二者間の信頼に基づきリソースの提供に対し少額決済手数料を受け取る。

SIRIN LABS のエコシステムおよび製品は、一つのデバイスから他のデバイスに大規模で信頼性が高くサイバー保護された P2P のリソース共有を実施させることができる。 このエコシステムはブロックチェーン開発者のコミュニティに少額決済ごとに、信頼性と安全性の高いリソース共有アプリケーションおよびサービスの多様なドメイン作成機会をもたらすものである。

例：

- **リソース** - データ接続、エネルギー、計算能力
- **データ** - 現地の天気情報、交通状況
- 制限なし

3.4 フェアな分散型アプリストアの必要性

ほとんどのユーザーは自分のデバイスの OS ベンダーにより管理されるアプリストアを介して使用するアプリを検索するが、これらのほとんどのアプリストアは特にマルウェアからユーザーを守るためのアプリの監査や評価を十分に行っていない。それにも関わらず、ユーザーは高い使用料を払っている。そしてアプリストアは開発者のポケットマネーやほとんどのアプリ内の課金を含む開発者の収益のうち約 30%を要求している。Apple と Google が運営しているアプリストアの合計収益は近年で年間約 500～1000 億ドルだという。

しかし、ユーザーへのダメージはますます多くなっている。認可されていないコンテンツ（例：ギャンブルやアダルトコンテンツアプリ等）を含むアプリの禁止から、運営者の事業にリスクをもたらすアプリへの大幅な制限（例：Apple社が2014年に行った全てのブロックチェーンウォレットアプリ提供の停止等）まで、アプリストアの運営者は独占的なパワーを行使し提供アプリへの検閲を強要している。

SIRIN LABSのD-Appストアはありとあらゆるタイプのアプリを取り扱う分散型ストアで、ユーザーは使用するアプリの開発者に購入料金の100%を直接支払う。 セキュリティ保護、ペアレンタルコントロールなどを提供する監査サービスは信頼できる第三者により提供され、購入者に直接販売される。

4. プロダクト

SIRIN LABSのユニークな提案

分散型ネットワークにはネットワークのスケーラビリティ、支払いの処理スピード、セキュリティ、そしてプライバシーをはじめとする膨大な課題がある。開発における SIRIN LABSの技術とSOLARINスマートフォンの公開に基づき、今後の新たな課題に対処するため、FINNEY™スマートフォンとPC接続デバイスをベースにした新しい分散型ネットワーク経済の構築を計画している。

4.1 最先端技術を使用したブロックチェーンスマートデバイス

SIRIN LABSは第2世代製品であるFINNEY™スマートフォン、そしてオールインワンPCであるFINNEY™を開発している。これらのデバイスは高セキュリティ暗号化コアを搭載したAndroid™ベースのオペレーティングシステムであるSIRIN LABSのオープンソースShield OS™を使用して動作する。SIRIN LABSのレガシー製品である SOLARINはSRNトークンを使用して購入することもできる（最大小売価格から10%割引）。

4.1.1 SOLARIN ™ スマートフォン

高セキュリティAndroidスマートフォン、SOLARIN - SIRIN LABSのSecurity Shield により完璧なセキュリティを実現した一台。

ハイレベル仕様：

特徴：

- SIRIN LABS Cyber Protection:
- ビヘイビアベース侵入防御システム (IPS)
- セキュリティスイッチ（コール&メッセージの保護）
- 高セキュリティ通信 (IP電話、テキスト、メール)
- 二段階認証：生体認証 （指、ロックパターン）

ハードウェア仕様：

- ディスプレイ 5.5” QHD内部メモリストレージ
- 128GB
- 8GB RAM
- Wi-Fi 802.11ac / WiGig（高速無線通信）
- BT 4.0
- 24MP メインカメラ
- 8MP 広角セルフィーカメラ

4.1.2 高セキュリティコール＆メッセージアプリケーションとサービス

高セキュリティAndroidスマートフォンであるSOLARINはSIRIN LABSのSecurity Shield により完璧なセキュリティ機能を搭載した。

SOLARIN特有のハードウェアや通信相手の認証から、256ビットAESエンドツーエンド暗号化（FIPS 140-2認定）といった、全ての通信をエンドツーエンド（端末相互間）で保護する複数のセキュリティレイヤーを適用した通信アプリケーションである。
SRNトークンの使用により高セキュリティコール&メッセージバンドルの拡張を行うことができ、アプリケーションは一般的なAndroidおよびiOSデバイスと互換性がある。

4.1.3 FINNEY™スマートフォン

SIRIN LABS製品ラインには、ブロックチェーンコミュニティを対象にした最初のスマートフォンを含む。 FINNEY™スマートフォンは比較的安価（～999USドル）で完璧に設計された高セキュリティスマートフォンであり、トランザクションの整合性を保証する高度なブロックチェーンと暗号通貨取引アルゴリズムが組み込まれている。

ハイレベル仕様：

希望販売価格：999USドル～

ブロックチェーンの特徴:

Shield OS™:

- 安全なP2Pリソース共有
- 内蔵ハードウェア「コールドストレージ」クリプトウォレット
- 分散型台帳コンセンサス SIRIN LABS Cyber Protection suite
- ビヘイビアベース侵入防御システム（IPS）
- ブロックチェーンベース改ざん完全防止
- セキュリティスイッチ（ウォレット保護）
- 高セキュリティ通信(VoIP、テキスト、メール)
- 三段階認証：生体認証（光彩＆指紋）、ロックパターン、行動認証

ハードウェア仕様：

- 5.2”QHDディスプレイ
- 256GB内部メモリストレージ
- 8GB RAM
- Wi-Fi 802.11ac
- BT 5.0
- 16MPメインカメラ
- 12MP広角セルフィーカメラ

4.1.4 FINNEY™ PC

SIRIN LABSの製品ラインは比較的安価（～799USドル）ので完璧に設計された高セキュリティオールインワンPC、FINNEY™PCを含む。これは(GPU / CPU / RAM）のように更なる計算力を備えた「シンクライアント*」上に構築され、SIRIN LABS P2Pリソース共有プロトコールまたはクラウドベースのサービスに基づいて追加することができる。

*ユーザーが使うクライアント端末に必要最小限の処理をさせ、ほとんどの処理をサーバ側に集中させたシステムアーキテクチャ全般のこと。

ハイレベル仕様：

希望販売価格：～799USドル

ブロックチェーンの特徴：

Shield OS™:

- 安全なP2Pリソース共有
- 内蔵ハードウェア「コールドストレージ」クリプトウォレット
- 分散型台帳コンセンサス

SIRIN LABSサイバープロテクション：

- ビヘイビアベース侵入防御システム（IPS）
- ブロックチェーンベースで改ざん完全防止
- セキュリティスイッチ（ウォレット保護）
- 安全な通信（VoIP、テキスト、メール）
- 3段階認証：生体認証（光彩＆指紋）、ロックパターン、行動認証

ハードウェア仕様：

- 24 "2Kディスプレイ
- バイオメトリックセキュリティ
- 8GBメモリ
- 256GBストレージ
- Wi-Fi 802.11ac

注記：仕様はローカル「シンクライアント」用。SIRIN LABSクラウドベースのサービスに基づいて更に計算能力を追加することができる。

4.2 Shield OS™

FINNEY™スマートフォンとFINNEY™PCデバイスは、高セキュリティ暗号コアを備えたAndroid™ベースのオペレーティングシステムであるSIRIN LABSのオープンソースShield OS™を使用する。Shield OS™の中心には分散型、スケーラブル、そして軽量でASIC耐性のあるレジャー（台帳）を備えている。Shield OS™は世界中の何百万ものスマートデバイス上で作動するよう設計されており、SIRIN LABSのSRNトークンエコノミーの原動力となるだろう。また、Shield OS™はユーザーフレンドリーで手間のかからないインターフェイスを備えた、高セキュリティP2P暗号通貨トランザクションメカニズムを実装している。これらは手数料がかからず迅速な支払い、リソース共有、およびサービス提供といったSRNトークンエコノミーを可能にする要因となる。分散型台帳トランザクションの整合性を保証するため、Shield OS™はマルチレイヤーから成る厳重なサイバープロテクションを提供する。これはウォレット、インターネット接続、およびブロックチェーンネットワークの間のインターフェイスで行われる暗号通貨取引において安全性の低いリンクを保護する革新的な方法となる。

Shield OS™は次に記述する機能を備えている。

4.2.1 BlockShield™

BlockShield™はトランザクションの整合性を保証するSIRIN LABSが誇る技術である。BlockShield™はSIRIN LABS、Trusted Display、IP Address Hiding、およびMAC Address Randomizationによって製造されたデバイスに組み込またマルチプロテクションレイヤーから成る。

4.2.2 内蔵ハードウェア「コールドストレージ」クリプトウォレット

ウォレットの主な目的は、ユーザーのプライベートキーを保護することである。ウォレットにはユーザーの残高、取引履歴、そしてパブリックアドレスが表示される。ウォレットはSIRIN LABSのBlockShield™技術により保護された改ざん防止要素であるTrustCore™にハードウェアベースで埋め込まれており、端末のスイッチにより非常に安全な場所で保護される。埋め込まれたウォレットが使用されていない場合、物理的におよび電子的にネットワークから遮断される。

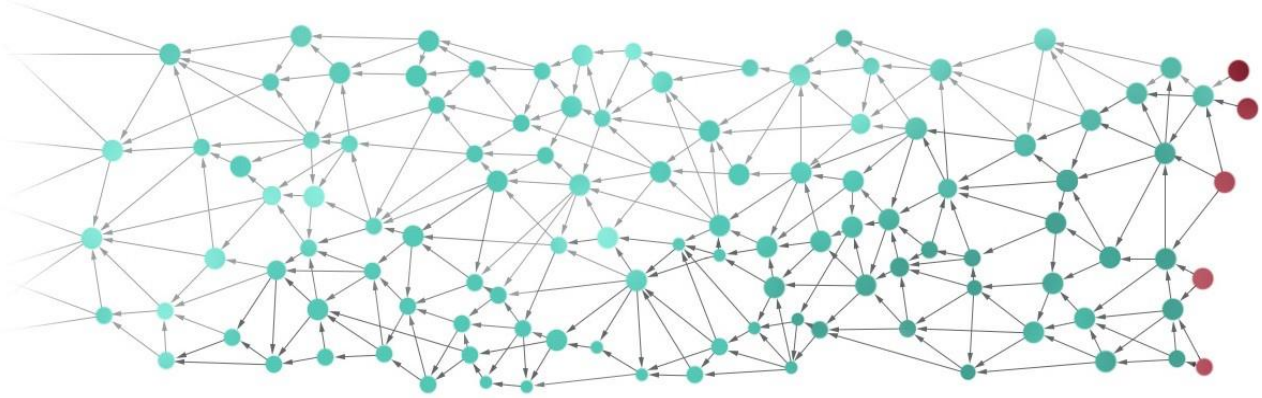
このウォレットは複数のアカウントを保有することができ、Bitcoin、Ether、Litecoin、Dash、Zcash、Ripple、Stratisおよび Dogecoinやその他の主要な暗号化通貨に加え、SIRIN LABSのトークンに対応している。

4.2.3 サイバープロテクション

低レベルのOSからアプリケーションレイヤーまで、デバイス全体が何重ものサイバープロテクション機能で保護されている。サイバー攻撃の脅威は常に変化することを認識し、SIRIN LABSは行動ベースやマシンラーニング（機械学習）を駆使してマルチレイヤー侵入防御システム（IPS）の開発を行っている。

4.2.4 分散型台帳コンセンサス（DLC）のモジュール

DLCモジュールにより手数料がかからないコンセンサスメカニズムでトランザクションを承認することができ、これによりマイニングを必要とせずにネットワークピア間での迅速な支払いが可能になる。コンセンサスはTangleネットワークコンセンサスアルゴリズムに基づく。



4.2.5 分散型アプリストア（D-AAP）

アプリのエコシステムの成功の鍵は多様性、連携性、開放性だと考える。このエコシステムを刺激するために、SIRIN LABSはアプリのための手数料がかからず検閲不要のマーケットプレイスであるD-APPストアを導入する。D-APPストアはアプリとサービスのデジタル配信チャンネルであり、開発者に配信、購入管理および課金におけるソリューションを提供し、ユーザーにはアプリの詳細情報、アップデート、そして監査サービスを提供する。

従来の中央集権型アプリケーションストアとは違い、Shield OS™アプリストアは分散型コミュニティによって管理され、ユーザーはアプリのレビュー、評価、およびまたはフィルター処理を行うために自身が選んだ信頼できる監査のサービスを使うことができる。

有料アプリおよび課金への支払いはアプリとサービス間、また開発者とエンドユーザー間で料金を分配する安全なP2Pリソース共有に基づく。従来のアプリストアと同様、ユーザーはあらかじめ定義されたカテゴリに基づきアプリやサービスを検索することができる。

4.2.6 P2Pリソース共有マーケットモジュール

Shield OS™は、開発者にOSのブロックチェーン機能および機能性へのアクセスを可能にするソフトウェア開発キット（SDK）を提供する代わりに、ピアまたはユーザーグループ間でのデジタルリソースおよびサービス共有の提供を行う。これらのサービスはデバイスのカメラ、データ、ストレージ、セキュリティ、ロケーションなどに基づいて実行することができる。

4.2.7 分散型アプリケーション開発のためのSDK

世界中の開発者にシームレスで安全なP2Pのリソース共有と支払いシステムを使用し、SIRIN LABSのネットワーク能力と機能に基づいた、ブロックチェーン世代向け分散型アプリケーションをより迅速で安全に開発できるソフトウェア開発キット（SDK）を提供する。

SIRIN LABS のSDKはゴシッププロトコル、分散型データベース、投票/ポーリングメカニズム、オラクルAPIといった全ての分散型構成要素を実装し利用可能にする。

SIRIN LABSのSDKを使用することで、開発者はSRNトークンを使用してソフトウェア、サービスおよび有形資産に対する支払いを受けとることができる。 さらに、ユーザーはSRNトークンを使用したP2P「アプリ内」マイクロペイメントを行うことができる（例：あなたの国を訪れている観光客にあなたのセルラーデータ接続を共有することにより報酬を受け取る等）。

5. SIRIN LABSの高セキュリティブロックチェーン技術

5.1 概要＆必要条件

FINNEY™デバイスの基盤となるShield OS™は、主流デバイス上のブロックチェーンアプリケーションを安全に使用できるように設計されたAndroid™に基づく分散型オープンソースオペレーティングシステムである。Shield OS™は、改良されたブロックチェーン機能および分散型リソース共有、そしてShield OS™全体で使用される量子コンピューティング攻撃防止機能を備えた軽量で手数料がかからないSRNトークントランザクションを提供する。

5.1.1 セキュリティの必要条件

ブロックチェーン技術をマスマーケットに導入するためには、暗号ツールはシンプルで誰でも使えるものでなければならない。 第1世代のオンライン決済システムの経験から、（ネットワークまたはストレージ上で）機密情報が処理される瞬間、そしてそれが（ディスプレイ上などで）エンドユーザーに表示される瞬間まで、最終的に悪用され利用される可能性があるという脆弱性を学んだ。今日のブロックチェーンユーザーにとって、ペアのキーの維持、プライベートキーの保護、リカバリー手順の計画およびトランザクションデータの検証といった複雑な手順は今日のブロックチェーンユーザーが日常的に行うことだが、全てのユーザーがこの一連の手順を行っているわけではない。

Shield OS™で使用されるセキュリティ対策ではユーザーを認証し、キーを使ってトランザクションまたはメソッド呼び出しに署名するOSの中に含まれる限定された一連の「セキュアモード」の手順を踏むことによってのみアクセスを許可し、プライベートキーを決して公開しない。マルウェア（有害ソフト）の使用やアプリのバグの悪用、そしてユーザーが騙され自分の秘密を他人に教えたりすることにより秘密が盗まれるが、それを絶対に起こさないための唯一の方法は、秘密を手の届かない場所に保管することである。

さらに、フィッシング詐欺を防ぐために、シンプルで誰でも実際の支払いインターフェイスからフェイクを識別できる方法を採用する必要がある。これにはデバイスがセキュアモードの時に作動するデバイスシェル上の物理的インジケーターが必要である。特有のLED、物理的スイッチ、またはセキュアモードである別スクリーンがインジケーターの役目を果たすことができる。デバイスのユーザーは支払いやその他のアクションを安全に行うためにインジケーターを設定する必要があるということだけを知っていればよい。

上記の要件は盗難、フィッシング、キーロギングによって損害を受けないために必須だが、FINNEY™が提供する高度機能はアタッカー（攻撃者）に新しい機会を与えるという点に留意する必要がある。具体的には、リソースの共有（特にCPUとネットワークリソースの共有）は盗聴やアクセス制限侵害の危険性が生じると考える。このリスクを軽減するため、FINNEY™はSIRIN LABSのサービスであるサイバーセキュリティ機能を搭載している。

5.1.2 ブロックチェーンの必要条件

Shield OS™により提供されるブロックチェーンサービスは他のブロックチェーン技術においても使用できるが、支払いやリソース共有といった一般的な使用においては、現在の標準ブロックチェーンのどれもが主流ユーザーには適していないことがわかる。

支払いとリソースの共有に使用されるネイティブブロックチェーンは、トランザクション承認を迅速に行い、マイクロペイメントを可能にするためにトランザクションにかかるコストを極限まで抑え、またネットワーク接続が制限されたエントリーレベルのCPUを持つデバイスでノードを操作できるライトクライアントが必要となる。集中型のマイニングプールよりも、ユーザーデバイスがネットワークの承認の大部分を担い長期間の均衡を保つPoWがネットワークの長期的な独立性を確保するために必要である。

5.1.3 ハードウェア 適合条件

Shield OS™が必要とするプライベートキープロテクション方式とフィッシング詐欺対策 を適用するためには、アプリケーションアクセスからのプライベートキーの保護およびフィッシングからのユーザー保護というセキュリティにおける2つの条件がハードウェア要素によりサポートされなければならない。

当然のことながら、特別なハードウェア要求がメーカーやデザイナーに負担をかける可能性があるが、これはShield OS™の普及の障壁はならない。これに反して、SIRIN LABSはこれらの要件を満たし、OEMが制約に最も適合した設計を選択できるようハードウェア設計において選択肢を提供する （また、第三者により提案された場合、他のデザインの認証を行う）。

5.1.4 リソース共有の必要条件

おそらく、ブロックチェーンデバイスの最も有用な機能は、リソースを他のデバイスと動的に交換できることである。つまり、ユーザーが必要なときにより良いエクスペリエンスを提供し、使用していない時はリソースを使いやすくすることができる。

マスマーケットのユーザーに提供するリソース共有はシームレス、安全、そして効率的である必要がある。Shield OS™は、OSインターフェイスと共有可能なリソース間にバーチャル化レイヤーを導入し、共有者とリソース共有を受けるユーザーによるバーチャール化した各リソースへのアクセスを可能にする。これにより、共有リソース（ネットワークやCPU等）のパートナー達は互いのセキュリティやプライバシーを損なうことがない。また、バーチャル化されたコンテナは共有リソースの正確な測定を行い、共有者は共有リソースの使用量を計算後換算し、公正な支払いが行われる。共有を受けるユーザーは共有者が実際より多く課金していないか計算し立証を行う（もし多く課金されているとする場合、共有リソースの利用を中止する可能性がある）。共有を受けるユーザーの損失が1セント以上を超えないようにサービスは細分化されている。

共有リソースプロトコルのデザインは直接接続されたデバイスとリソースを共有するLocalBoost™、そしてネットワークを介してリソースを共有するCloudBoost™の2つである。SIRIN LABSは両方のプロトコルに共有のRFC*を実施する予定である。オープンプロトコルであるため、Shield OS™デバイスだけでなく、あらゆるデバイスによるリソースの提供や使用を可能にする。これにより、WiFiルータ、クラウド、エッジクラウドコンピューティングサービス、充電スポットそしてその他様々なデバイスをリソース共有ネットワークの一部にすることができる。

*RFC: Request for Comments、技術仕様の保存および公開形式。

5.1.5 開発

Shield OS™はSDLC（Security Development Lifecycle/セキュリティ開発ライフサイクル）および専門の第三者によるセキュアコーディングや侵入テスト、そして時折行われるハッカー発見プログラムを含むOWASP SCPに基づき開発されている

5.2 ハードウェア設計＆抽象化ワークフロー

ユーザーがブロックチェーンのアプリを安全に使用するためには安全に実行できるハードウェアが必要である。プライベートキーの使用を他の機能から隔離し、セキュアコードが独自の安全なストレージにアクセスできるようにし、安全でないコードによる盗聴や改ざんからディスプレイやユーザーインプットデバイスにおける通信を保護する。もう一つの必要なハードウェアの特性は視覚表示であり、ディバイスがセキュアモード時にユーザーに対し明瞭かつシンプルに表示する必要がある。

SIRIN LABSは、これらの安全な実行条件を満たすため、少なくとも2つのハードウェアの設計を提案する。一つは高セキュリティ領域をサポートするメインチップセットアーキテクチャを必要とするもの（例：TEE/Trusted Execution Environment サポーティングチップ等）そしてもう一つはSecure Element（SE）チップに接続時にサポートされるチップセットである。前者はOEMハードウェア製造者が自身の既存ボードデザインほとんど、または全く変更せずにShield OS™を適用することができる。これに対し、後者は新しいボードデザインを必要とする可能性はあるが、SEチップのコストが低いため、全体BOMへの影響は非常に少ない。

視覚表示に対する要件を満たすには、セキュアモードとウルトラセキュアモード間の移行をユーザーが自身で動かす必要がある物理的スイッチが必要であると考える。代わりに、セキュアモード時のみ点灯する専用インジケーターLEDを使用することもできる。このインジケーターはデバイス上の他のインジケーターと容易に区別できるようにする必要があり、これはユーザーがセキュアモード時にのみトランザクションを認証する必要があることを気づかせやすくためである。

例：抽象的なワークフロー

デザインオプションはウォレットのストレージとコンピュテーション（計算）を隔離するために様々なアプローチを用いるものの、入出力について安全な方法で表示するためにウォレットに対し同一の抽象ワークフローを使用する。例えば通貨の送信は次のように行われる：

1. ユーザーがサポートされているアプリケーション（例：P2Pメッセージアプリケーション）で通貨を送信することを選択する
2. アプリケーションがトランザクションの詳細を含むドキュメントを作成する（ロウトランザクション）。プリケーションは任意で宛先アドレスの所有者である受信者の実際の名前とアドレスを示すSSL証明書を取得することができる。
3. アプリはShield OS™が提供する「ウォレットインターフェイスサービス」のSignTransaction方式を呼び出す。これはウォレットのハードウェア（高セキュリティ領域またはSEチップのいずれか）に、ロウトランザクションを送信する。
4. セキュアモードの表示がオンになる。
5. （セキュアディスプレイ上の）ハードウェアウォレットがトランザクションの詳細を表示：送金額および宛先アドレスが表示され、トランザクションに所有者のサーティフィケートが添付されている場合、受信者の名前と住所も表示される。その後、トランザクションの承認のためにユーザー認証が要求され表示される。
6. ユーザーがトランザクションを認証して承認した場合、セキュアコードが高セキュリティのストレージに保管されているプライベートキーを使用してトランザクションに署名し、アプリに送り返す。その後セキュアモードを終了する。
7. セキュアモードの表示がオフになる。
8. メッセージアプリが署名されたトランザクションを受信し、トランザクションをコミットするためにブロックチェーンに送信する署名付きトランザクションを受信する。

5.3 アーキテクチャ

適応レイヤー＆HAL（ハードウェア抽象化レイヤー）

適応レイヤーおよびHAL（Hardware Abstraction Layer/ハードウェア抽象化レイヤー）は、リソースアクセスを安全な方法で抽象化するために、OEMが既存のソフトウェア/ハードウェアプラットフォーム上にShield OS™を統合するための標準インターフェイスとして定義される。

リソース共有プロトコルのように、LocalBoost™やCloudBoost™は特定のデバイスに限定されない。ハードウェアをサポートするためにShield OS™に組み込まれた抽象化レイヤーは、あらゆるタイプのデバイスや既存のオペレーティングシステム上に移行することができる。

5.4 システムサービス＆コアライブラリ

システムサービスは、Shield OS™によってアプリケーションフレームワークおよびそのAPIに公開されるモジュラーコンポーネントである。

システムサービスは協力し合い、Shield OS™のコアライブラリの利点を利用して既存のハードウェアデバイスにShield OS™のコア機能を提供する。次のシステムサービスレイヤーのコア構成要素を含む。

5.4.1 DLC（Decentralized Ledger Component/分散型台帳コンポーネント）

ネイティブブロックチェーンの要件（迅速で手数料がかからないライトクライアントに対するスケーラブルなトランザクションの実行）を十分に満たすため、SIRIN LABS は IOTA Foundation と共同で Shield OS™への Tangle ベースの LED 技術の統合を目指している（IOTA Tangle については[1]を参照）。

DLC（分散型台帳コンポーネント）は、IOTA の実装要件を満たすために設計された構成要素である：

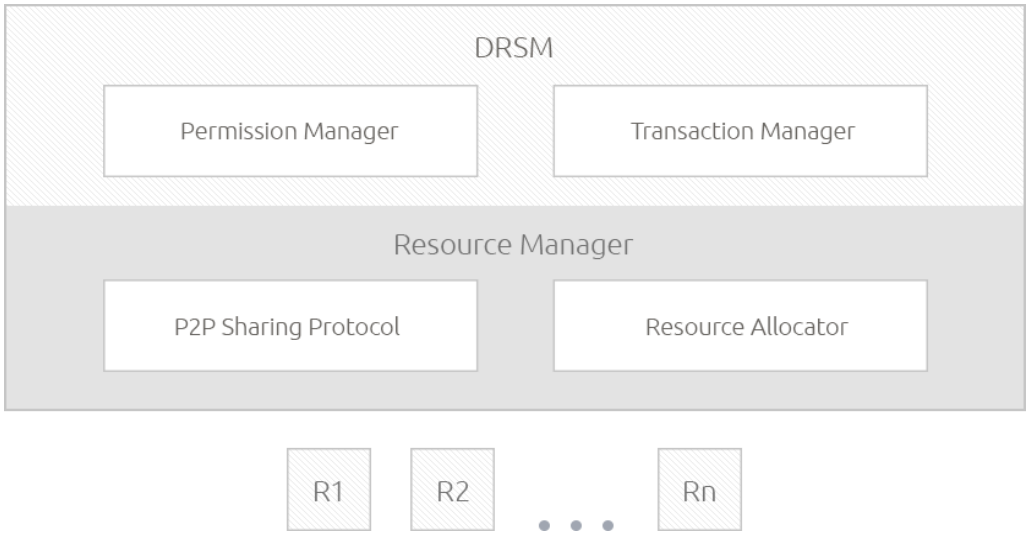
- Tangleネットワーク上のデバイス間の安全なP2Pトランザクションの管理
- Tangle's Tip Selectionのアルゴリズムの実行 （IOTAのホワイトペーパーに記載されている通り）
- ハッシュ計算の実行および選択された前のトランザクションの検証

5.4.2 ウォレットインターフェイスサービス

Shield OS™デバイスでは、プライベートキーへのアクセスはハードウェアウォレットモジュールのみ行うことができる。ウォレットインターフェイスサービスは、アプリケーションにウォレットへのAPIアクセスを提供し、通貨送金とスマートコントラクトコールに署名を付けることが可能。 ハードウェアウォレットは（独自のストレージを使用した隔離されたチップ上、またはプライベートキーを保有する安全なストレージへの排他的アクセス権を持つ領域内において）ユーザーの認証と承認を求め、承認された場合は署名されたトランザクションを返す。

5.4.3 DRSM（Decentralized Resource Sharing Manager/ 分散型リソース共有マネージャー）

DSRM（分散型リソース共有マネージャー）は分散型ネットワーク上で安全で信頼できるプライベートな方法において、リソースの割り当て、許可、そして共有を行う役割を担う。DRSMによって運用されるバックグラウンドサービスは、動的に計算されたコストプロトコルに従って、リソース共有者へのSRNトークン決済を管理する。



DSRMによって次のリソースが管理される：

- デバイスセンサーデータ
- ネットワークコネクション
- CPU タイム
- GPU タイム
- デバイスストレージ　など。

5.5 BlockShield™

Shield OS™は本質的に安全な構造であるため、安全なブロックチェーン操作を提供するだけでなく、セキュリティおよびプライバシーに関連するサービスのツールキットを提供することができる。このツールキットの一部は、ブロックチェーン以外の用途にセキュリティ機能を提供するように設計されている。これはオプションであり、OEMは自社製品への適用を選択できる。

5.5.1 アプリケーションレイヤー

Secure Shield ™（アプリケーションコンテナ）

Secure Shield ™は選択したアプリケーション（ウォレットアプリ、暗号化されたVoIP /メッセージ、暗号化されたEメール等）を保護するために、OSレベルでのサンドボックス型セキュリティを提供する。Secure Shield ™は、次のようなデバイスおよびシステムリソースへのアクセスからアプリケーションにパーミッションベースの隔離を提供する：

- **センサー**：カメラ、マイク、バイブレーター、スピーカー、モーション、GPS
- **コミュニケーション**：Bluetooth、NFC、通話および SMS
- **周辺機器**：USB、HDMI、シリアル/パラレルポート
- **システムプロセス**：オーディオ録音、またはビデオ録画、アプリのインストール、スクリーンショット、工場出荷時設定へのリセットおよびデバッグ

物理的なセキュリティスイッチおよび認証マネージャーによって管理される二段階認証により、Secure Shield ™によって保護されているアプリケーションへのアクセス保護をさらに強化することができる。

SCS*（Secured Communication Suite/高セキュリティコミュニケーション）
*OEM向けオプション

SCS（高セキュリティコミュニケーション）は、悪意のある人物による盗聴から機密会話を保護するために、接続されたデバイスで安全な通信を提供するエンドポイントからエンドポイントまでの包括的な一連の暗号化ソリューションである。

SCSは暗号化された音声通話、安全なテキストメッセージ、ファイル転送、Eメールで構成されている。SCSは、SIRIN LABS Trust Core™に搭載されたハードウェアで保護されたキーストアに格納されたPKI暗号システムを使用する。堅牢な暗号化フレームワークは、2048ビットRSAおよびAES 256ビットのシンメトリックセッションキーを持つ暗号システムを利用している。

開発者や提供者がShield OS™を採用し、コミュニケーションおよびリソース共有開発のセキュリティとプライバシーが強化され、Shield OS™の利点が一般に浸透することを期待し、SCSアプリケーションも同様にShield OS™APIを使用してセキュリティとプライバシーを強化する。

SCSはShield OS™を以下の目的で使用する：

1. サービス認証
2. ピア間の交渉（例：暗号化された通話の確立等）
3. 決済および小額決済（例：ユーザーへのアプリサービス料金の請求およびユーザー間における決済の送金等）
4. セキュリティソースの共有（例：ユーザーによるデバイスのハードウェア暗号化エンジンのリース等）
5. 脅威が検出された際の他者への警告

5.5.2 OSレイヤー

ポリシーマネージャー

ポリシーマネージャーは、OSカーネルに埋め込まれたセンサーとデバイスファームウェアから収集されたデータを集約する。サイバー攻撃を抑制し、次のような阻止を行うためのアクションや対策を実行することができる：

- ソフトウェアインストールの一時停止/ブロック
- 接続のブロック
- 疑わしいプロセスの終了等

SIRIN LABS PROTECTOR™バックエンドシステムは、世界のサイバー脅威の日々の変化に応じ、サイバー脅威の動的ポリシーを管理する。これらのポリシーは、必要に応じてOTA*でデバイスにプッシュされる。

*OTA: Over the Air、無線ネットワークを利用（経由）した通信。

IPS*（Intrusion Prevention System/ビヘイビアベースの侵入防止システム）

*OEM向けオプション

SIRIN LABSはサイバー脅威の動的な性質を認識し、既知および未知の脅威（ゼロデイ攻撃を含む）から保護するマルチレイヤー、ビヘイビアベース、そして学習機能を持つIPSを開発している。これは私たちの世界で最も安全なスマートフォン、SOLARINの開発における豊富な経験を基盤としている。
（「世界で最も安全なスマートフォンに会いましょう！」– https://bballmaster.com/meet-safest-smartphones- world/）

Block Shield™はネットワーク攻撃、ホストベース（マルウェア）攻撃、およびフィジカル攻撃に対し、継続的なビヘイビアベースのサイバープロテクションエンジンをデバイス上に搭載している。常時稼働（オフライン時およびフライトモード時を含む）しているIPSエンジンは、デバイス全体の悪意のある動作を監視し、既知および未知の脅威と攻撃（ゼロデイを含む）の両方をリアルタイムで動的に検出する。IPSエンジンは次のような様々なエントリーポイントからの幅広いサイバー脅威や攻撃に対し、識別、防御しデバイスを保護する：

- Wi-Fiネットワーク攻撃 - ARP MITM（中間者攻撃）、トラフィック改ざん、SSLストリップ、ICMPリダイレクトMITM、偽SSL証明書攻撃、不正Wi-Fiアクセスポイントからの攻撃
- 不審なベースバンド動作 - サイレント SMS、3G/4G 暗号化の予期しないダウングレード等
- ホストベース攻撃（シグネチャーベースでは無くビヘイビアベース） - 疑わしい APK（Google Play ストア、他のアプリストア、ウェブサイト、E メール、FTP 等）、EOP（権限昇格）、システムの改ざん、端末のジェイルブレイクまたは root 化
- フィジカル攻撃 - ROM 改ざん、プリロードされたアプリケーションの真正性の改ざん、ハードウェアの改ざん

IPS エンジンは、積極的な監視と分析を使用してデバイスのサイバーセキュリティレベルを向上させる Cyber-Incident Response Team（CIRT）によりバックアップされている。CIRT はユーザーのデバイス使用に関連するセキュリティ管理をサポートするためにオンラインのサイバー脅威を調査し軽減する。

認証マネージャー

SIRIN LABSはPIN、パターン、またはパスワードなどの従来の認証方法の固有の弱点を認識し、生体認証と統合した様々な認証方法を提供している。
Block Shield™は各ゾーン（「通常」ゾーンおよびシールドゾーン）に1セットずつの計2セットの認証方法をサポートしている。顧客はプライバシーとセキュリティを保護するために使用する認証方法を各セット別に選択することができる。

オプションの認証方法は次の事項を含む：

- 個人設定 - パスワード、PIN、パターン、スワイプ、または設定無し
- 生体認証 - 指紋、虹彩認識および/または網膜スキャン（対応デバイスのみ）

デバイスにより、エンドユーザーは選択したセクションの認証保護レベルを設定できる:

1. 無し
2. 個人設定のみ
3. 個人設定+生体認証
4. 個人設定+二段階生体認証
5. 生体認証
6. 二段階生体認証

個人設定および生体情報は、スマートフォンおよびオールインワンコンピュータ内のハードウェアで保護された構成部分に格納され、機密データのセキュリティレベルを向上させる。

デバイス保全（OEM向けオプション）

サイバーセキュリティ分野における脅威の一つは、製品のハードウェアおよびソフトウェアの改ざんである。主な対策は、ハードウェアおよびソフトウェアコンポーネントの真正性を改ざん不可にすることである。

SIRIN LABSは、電子デバイスのハードウェアとソフトウェアの両方のコンポーネントに対して、独自の高度なブロックチェーンベースの改ざん防止メカニズムを開発している。デバイスインテグリティサブシステムは、デバイス間のファームウェアとハードウェアの真正性を検証するためのメカニズムを検証する。

ハードウェア改ざん防止（OEM向けオプション）

デバイスインテグリティモジュールは、ブロックチェーンによって制御されるサプライチェーンマネジメントを使用し、工場内の安全なデバイスの組み立ての統合をサポートする。
選択されたハードウェアコンポーネントの真正性の検証は、ODM*による組立ラインから出荷まで、ライフサイクル全体を通じて実行される。選択されたコンポーネントのハッシュは、分散型台帳に保管され、SIRIN LABSのブロックチェーンネットワークの関連デバイスに対して検証される。

デバイスの選択されたハードウェアコンポーネントを改ざんまたは置換を試みる場合、デバイスインテグリティモジュールによって検出され、UI（ユーザーインターフェイス）に表示されることでユーザーに通知するIPSを起動させ、分析された事象の重大度に従って適切な対策が行われる。

*ODM：Original Design Manufacturing、製品の開発から設計、製造までを行い委託者が製品を販売するという生産方式。

ファームウェア改ざん防止（OEM向けオプション）

同様に、デバイスに影響を受けやすいコンポーネント（ブートローダー、カーネル、システムサービス等）および他の重要な選択されたソフトウェアコンポーネントの不正なソフトウェアの更新や置換を試みる場合、IPSにより検出され適切な機能対策を講じる。

セキュアブート（OEM向けオプション）

Block Shield™に組み込まれているセキュアブートメカニズムは、ハードウェアの信頼の起点（root of trust）からシステムパーティションまでのデバイスソフトウェアの整合性を保証する。ブート中、各ステージは、実行する前に次のステージの保全と真正性を検証する。ブート中に整合性違反が検出された場合、IPSに報告されローカルデバイス上で警告が表示された後、起動シーケンスが保留される。

暗号ストレージ（OEM向けオプション、ハードウェアウォレットは除く）

暗号ストレージサブシステムは、ソフトウェアまたはハードウェアのいずれかによってバックアップされた完全に暗号化されたストレージの統合をサポートする。

トラステッドディスプレイ

トラステッドディスプレイは、Trusted Execution Environment（ARMのTrust Zone、QualcommのQSEE等）を利用し、エンドユーザーが入力した情報を安全に管理する。また、入力デバイス（タッチスクリーン、指紋センサー、キーボード、マウス等）からUIやデバイスのディスプレイまでの入出力チェーンを保護し、検証する。表示される情報はユーザーがトランザクションを行う度にTEEから導出される。これにより、セキュリティ保護されていないアプリケーション、潜在的マルウェア、悪意のある者がトランザクションの詳細を改ざんまたは盗聴することを防ぐ。

プライバシーマネージャー（OEM向けオプション）

プライバシーマネージャーサブシステムはユーザーのプライバシーを保護するため、トグルにより設定可能な匿名化を提供する。

MACアドレスランダム化（OEM向けオプション）

ブロックチェーン上でトランザクションが開始されると、ユーザーは必要なデータを他のユーザーに送信し、効果的にネットワークへの転送ブロードキャストする。ほとんどのブロックチェーンプロトコルはトラフィックを暗号化しないため、悪意のある者がトランザクションを覗き込んで、少しの労力でウォレットの残高を覗くことができてしまう。洗練された第三者にとって、実行されるトランザクションに関するデータを収集し、大規模な暗号通貨ユーザーのアイデンティティを完全に明らかにすることは可能である。

プライバシーマネージャーは、第三者が提供するVPNへの統合もサポートしている。

5.5.3 ハードウェアレイヤー：Trust Core™（OEM向けオプション）

SIRIN LABS Trust Core™は、機密データと暗号データ（キー管理等）の安全なホスティングを行い、秘密データをメインCPUまたはストレージに公開せずにトランザクション認証に使用できる改ざん不可ハードウェアSecure Element（SE）である。

Shield OS™はTrust Core™を使用して次のデータを安全に保管する：

- 暗号化キー（暗号化ストレージ、暗号化コミュニケーション等）
- 生体情報（指紋、虹彩、網膜等）

注記：Shield OS™を採用しているOEMは、互換性に基づいて他のSecure Elementチップを使用する場合がある。

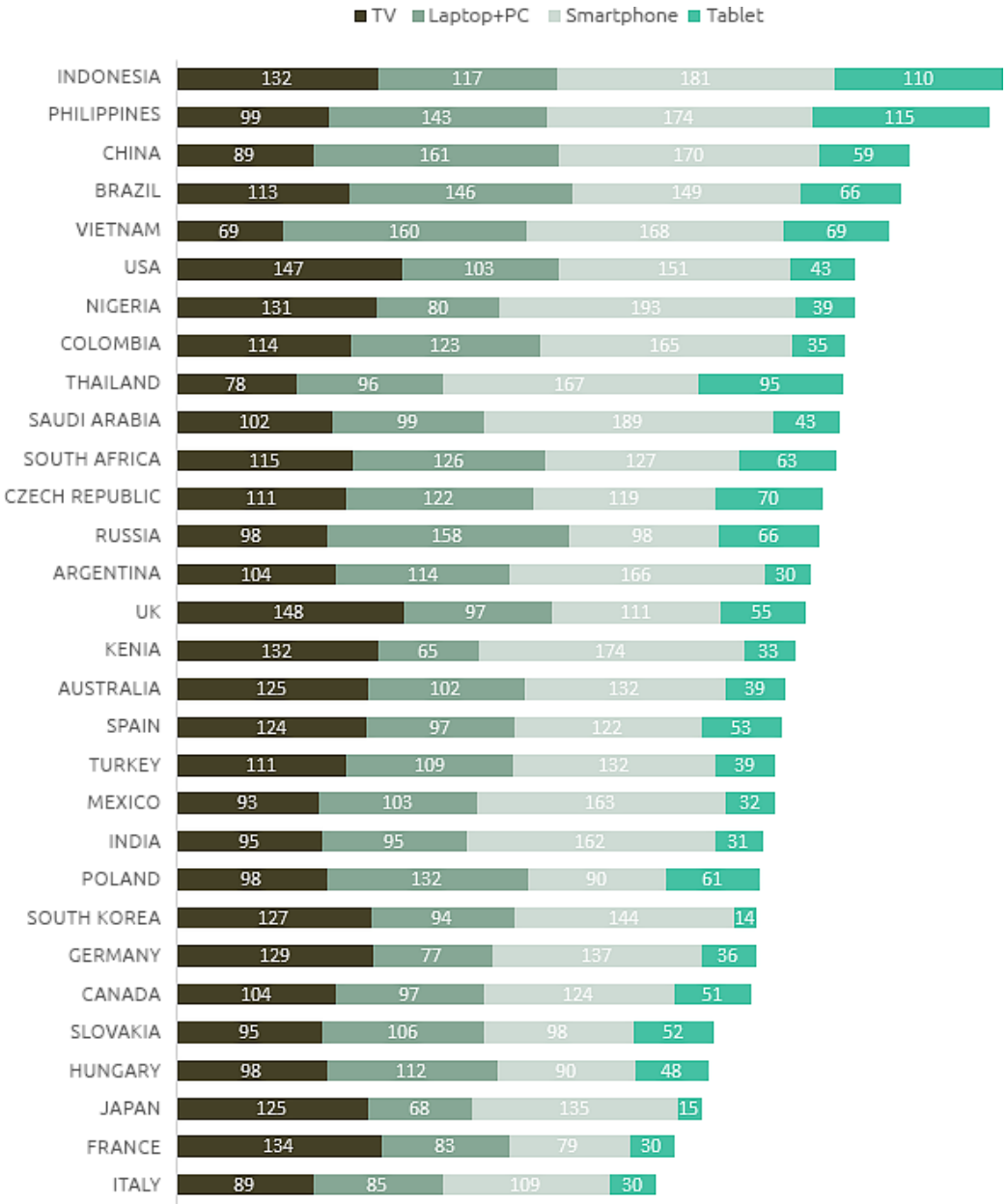
6. マーケティングプラン

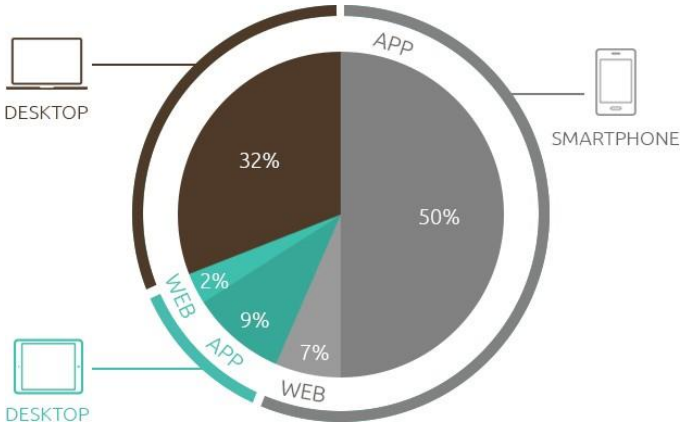
6.1 一般的な市場データ

SIRIN LABSのブロックチェーンソリューションは携帯電話やPCなど、よく使用される電子機器の主要な問題（セキュリティ、プライバシー、信頼等）を解決する。

2016年には、世界中で16億台の携帯電話とPCが販売された。さらに、携帯電話およびPCは、主に通信およびスクリーンビューイングに使用されている。

1日の国別スクリーン表示時間（分）





6.2 ブロックチェーン時代のセキュリティ

データプライバシーは大きな問題となっており、サイバー犯罪は個人や企業に莫大な被害額を生じさせると予測されている。サイバーセキュリティ市場は、2017年の1375億USドルから2022年には232億USドル以上に拡大すると見込まれている。

モバイルおよびネットワークのセキュリティに関する世界的な支出は、年間推定で110億USドルとなっている。電話およびPCの安全を守る既存の製品は非常に限られており、消費者にとって魅力的ではない。例としてGSMK CryptophoneとBlackphone2が挙げられる。FINNEY™は、ユーザーのライフスタイルニーズを満たす高いレベルの利便性を提供する、最高のブロックチェーンによるセキュリティを組み込んだ高セキュリティデバイスの最前線を行く。

6.3 ターゲット層（Shield OS™＆注目商品）

SIRIN LABSの専門分野は、高セキュリティ家電製品の開発である。ブロックチェーン技術は、セキュリティとプライバシーの分野における被害を緩和し、特に2つの主要顧客に対し豊富な機会をもたらす。

1. **クラウドセール参加者** - 主に早期採用者で構成される

クラウドセールの参加者は資金や機関を基に、「早期採用者」からはるかに精通したトレーダーへと進化した。クラウドセールで得られた資金は、資本のプールとして機能する。この規模を考えると、クラウドセール参加者は将来の暗号通貨プロジェクト貢献者のための主導的な役割を果たすだろう。

2. **OEM（Original Equipment Manufacturers/オリジナル機器メーカー）**

SIRIN LABSの製品にShield OS™をインストールするだけでなく、世界中のメーカーとの初期段階における話し合いに基づき、私たち独自のOSがブロックチェーン業界に進出したいと考えている大手家電企業にとって魅力的なものになると強く信じている。

3. **開発者コミュニティ**

Shield OS™SDKは、ブロックチェーンの力でより良い世界を創り出すことに尽力する技術者集団として知られているブロックチェーン開発者コミュニティ向けに設計されている。

4. **消費者**

ブロックチェーンの技術と暗号通貨は、人口の99.99%に対し複雑すぎると考えられている。SIRIN LABS独自の電化製品であるFINNEY™は、誰もが暗号通貨にアクセスすることができる真の機会を提供する。

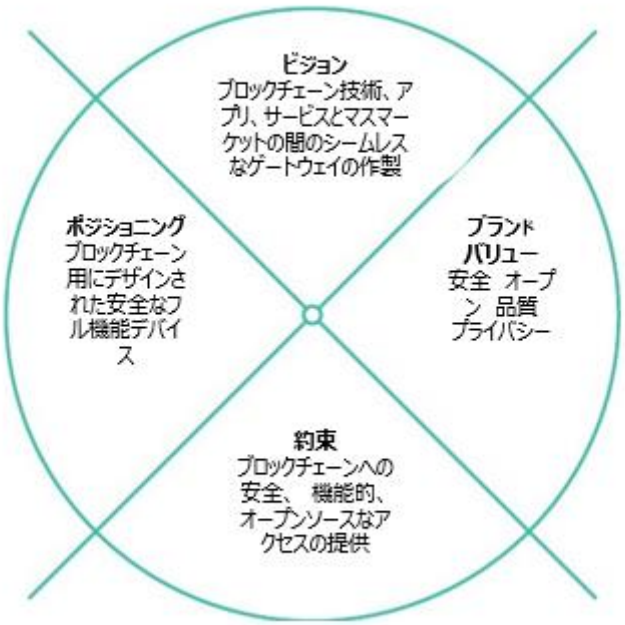
SIRIN LABSのセキュリティおよびプライバシープロトコルは、SOLARINおよびFINNEY™のコアに実装されている。さらに、価格は魅力的で競争力のあるレベルに設定されている。使いやすいコールドウォレットおよびSRNエコノミーは、ユーザーフレンドリーで使いやすく、製品を購入しブロックチェーンの革命の一部になることを望む全ての消費者によるアクセスを可能にする。

6.4 SIRIN LABSブランド

ロシアの神話によると、「Sirins」は、本当に幸せな人だけが歌声を聞くことができる美しい生物である。人間の幸福と同じくらい速くて捉えにくく、永遠の喜びと天の幸福を象徴している（ウィキペディア）。SIRIN LABS の最初の製品は、**セキュリティ**、**技術**、**デザイン**、および**品質**というブランド価値を根底に持つ、世界で最も安全な携帯電話である SOLARIN であった。

SIRIN LABS は家電製品の開発を続けているため、ブランド構築の重要性を認識している。私たちは高い基準と価値を維持しながら、製品がマスマーケットで購入できるようになることを目指している。

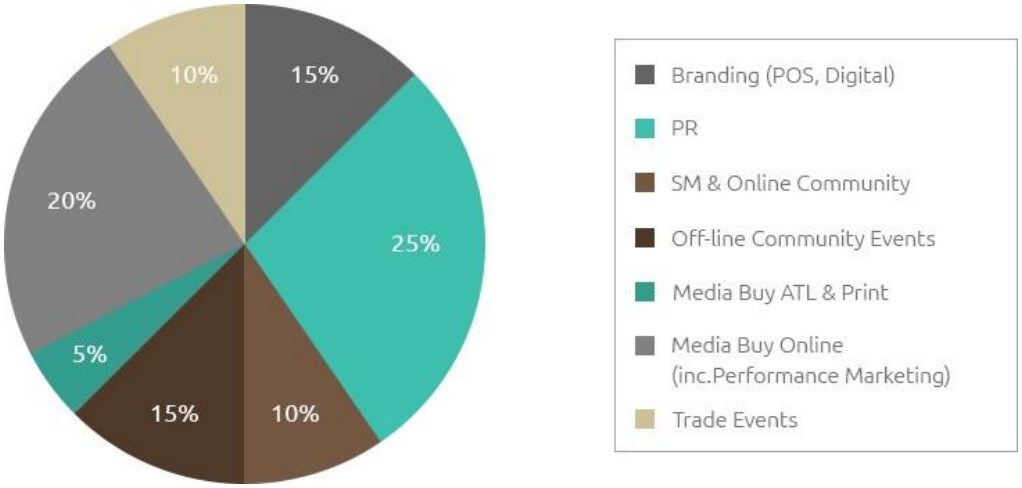
ブランドコンパス



6.5 Go-To-Market戦略（概要）

チャンネル	説明
ブランディング	ユニークで独特なブランドと製品の認識 - ビジョン、名前、ルック・アンド・フィール、価値観、メッセージおよび言語の確立
PR	マスマーケットやターゲットメディアを介した製品や価値の伝達 - 貿易出版や記者会見など
ソーシャルメディア（コミュニティーマネージメント）	Telegram、Facebook、Twitter、LinkedIn、YouTube、Mediumなどのソーシャルメディアチャンネルを介したニュース、洞察、機能、パートナーシップ、リリースなどの「ストーリー」の作成、および製品と価値の提供
メディア・バイ	有料チャンネルを使用したマーケティングおよび販売目標の達成：予算の大部分はオンラインキャンペーン（SEM、PPC、FB広告、IG）に割り当てられる。利用可能なマーケティング予算とオンライン結果に応じて、紙媒体またはテレビを介して行う。
アフィリエイト	「Pay-per-Success/成功報酬」オンラインチャンネルの使用（パフォーマンスベースマーケティング）
イベント	認知度、売上高、パートナーシップおよびポジショニングの確立 & SIRIN LABS製品紹介を目的としたトレードイベントへの出席
ビロウ・ザ・ライン	販売時点でスタッフトレーニング、ブランディング要素および付属資料を含む「ブランドエンハンサー」の導入
eコマース	eコマースのベストプラクティスの使用。ユーザー、再販業者、そしてパートナーがSIRIN LABSに従事できるようにする。
クラウドセール	認識度の向上とプレセールのサポートを目的とした発売前の話題作り

マーケティング予算の配分



6.6 セールス&ビジネス展開

チャンネル	Shield OS™	FINNEY™スマートフォン	FINNEY™ PC
OEM	✓	X	X
卸売店（代理店）	X	✓	✓
消費者向け電気小売チェーン	X	✓	✓
オンライン	未定	✓	✓

7. トークンシステム＆クラウドセール

7.1 SIRIN LABSトークン（SRN）

SIRIN LABSエコシステムは、SIRINトークン（SRN）というオープンソース暗号トークンを基盤とする。SRN暗号通貨トークンは、分配、転送および取引可能である。

トークンセール中、SRNトークンは公開されているEthereumブロックチェーンを介してERC20互換トークンとして実装され、IOTAネットワーク上のコインに互換され発売される。

7.2 SRNトークンの目的＆使用法

SRNトークンを使用することにより、SIRIN LABSの既存製品やサービスの使用および購入、そして将来の製品の事前注文が可能である。

7.2.1 クラウドセール終了直後の使用法

SIRIN LABSのエコシステムにおける活動はSRNトークンを使用して実行され、デバイスの使用および経済にとって不可欠な部分となる。これらは次の事項を含む：

- SOLARINライン製品の購入：SOLARINスマートフォン、Berylliumイヤホンおよび海外用チャージャーを小売最大価格から10%割引
- 暗号化された通話やメッセージ、一連のサイバーセキュリティなど、SIRIN LABSが提供し運営するアプリやサービスの購入
- SIRIN LABS FINNEY™スマートフォン、FINNEY™オールインワンPCおよびその他の将来のハードウェア製品を小売最大価格から20%の割引で購入可能な予約注文

7.2.2 FINNEYブロックチェーンリリース時に利用可能となるサービス

- FINNEYライン製品の購入：FINNEYスマートフォン、FINNEY PC
- P2Pリソース共有、暗号化された通話とメッセージ、一連のサイバーセキュリティ等、SIRIN LABSによって提供および運用されるアプリおよびサービスの購入
- インターネット接続、CPU/GPU共有、バッテリー充電などの共有リソースに対する決済の送受信
- SIRINLABS D-Appストアを 介して第三者により提供されたアプリやサービスの購入
- 保証、修理およびその他のサービスパッケージ
- 様々な媒介によるその他のマイクロペイメント

7.2.3 SRNトークンを使用したSOLARIN製品およびサービスの購入

- SRNトークンはトークンが発行され、クラウドセール参加者に配信された（クラウドセール終了から24時間後）時点から、SIRIN LABSの製品、アプリケーションおよびサービスの購入に使用することができる。加えて、SRNトークンを使用して商品を先行予約または購入するユーザーには特別割引が適用される。
- SOLARINは、SIRIN LABSのフラッグシップストア（34 Bruton place, London, UK） またはオンライン（www.solarin.com）にて購入することができる。

• SECURE CALL AND MESSAGEアプリケーションとサービスは、SIRIN LABSの代理店から https://www.solarin.com/contactでのコミュニケーションを通じて購入することができる。

7.3 持続可能な経済

SRNトークンが成功するためには、持続可能な経済の原動力となる必要がある。

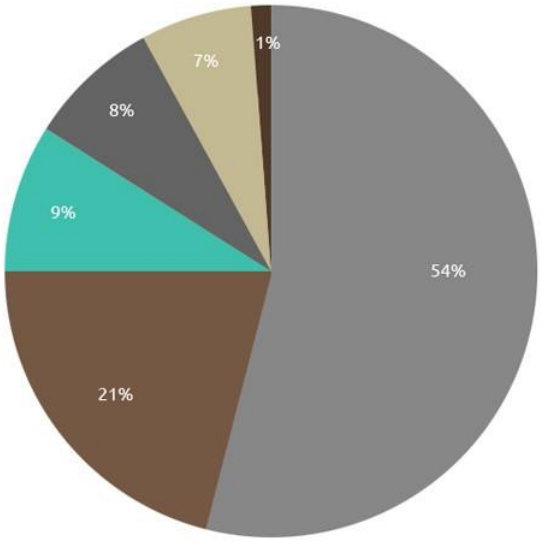
SIRIN LABSは、ユーザーとブロックチェーンコミュニティ全体のSRNトークンの採用と使用を最大限促進することを目指している。したがって、SRNトークン保有者とトークンセール参加者の利益のために持続的な成長、そして価値を生み出す。エコシステムの経済を強力にするためには、SRNトークンがSRNネットワーク内で需要を増やし、供給が比例して増加することが要求される。この等式はデバイス上でのセールスを介して提供され、メトカーフの法則ではSRNトークン使用の需要は使用中のサポートデバイスの数に比べて超直線的に増加すると予測されており、SRNトークンによるリベートをユーザーのウォレット初期起動時に直接提供することにより供給が制御される。

リベートは、毎日一定の割合で分配されるプールから取得される（デバイス販売の段階的な成長を仮定すると、リベートは公称サイズで徐々に減少する）。

これに加え、SIRIN LABSはD-App開発者およびSDKを使用している初期の開発者に、戦略開発事業に指定されたSRNトークンプールからSRNトークンを報酬として授与する。

SIRIN LABSはOEMと協力し、グローバルな流通の拡大、SRNトークンの使用、そして需要の拡大を図る。

7.4 収益の用途



USE OF PROCEEDS

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

***管理上の決定に基づき変更する可能性あり ***

7.5 トークンの発行

近い将来、SIRIN LABSのロードマップと活動に資金を提供するため、SRNトークンの初期供給のトークンセールを予定している

セールイベントは14日間にわたり開催され、出資額の制限なしに行われる。SRNトークンはETHで固定価格にて販売され、最初の供給は販売されたSRNトークンの量に基づく。

総SRNトークン配分は次の通りである：

- SRNトークン総発行量のうち40%はトークンセール参加者に分配される
- SRNトークン総発行量のうち10%は創設者およびチームに12ヶ月にわたって分配される
- SRNトークン総発行量のうち10%はOEM、オペレーティングシステムの実装、SDK開発者、デバイスおよびShield OS™ユーザー（リベート）に分配される
- SRNトークン総発行量のうち5%は専門家報酬および賞金に分配される
- SRNトークン総発行量のうち35%はSIRIN LABSに分配され、作成されたエコシステムの将来の戦略計画やリザーブとして使用される

トークンセールイベントでは次のように価格が設定される：

トークンクラウドセール実施時間	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. ロードマップ

SIRIN LABSのロードマップは、調達資金に基づいた3つのシナリオに基づいている。

- 2500万USD - OEM（携帯電話）向けのShield OS™の開発およびリリース
- 5000万USD - 上記に加え、FINNEY™スマートフォンの開発および発売
- 7500万USD - 携帯電話に加え、FINNEY™PCの開発および発売（予定）

2014

2015

2016

2017

レガシー

- 2014-SIRIN LABS設立
- 2015-SOLARIN初代プロトタイプ
- 2016-SOLARINローンチイベント

クラウドセール

2018

- FINNEY™スマートフォン　コンセプト研究
- Shield OS™コンセプト調査
- クラウドセール準備＆ローンチ

H1’2018

FINNEY™開発

- FINNEY™デバイス開発
- Shield OS™　OEM向けベータリリース
- D-App開発者向けSDKリリース
- 生産ラインの設立

H2’2018

H1’2019

FINNEY™ローンチ

- FINNEY™ローンチイベント
- オープンソースShield OS™ローンチ
- 流通媒体の開発

9. 付録

9.1 リスク開示

SIRIN LABS事業全般およびSRNトークンセールイベントに関するリスク要因は次の通りである：

- SRNトークンはデジタル通貨市場の動向によって大きく影響を受ける可能性があり、SRNトークンの価値はデジタル通貨市場における非SRNトークン関連イベントのため大きく下がる可能性がある。
- 将来的に当社は取引のためのトークン使用を制限する可能性のある世界的、または地域的な規制に影響される可能性がある。
- SIRIN LABSはBancorのインフラストラクチャおよび技術に依拠しているため、Bancorで発生する損害はSRNトークンに大きく影響する可能性がある。
- SIRIN LABSは複雑なハードウェアおよびソフトウェアプロジェクトを開発しており、予想外の開発障害のために公開が遅れる可能性がある。
- 国際法および規制によりSRNトークン取引が不可能となる場合がある。
- SRNトークンの使用は、政府機関の精査の対象となる可能性がある。
- SRNトークンの所有権は、SRNのメリットを損なう新たな予期しない課税法に該当する可能性がある。
- 本書で概説されるポジションおよび計画は、プロジェクトの進行に伴い変更される可能性がある。
- SIRIN LABSトークンセールおよびクラウドセールは、ハッカーやその他個人からの悪質な攻撃を受ける可能性があり、この場合トークンの盗難につながる可能性がある。このような出来事は、購入者および当社に大きな損失をもたらす。

9.2 Bancor （トークンプラットホーム）

スマートトークンとしてSIRIN LABSトークン（SRN）を実装する予定であり、Bancorプロトコルを使用して流動性を維持する。

BancorはERC20と互換性のあるトークンテンプレートであり、オンチェーンのマーケットメーカーを介して継続的な流動性を提供する。Bancorは2017年第2四半期にICOで1億5,000万USドル以上を調達し、ブロックチェーン業界で最大の資金調達キャンペーンの一つとした。

Bancorのスマートコントラクトは、SRNトークン時価総額の4%に相当する別の通貨（BNT）のリザーブを保有し、BNTトークンとSRNトークン間の適切な為替レートを決定し、BNTリザーブが4%のままであることを保証する。SRNトークンの取引を希望する個人は、現在の価格でマーケットメーカーから購入または販売を行うことができる。マーケットメーカーはSRNトークンを購入できるBNTトークンリザーブを保有しているため、常にその取引のカウンターパーティとして行動することができる。

トークンの特性は次の通りである：

- カウンターパーティを持たないリスクなしに、所定のコストで（取引中の為替レートの変動を事前に計算することができる）いつでもSRNトークンを売買することができる。
- SRNトークンのコア価値はBNTトークンリザーブによってバックアップされ、トークンが本質的な価値を持つことを保有者に保証する。
- BNTトークン自体はETHに裏打ちされたスマートトークンであり、ETHとの交換を簡単な二段階機能に設定している。

Bancor の詳細については、Bancor の Web サイトおよび Bancor のホワイトペーパーを参照。

9.3 参照

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

9.4 略称

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