Libra & Calibra Security

A White Paper by Rivetz Corp.

June 25, 2019

Version 1.0

steven@rivetz.com

len@rivetz.com

Executive Summary

This week, Facebook launched Libra. Their stated purpose is to "transform the global economy." Their first product will be a stablecoin, "which will be fully backed with a basket of bank deposits and treasuries from high-quality central banks." These lofty goals have the potential to truly transform international commerce.

After a review of their technical documentation describing the Libra protocol and the associated ecosystem, we believe they left out the foundational components of user security: Protection of the private key, proof of user consent, decentralized compliance and global privacy. This paper serves to share a vision and an architecture for integrating real protections and evidence into the consumer experience for the "Internet of Money" with a primary goal of ensuring all transactions on the Libra network are purposeful, intended and compliant. Rivetz and its partners are working to provide the seamless integration of these components to build a safer and simpler future. We believe that provable controls will accelerate the global adoption and address many of the digital security and regulatory challenges.

Libra has architected a permissioned chain with plans to move it to a public chain in the future. Rivetz believes there is value in starting from day one to have a vision for decentralized controls and privacy, it is imperative to reduce the reliance on the old network security models of monitoring and big data and endorse a modern decentralized network with provable compliance and controls. Rivetz is developing the architecture and tools to help Libra embed these controls in every transaction.

Libra can be a catalyst for every user to finally have a secure digital identity and the secure instructions they will need to operate their digital future. The Rivetz solution enables these next generation capabilities by leveraging the billions of dollars invested in hardware device security built on global industry standards. Libra is the use-case that can drive adoption of decentralized device cybersecurity and change how all of us access, consume and create digital services. It is time to put the global investment in built-in security to work.

Rivetz has identified three core principles that we believe are required in order to provide the consumer with protections necessary to deliver provable user intent, global compliance and privacy for the "Internet of Money".

The first principle must be to ensure the user is the owner of the private key and always remains in control of its use. The cybersecurity and compliance technology should be independent from the operation of the Libra Chain and the Libra token in order to allow the user a choice of providers. Proof of compliance is critical and the user should be guaranteed the recording of compliance for every transaction. Transactional privacy must remain in the hands of the owner and must not be circumvented by any central service provider.

The second principle is that the user must be able to prove they intended and consented to a transaction. The Rivetz decentralized compliance model allows for policies to be verified prior to the use of the private key, prior to the issuing of a transaction to the ledger. Policies can cover anything from geolocation to ensuring that appropriate anti-money laundering checks have been completed. The evidence that required policies have been verified can be bound into the transaction and recorded on the ledger. Proof of controls can be independently verified by multiple parties with strong user consent while preserving privacy. Matching an open decentralized security and compliance model with decentralized operations provides the maximum flexibility.

The third principle is to minimize risks created by the supply chain. In order to maximize user protections, wherever possible, private keys should be stored and used in a manner which minimizes the impacts of security subsystem failures. Rivetz believes the consumer will require multiple redundant protections for the private key. Rivetz has partnered with Telefonica to develop the CLIP program to define and promote dual roots of trust, a method of cryptographically combining multiple hardware elements to offer separate supply chains for protection that are used cooperatively to protect the consumers private key. This fully integrated technology dramatically reduces the supply chain risk for the trust systems as the installed base grows into the millions of users. The technology also delivers the added benefit of providing an alternate control plan for private keys when devices are not in the physical possession of the user.

Any new system needs a viable business model to assure the long-term operation of the service. Rivetz has built into the security model the use of a utility token to operate and consume cybersecurity and compliance services. The innovation of giving a device an allowance automates the compensation of a service and creates a safe and simple model for the user. The use of a token can power an economy of services to enhance the operational security and compliance for millions of devices.

The future is decentralized and the technologies of blockchain will provide the “Internet of Money”. Secure devices and trustworthy computing will provide the users with the protection, compliance, control, privacy and freedom they need for the digital future.

The Problem

The advent of digital currencies has empowered millions of users to experience a new model for the exchange of value. The solutions are available to anyone with a PC or smartphone. The revolution has been caused by a decentralized method of payments built on the incredible innovation of blockchain, a shared immutable ledger with trust and history anchored in MATH.

The Achilles' heel of the blockchain is that the user must protect their private keys and transaction instructions. One of the most valuable pieces of data on the internet is now a crypto private key. The benefit of decentralized operations, censorship resistant transactions and transactional privacy are built on the fact that a user is in sole control of their instructions to the blockchain. It is not enough to just protect a key, the system needs to create evidence that the transaction was intended and that the desired controls were in place. Global compliance and regulations will require this. Once a transaction is written to the chain it cannot be undone. The optimal approach is to pre-validate the cybersecurity controls and compliance before a transaction is committed to the chain. The full value of blockchain technology and a global payments model will only be realized when decentralized security and compliance are enforced at the devices issuing instructions to the chain.

The Libra white paper defines the use of blockchain technology but does not specify the techniques to address consumer protections and regulatory compliance. The challenge is to enable a shift from a centralized compliance model where a third party authorizes transactions based upon evaluating a set of compliance requirements, to a decentralized model where the user and their device can determine compliance before a transaction is submitted. Utilizing the foundations of Secure Identity and Trustworthy Computing, blockchain nodes can process proof of compliance embedded in the transaction request. This allows much greater choice, privacy and a stronger and more flexible compliance solution.

The shift to a device-centric trustworthy computing model has been proven to work. The Point of Sale terminal model uses the terminal and smartcard together to form secure instructions for the global payments network. The advent of chip cards and secure terminals in Europe over the last 15 years has driven fraud and the actions by bad actors to historical lows for physical presence transactions in bricks and mortar. The e-commerce security model of only card numbers and security codes has seen continued growth in fraud rates around the world, demonstrating that big data and continuous monitoring is not a viable long-term model.

The core of this problem is anchored in the fact that the mobile apps and browser services market are built on a foundation of "any device" with username and password. The compromise of passwords, a well know industry problem, has resulted in increasing fraud for these services. However, the Trusted Execution technologies used in SIM chips, Smart Cards, PCs, smartphones, cable boxes, and other devices have proven to be resilient for managing subscribers, and these technologies are broadly standardized in billions of devices. The application of Global Platform standards, leveraging the industry's enormous

investment in embedded security, can provide the modern e-commerce security that will be required by a new global billion customer e-commerce solution.

To understand this more fully, it is important to understand the challenge of transactional security is not just assuring the proper identity of the originator of a transaction, but also that the instructions associated with that transaction are the ones intended by the originator. Cybersecurity technology enables the assurance that a transaction created was the transaction intended and includes not just the signing of the message with an identity but also assurance that the ***sender*** verified and consented to the instructions being sent. ***A secure instruction also requires that the sender and receiver are both confident that the identities and cybersecurity controls were used as intended, and that the message wasn't changed after being sent.*** The blockchain networks of the world are all operated by secure instructions. The quality of the data on the chain is only as good as the quality of the instruction transmitted to the chain. Decentralized networks should require the evidence of controls to be immutably bound to the transaction.

The science and practice of cybersecurity has been a model built on big data, monitoring, censorship and central control. Typically, traffic is watched and blocked to attempt and filter out bad transactions. In addition, financial compliance is usually applied after a transaction is submitted but before it is cleared and settled. Facebook's Libra Chain needs a reliable infrastructure to enable decentralized cybersecurity and compliance in order to fully realize the power of the decentralized model. The private keys and the compliance controls must be under the exclusive control of the owner of the private key. While the owner can select partners to enable cybersecurity services and controls, ultimately the decision to engage those controls must be the user's decision. Users must have the choice to switch service partners creating a competitive and open market for the compliance and security controls touching the user's most sensitive data.

The Libra chain will have many third-party service providers as the on and off ramps of Libra. In addition to the chain nodes, additional centralized services will be required for the ecosystem to deliver value to its customers. These supporting applications require the same decentralized cybersecurity and protection models that users require. Evidence that the built-in cyber controls are present for every transaction will be required for compliance. **If a device or server cannot prove that it is in the appropriate state, controlled by the appropriate party, with the appropriate permissions to conduct the transaction, the transaction should be denied before it is ever completed. This is a revolutionary and critical approach to enabling decentralized, worldwide transactions.**

Libra has the potential for incredible global impact. The perception created by cryptocurrencies and blockchain is that the solutions are secure. The lack of protections for integrity and consent have stalled many global projects. Libra has listed 3 core goals:

- It is built on a secure, scalable and reliable blockchain.
- It is backed by a reserve of assets designed to give it intrinsic value.
- It is governed by the independent Libra Association tasked with evolving the ecosystem.

The project is missing **a fourth**, **critical goal**;

- It is decentralized and operated by keys and instructions anchored in trustworthy computing with strong consumer protections, controls and privacy.

Libra is missing the fundamental device cybersecurity components to deliver secure e-commerce. While great attention has been paid to the security of the protocol, the protection of the user's intent and compliance also requires a revolutionary response. It is the combination of blockchain principles and technologies as well as the integration of trusted computing principles and technologies that will deliver the freedom and protection needed for the "Internet of Money".

Rivetz Solution

The “Internet of Money” requires that the consumer protections and transactional security exceed any solution available today. Hooking a blockchain to an exchange that authenticates via username and password will not meet the needs of a billion users. The challenges of identity, control, privacy, compliance and ease of use must all be addressed. The principles of decentralized operation must be preserved to protect the consumer’s privacy and freedom. Consumers must own their private keys to allow for choice. Global custodial solutions are required to assure users never lose control of their keys.

The Rivetz solution is built on the foundations of payment and device security standards established over the last 20 years. Rivetz uses the technologies and standards of Trusted Execution, Global Platform, Trusted Computing, NIST information assurance, Payment Security Directive 2, GDPR and many others. The Integration of Trusted Computing standards and the billions that have been invested into the embedded hardware offers a set of global industry standards and vendor neutral solutions to address the challenge. These technologies enable the creation of secure instructions with embedded attestation and identity, providing for provable, reliable and intended transactions.

The Rivetz solution is built on separating user intent, compliance and controls from the underlying transaction network. The transaction network only needs to know provable controls are in place. The parties to a transaction can agree to the infrastructure for compliance and it can operate separately from the underlying Libra Chain. The global complexity of the “Internet of Money” can be reduced to verified proof of user intent and compliance. Verification of the proof is a simple and private cryptographic transaction with integrated privacy. Decentralized compliance and control will operate across borders and across industries simplifying the process and delivering a safer solution. There are no shortcuts; identity, privacy, compliance and assurance must be built-in.

Rivetz has built and demonstrated the infrastructure for the existing network operators to empower their users with the next generation technologies to operate the blockchain. Simple integration into wallets will allow for an API driven compliance model that is under the transacting parties control. Policies and API’s on a decentralized basis controlled by the owner of the private key will embed the proof of compliance at the transaction level. The nodes and eventually the Move modules can then validate the proof of compliance, or just record it.

Secure Instructions – How Users Operate Blockchains

Global financial services are more complex than just authentication. The “Internet of Money” is operated by secure instructions. A secure instruction is a message that is signed by the user’s private key. The quality

of the instruction is dependent on the system that creates it. If an instruction is created on a computing device with malware then there is a possibility the transaction can be altered during creation or that the private key can be stolen.

To securely move value from one address on any ledger to another requires a secure instruction. Systems like EMV, the consumer chip cards and Point of Sale terminals in use every day, deliver the instruction security required for the credit card networks. Modern mobile devices and PCs now have all the technologies required to create secure instructions.

A secure instruction consists of:

- **What you see is What you Sign**

  It is critically important that the instruction being signed is the actual instruction the user wishes to be processed. Technologies such as Trusted User Interface 1.0, part of the Global Platform specification, provide the isolation technology to assure the information on the screen of your mobile phone cannot be altered. The display is isolated from the operating system and is part of the trusted computing capabilities of the hardware. Instructions can be created on any system if appropriately confirmed by a user with a trusted display.

- **Provable Human Consent**

  The use of Secure PIN or Biometrics assures the user is part of the instruction and that malware cannot commit transactions on the device without the user's permission. The PIN or Biometric provides proof the user consented to the instruction being sent. User consent is an important piece of the financial services and the existing regulatory landscape that needs to mature to be more than a one-time click through agreement.

- **Protection of the Private Keys & the Transaction Signing**

  The protection of the private key and the signing process is the point where the instruction comes together. All information needed to process the instruction must be part of the signed message at the time it is signed. A simple signing process is not enough. The Rivetz process enables the Trusted Execution Environment to assemble multiple sources of information securely into one instruction and to authorize that instruction for processing by signing with a private key whose lifecycle has been entirely resident in a tamper-resistant protected environment.

- **Provable Compliance**

  The Rivetz Trusted Execution app will enable a manifest of controls to be performed prior to the signing of an instruction. These controls are the result of internal and external queries that are established by the owner of the private key and required to be processed before a key can be used. The evidence proof of this manifest can be a hash of the completed controls bound into the signed instruction and recorded on the chain.

- **Attestation of the Device That Created the Instruction**

  A core capability of Rivetz is the global attestation network that enables the owner of the platform to record the measured state of their device and assure that the device is operating as measured. Attestation assures the Trusted Execution Environments are configured as intended and that the required computational resources were verified to be operational.

- **The "Second Hash"**

  In order to measure and record compliance, Rivetz has created the "second hash" as a measure of the integrity, intent and compliance for a transaction. The second hash is a created by combining the measurement of pertinent characteristics and controls into a single digest which encapsulates the full manifest. Rivetz leverages the guidance from the Trusted Computing Group standards and provides a privacy preserving model. The second hash is mathematically bound to the instruction and recorded on the chain providing the provable evidence that the decentralized controls were verified. The second hash can assure to either the receiver, or an auditor of a transaction, that the controls intended were in place.

The Libra chain can participate as validators of the proof of controls assuring a flexible and dynamic solution for integrated compliance with privacy. The second hash in a transaction provides the mathematical permission slip that compliance has already been satisfied. This opens the market to a global third-party cybersecurity and compliance model that can be verified, audited and enforced by the transacting parties and regulators.

The User is in Control

At the center of the "Internet of Money" is the owner of the private key. The blockchain infrastructure is trustless and should not have the ability to alter transactions, freeze accounts, or change balances. The chain is just the immutable ledger that records the evidence of the transactions processed.

The real power should only be in the hands of the owner of the private key, generally the consumer. The owner can then choose to connect to many services and utilities that help them to manage this new role as the controller of their financial services. The ultimate protection needs to be the owner's control of their private keys.

Transactions with Compliance vs Platforms with Compliance

Transactions with Rivetz enforced compliance, provides a solution for permissions that can deliver billions of users the security and compliance they require across the infinitely complex and constantly shifting

regulatory landscape that is our world today. The transition from centrally delivered permission to transactions with provable controls will allow the systems to deliver on the global promise of the "Internet of Money". It is critical to start day one with a clear vision to achieve that goal.

The systems for bank secrecy, payment licensing, cross-border regulation, micropayments, large payments and identity can all be automated with privacy and provable compliance and consent. Decentralized controls with blockchain more closely matches the user's natural expectations. Users expect to conduct commerce with known parties and with rules. Users are uncomfortable with central controls and fraud from unknown users. Assuring the information created comes from a known device in a known condition with provable control reduces the risk that malware is creating instructions or sharing bad data.

The Rivetz solution isolates the compliance and control layer from the blockchain ledger allowing the transacting parties to choose their agreed methods of compliance and create the evidence that regulators will require. The open systems solution supports programable compliance and policy to drive efficiency into every transaction. The second hash in the transaction is the evidentiary proof of the compliance process conducted prior to the execution of that transaction.

The Rivetz solution will meet the needs of global regulators, the privacy requirements for users and control needs of the individual asset owners. Rivetz helps to remediate some of the negative aspects of a permissioned chain with central controls and shift the permission to a decentralized model that meets the needs of the transacting parties. The decentralization of power will provide a robust market driven network that is fueled by consumer choice and controlled by many systems.

Privacy will be a cornerstone and the owner of the private key will need the tools to assure their data is only shared with consent and only with those who need to know. Ultimately, automation will introduce central authorities as service providers, but the authority is bound to the owner of the private key and not the Blockchain.

The process to validate compliance can ultimately be part of the blockchain. With the appropriate virtual machine capabilities in place, compliance can be integrated into Move modules. Ultimately, on a public chain architecture, the compliance validation is between the two parties.

The "Internet of Money" should be controlled by the owner of the private key.

- There will be rules.
- Digital money will have history.
- Quality is earned by compliance.
- Certain services might require higher quality money.
- Owners will need help.

The chain is the record and should only enforce controls that the transacting parties agree upon. The control layer should remain separate, as its functions are very different than the existing digital services

of today. Rivetz is building the core systems required to operate the “Internet of Money” and assure that their financial services operate as they intend.

Decentralized Provable Compliance & Cyber Controls

The Rivetz network provides the key management to uniquely bind policy service providers to individual keys. The system supports the registration and integration of multiple services from multiple providers. It is based on a simple messaging construct allowing a trustworthy compute environment to act as a policy enforcement point or toll booth. Once the pre-established policies for compliance, cybersecurity and operating controls are satisfied, then the private key can be used to authorize an instruction.

The advantage of executing policy controls within the consumer’s device is that privacy is built-in. The evaluation and the request for verification takes place from within a secure enclave on a device that is isolated from view by any third party. The validation of a control uses a secure message with privacy protecting end-to-end security. Only the user’s chosen validator and the user are exposed to the personal data. The validator is also only provided the data they need to know, protecting the validators from aggregating or collecting information they don’t need. The solution is built on a foundation of consent, assuring not only the regulations, but also the spirit of data protection is designed in.

The manifest of controls can be published or kept secret by the owner, and it can be securely provided to the transacting parties or to the regulators. The evidence of the controls is mathematically bound to the transaction by embedding a second hash, helping the owner of the private key to make any claims required. Using the existing transaction key’s access to a manifest can be easily provided to the receiving party with simple end-to-end encryption and integrity.

Multiple Roots of Trust

Consumers outsource security and that can create significant risks. Until appropriately patched, client devices were exposed by design failures such as Spectre and Meltdown. Zero-day attacks are a potential for all devices at any time. As part of our trust architecture, we have researched fault tolerant protection mechanisms for private key lifecycle protections.

Rivetz has built a partnership with Telefonica to research and develop next generation protections that allow multiple roots of trust to protect the owner’s keys and instructions. The goal has been to leverage the existing hardware that is already present in modern mobile devices and to take full advantage of existing embedded hardware. The result is the CLIP Program.

The Carrier Level Immutable Protection (CLIP) Program takes full advantage of the SIM and the Trusted Execution Environment in a device to protect the private keys. The solution leverages the separate trust

infrastructures of the carrier and the device manufacturer assuring that no single supplier can compromise the owner's keys, either intentionally or by accident. The additional benefit for the owner is the integration of the global carrier network as a control system to enable and disable access to specific keys on a specific device. This provides the owner with unprecedented global control over their personal or corporate devices, independent of whether they are in their physical possession.

The CLIP Lab is operational today and provides a real-world test environment for the integrated carrier controls and key management for next generation cybersecurity capabilities. Rivetz publishes developer tools that allow any application to take advantage of these capabilities and incorporate carrier grade protections for identity, loyalty, payments and general security. We will continue to onboard partners to join the program in providing state of the art local protection for keys and instructions within the mobile and IoT ecosystem. Hundreds of millions of global customers already have the technology to deploy CLIP within their handsets today.

With the Rivetz solution the carrier and network providers can deliver the decentralized cybersecurity and compliance controls that every user will require. Leveraging the existing KYC and support infrastructure, millions of users are already equipped to operate the "Internet of Money". The decentralized control, privacy and user choice will be a critical part of assuring global acceptance for these new financial service models.

Never Lose the Keys

Rivetz believes it must not be possible to lose your keys. The same security mechanism that is used to bind policies to keys can be used to create a provable custody model. Multiple keys or shards can be used to recover a single private key. The recovery keys can be securely transmitted to a collection of other user devices or services to assure that the private keys cannot be lost.

One of the policies for usage of a private key could be to ensure that the private key remains securely archived. Custody and escrow services, such as Blockchains.com, who provide geographically dispersed and physically secure locations to archive portions of a user's private key, could provide secure assertions of an escrow condition.

Rivetz believes the ultimate consumer choice is that the keys can be recovered into any compliant device. It is important to allow the user to change how cyber controls, compliance and operations are executed. The power to switch providers created the competitive marketplace for internet service providers and the power to switch must be at the heart of how users choose to operate blockchain infrastructures.

The Business Model for Decentralized Security

The business model for decentralized security is built on a foundation where compliance and controls are verified prior to the execution of a transaction. Service providers who participate in providing or validating these controls will be paid on a per transaction or subscription basis. The core driver of revenue is the transaction originator needing to demonstrate provable cybersecurity and compliance controls, whether dictated by a geopolitical entity, an enterprise, or by the owner for personal use.

Rivetz has developed a token-based model to provide the device with a store of value that can be exchanged for services delivered to the device. The model additionally supports zero fee transfers between devices and service provider accounts in order to enable micro-transactions. The model also separates the digital currencies from the compliance controls, offering additional privacy. A user may authorize the exchange of tokens to occur automatically and not require user interaction for every micro-transaction. The use of the Rivetz token will be an integral part of the audit process, providing evidence the policy services were consumed. This creates a new model for controls and for service compensation taking advantage of the embedded identity that is part of every transaction on a blockchain.

The breadth of services which will be valuable to devices is almost unlimited. Rivetz is working with many organizations to build a network of service partners to provide the solutions every user will require. The goal is to ensure that all deployed applications take full advantage of these capabilities to assure the consumer has a simple and safe experience.

The ecosystem for centralized cybersecurity and compliance is mature, with an emphasis on providing service to the application and the network layers. Rivetz is expanding the market opportunity to provide trust services to the transaction formation in a decentralized manner. The use of these tools to improve the quality of the transaction has the potential to create a global market for higher quality data and the services that create it.

The Future

Blockchain has created a catalyst to disrupt the foundation of financial services. The shift to decentralized applications and services requires a new approach for the security and compliance models. Centralized compliance, identity and security dramatically weakens the blockchain promise. Rivetz believes the future is one where digital identity and the ability to create data that is intended are just part of the fabric of our everyday life. Much of the promise of blockchain is built not only on the chain, but also the public-private key technology that secures the instructions. Proof of compliance and integrity will ultimately increase the trust of the data recorded and secured by blockchains.

Our collection of devices is our identity and not just a single personal device. Our collection of devices can provide shared redundant protection for the storage and use of our digital assets, including the keys that operate Libra and the keys that manage our IOT. The mobile device will be our primary interface device and it is logical that the existing network operators continue to help us to manage and operate our digital

lives. The global infrastructure of the carriers can dramatically simplify and deliver familiar touch points to help consumer connect, use and move services.

The new paradigm is a world built on collections or groups of devices providing their users an identity-based model of the network, where services are delivered not based on connections but based on identity. This revolution has already changed the telephone industry entirely. It is now time for the rest of the global network to go mobile from payments to enterprise. Cybersecurity has been a network security model for the last 30 years. The new identity model of networking will require security to move to the device that creates the data and not a model where services watch the data. A future that is simpler and safer to operate and where control is in the hands of the owner of the KEYS.