The Financial Passport

The Financial Passport – FINPASS – is a digital container that holds the most important information needed to obtain a loan quickly, ***from customer identity and compliance to financial history and credit ratings***.

The value of FINPASS is its ability to provide any institutional lender with the necessary, secured data to make quick, accurate decisions on credit worthiness and borrowing capacity, with all appropriate compliance being satisfied.

Draft 37 – Contents are subject to change

Andre-Ivor Wills, Kyle Boyko

Last updated on July 22nd, 2019

Finpass

Contents

1. Glossary

Distributed - in an information technology (IT) context, means that something is shared among multiple systems which may also be in different locations. In distributed computing, processing and data are spread out over multiple computers, usually over a network.

State - In information technology and computer science, a program is described as stateful if it is designed to remember preceding events or user interactions; the remembered information is called ‘the state of the system.’

The set of states a system can occupy is known as its ‘state space’. In a discrete system, the state space is numerical and often finite, and the system's internal behavior or interaction with its environment consists of separately occurring individual actions or events, such as accepting input or producing output, that may or may not cause the system to change its state.

Step change - (in business or politics) a significant change in policy or attitude, especially one that results in an improvement or increase.

Blockchain - a type of digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly.

Distributed Ledger - A distributed ledger (also called a shared ledger or referred to as distributed ledger technology) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.

EVM – the Ethereum Virtual Machine is designed to serve as a machine which acts as a runtime environment for Smart Contracts based on Ethereum

Adjudicate - make a formal judgment or decision about a problem or disputed matter. In the context of Credit, adjudicate refers to the formal judgement regarding the credibility of an applicant (business or consumer).

KYC/AML - Know your customer ('KYC') is the process of a business identifying and verifying the identity of its clients. The term is also used to refer to the bank and anti-money laundering regulations which govern these activities.

Credit score - a number assigned to a person that indicates to lenders their capacity to repay a loan.

Business credit score - A number indicating whether a company is a good candidate to lend money to or do business with. Business credit scores, also called commercial credit scores, are based on a company's credit obligations and repayment histories with lenders and suppliers; any legal filings such as tax liens, judgments or bankruptcies; how long the company has operated; business type and size; and repayment performance relative to that of similar companies.

Ethereum - an open-source, public, blockchain-based distributed computing platform and operating system featuring Smart Contract (scripting) functionality.

Smart Contracts - a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

API - In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. A good API makes it easier to develop a computer program by providing all the building blocks, which are then put together by the programmer.

2. GENERAL BACKGROUND

Rapidly evolving customer demands for faster digital services, combined with increasingly complex compliance requirements are subjecting traditional financial institutions to growing costs and exposing the limitations of their decades-old technology.

As well as becoming more complex, compliance requirements are tightening. The scope of rules established by governments to protect their citizens is expanding. Regulators are becoming more effective, laying heftier fines on banks who don't comply fully with the law.

Costs to stay compliant have increased every year, with most banks reporting a **20%** increase in compliance costs from 2016 to 2017. Banks are focused on lowering these costs, and to do so they are turning to technology to streamline their reporting and verification methods. The basis of the first half of this paper is to address this issue of rising compliance costs. [i]

Customer demands for faster digital services are increasing; they want to do more, but with less effort. During and after the 2008 recession, financial technology (fintech) companies - small technology companies that offer a digital alternative to banks – appeared to fill product areas big banks had vacated on account of the recession. The rise of fintech companies, coupled with customers' increased use of technology in their daily lives, has forced banks to move aggressively to meet the new needs of their consumers. The increase in customers' demands has forced banks to rethink the way they offer credit products. Their response -- or lack thereof -- is the basis of the second half of the solution described in this paper.

But upgrading is not that simple. Core-banking systems are notoriously out of date, making updating old frameworks expensive and clumsy. Updating the ways of utilizing data and technology for both the customer and bank also mean adapting to new rules for compliance.

Outsourcing process digitization and automation are the answers to these problems. Technologies like the Financial Passport (FINPASS) - can lower the costs that banks incur when observing know-your-customer (KYC) and anti-money-laundering (AML) compliance laws. At the same time, these technologies enable banks to upgrade their onboarding and adjudication processes for banking products in order to meet today's customer demands.

This will allow banks to satisfy their customers' increasing need for an improved banking experience, while cutting costs.

There is an undeniable shift in the banking industry towards digitization and automation. Those who do conform to this industry shift will have the tools to attract new customers, retain existing ones, and deepen the relationship with current customers. Not adapting to the change today will have consequences that will be hard to reverse tomorrow. This paper will introduce the reader to a simple-to-implement technology for compliance verification and consumer/commercial scoring technology. It is called FINPASS.

Overview

Sqirl is pleased to introduce a global identity verification and financial history tracking service, FINPASS.

FINPASS is an online service that verifies individual or business banking customers, while incorporating their financial history and health in an easy-to-update 'passport' that the customer carries on their person and uses when engaging with a bank of their choice.

A Financial Passport contains:

- Yes/No (KYC/AML/PEP/etc. – compliance-based verification)
- Personal credit score
- Commercial credit limit (Value under x for instant approval)
- Image of the business owner
- ID Key

Value Proposition

The value proposition is that FINPASS saves time and money for both banks and their customers. Having important information readily available when a customer engages with a bank is the foundation to the financial passport's value.

FINPASS is like a country issued passport. A country issued passport verifies who you are and where you're from. A country issued passport's value is the quick access into sovereign nations.

The Financial Passport draws parallels to a country issued passport. The Financial Passport *verifies your financial identity* via government stated compliance rules and your *financial creditworthiness* in an instant. Its value is the quick access to credit products including credit cards, mortgages, personal loans, personal or asset financing, commercial SME loans and more.

FINPASS has clear value for both banks and customers.

For banks:

- Lower costs – It dramatically cuts the cost of verification and credit adjudication
- Best in-class data security – Top-notch protection and security of verified customer data
- Easy for banks to implement – FINPASS is not reliant on a separate technology and does not have to connect to existing core banking systems. Current core processes will also not be affected.
- Faster sales - Saves time by reducing the sales cycle when KYC/AML and adjudication are made ready by FINPASS

For customers:

- Speed – Decision wait times for large ticket products like mortgages and commercial/SME loans will decrease.
- Speed of the process – Customers will benefit from a streamlined interaction with their bank because they and their credit situation are verified and updated in milliseconds.
- Personalized service – With all the data readily available, the customer experience will dramatically increase for a FINPASS holder
- Data transparency – Customers will be able to view their credit score from the customer dashboard and know how it will affect their potential banking plans (which banks are more likely to approve them for a loan at their current credit rating for example).

Banks who use FINPASS will significantly cut the cost for adhering to KYC rules and AML regulations. At the same time, FINPASS will also decrease costs to onboard and adjudicate people looking for credit products. Through FINPASS, financial institutions will have instant, real-time knowledge about the complete current and historical financial health of the FINPASS holder. This is because the current and historical debt obligations, as well as the associated risk scoring that FINPASS has completed, can now be immediately accessed by the simple click of a button. This enables a bank to understand a user’s creditworthiness.

FINPASS will have a dramatic impact on everyday banking in North America. People will now have a tool to simplify their everyday banking experience. The ability to carry their easy to update financial history and verified identity application is just short of a priceless advantage.

This paper will argue that current banking standards and practices have failed to produce step-change innovation, thus leaving an **antiquated system for compliance and financial scoring** in place for FINPASS to leverage.

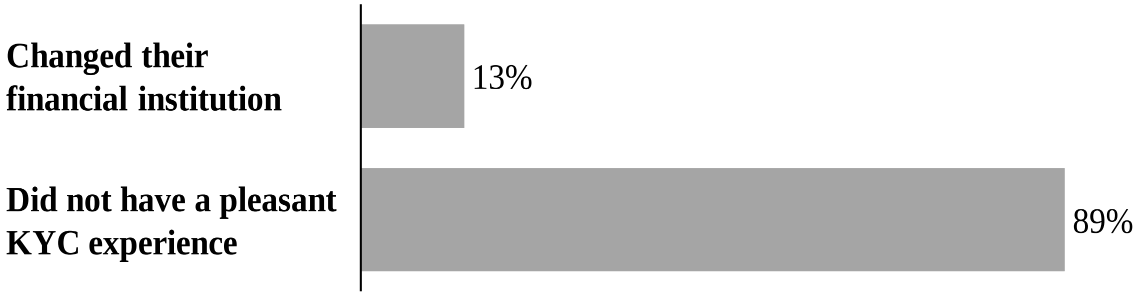
3. Market Challenges

Lenders spend too much time and resources satisfying KYC/AML

In 2016, Thomson Reuters released parallel surveys showing differing perspectives on the effect of financial firms around the world spending up to $500 million annually on KYC. [ii]

The lack of sufficient human resources and the volume of regulatory change are top concerns among global financial institutions and their customers. Nearly 800 financial institutions responded to a recognized Thomson Reuters survey on the impact of global changes in know-your-customer regulation. A parallel survey of their corporate customers found that 89 percent had not had a good KYC experience, and 13 percent had changed their financial institution relationship as a result. [iii]

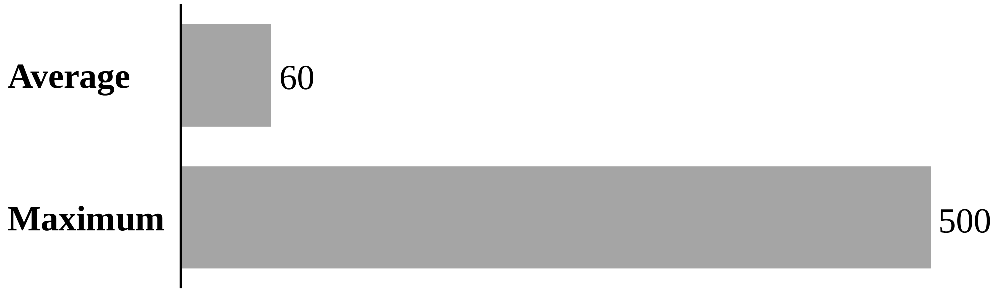
EXHIBIT 1 – IMPACT OF GLOBAL KYC CHANGES ON CUSTOMER EXPERIENCE (% OF RESPONDENTS)



Source: Thompson Reuters

The global surveys revealed a single, clear message: The costs and complexity of KYC regulations are rising and having a negative impact on lenders businesses. While financial firms' average costs to meet their obligations are $60 million, some are spending up to $500 million on complying with KYC and overall Customer Due Diligence (CDD) laws.

EXHIBIT 2 – KYC/AML COST PER BANK ($M/YEAR)



Source: Thompson Reuters

Both financial institutions and their corporate customers agreed that longer KYC procedures are putting more strain on the onboarding processes and bank to client relationships. The time to bring a new client onboard is up 22 percent from 2016, an amount that is anticipated to increase by 18 percent over the next year. Furthermore, 30 percent of corporate respondents reported that the average time to onboard clients is more than two months, and 10 percent of the corporate respondents claim an on-boarding time of more than four months. Customers claim that they have, on average, eight different interactions with the bank during the process. [iv]

A Sqirl Solution

As mentioned, the know-your-customer and anti-money laundering due diligence process is outdated and generates costs of between 50 to 500 million USD per year, per bank.

Sqirl proposes a new 'one and done' system. In it, **the core KYC verification process is only conducted once for each customer when onboarding onto FINPASS**, regardless of the number of financial institutions with which that customer intends to interact with or the number of financial product applications they intend to submit. Thanks to **distributed ledger technology**, the result of the core KYC verification can be **securely shared and trusted** by all the financial institutions with whom the FINPASS holder intends to work with. This system allows for efficiency gains, cost reduction, improved customer experience, and increased transparency throughout the process of onboarding a customer.

Acquiring and Utilizing Financial Performance Data is Difficult

Core banking software is defined as the software that supports a bank's transactions like the opening of accounts and processing of cash deposits. The challenge presented by the current selection of core banking systems is their inability to adapt to today's standards for utilizing data.

Historically for banks, big data initiatives have predominately revolved around acquiring and improving customer intelligence, reducing risk, and meeting regulatory objectives. These are all activities large Tier 1 financial firms continue to tackle today and into the near future. However, down-market, we see mid-tier and small-tier firms (brokerage, asset management, fintech startups, etc.) are able to adopt new data platforms more rapidly which are helping them leapfrog the architectural complexities that their larger counterparts must work against.[v]

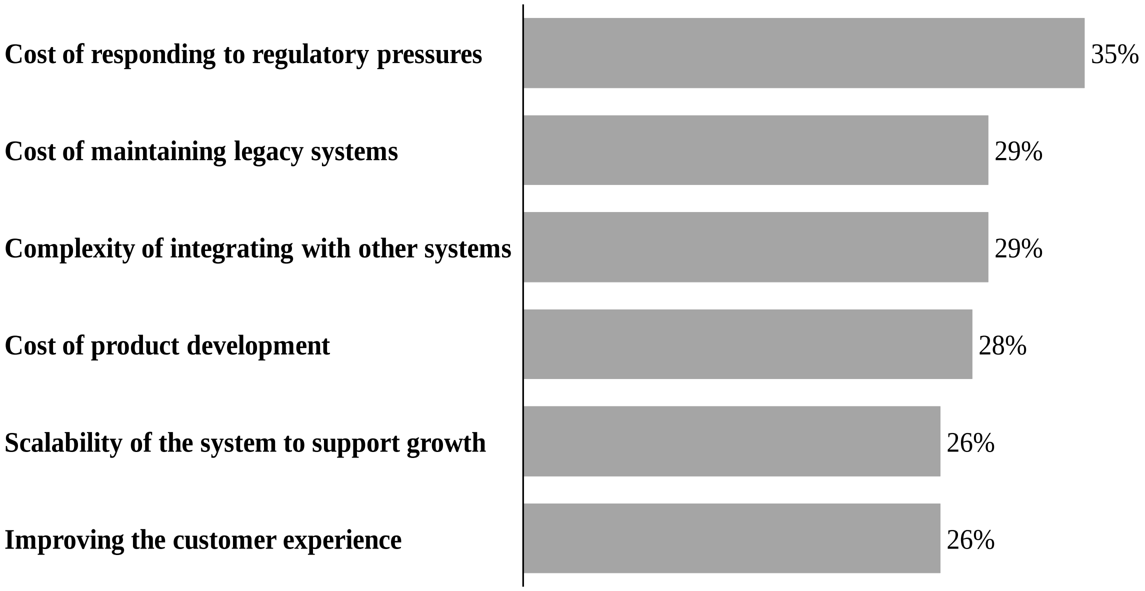
For example, companies like QuickBooks – a market leader that offers seamless accounting solutions for businesses – allow third-party vendors to access their data pipeline through Application Programming Interfaces (API's). QuickBooks offers an API enabled technology of their core accounting software called QuickBooks Online or QBO. API enabled software's like QBO are special because they have given alternative financial service lenders an advantage over large banks and credit unions for years.

With this API data advantage, alternative lenders can service their customers online, **fully and immediately**, delivering the competitive edge in customer experience and quality of service. Through API's, frictionless access to these **data points** have enabled the innovation of data analytics, financial analysis and compliance checks that give alternative financial service providers a variety of runoff products.

This is not to say that incumbent financial institutions today do not use API technology, because they do. It is to illustrate the reality that traditional financial institutions move slowly and are usually playing catchup to their smaller, tech-forward peers.

In order to rival this new breed of competitor, banks are under intense pressure to increase efficiencies and reduce costs, while delivering next-generation digital services. However, incumbent application vendors that help service the banks have been slow to respond to new requirements, according to a new report from NTT Data Consulting.[vi]

EXHIBIT 3 – MAJOR CORE BANKING SYSTEM CHALLENGES FACED BY FINANCIAL INSTITUTIONS (% OF RESPONDENTS)



Source: NTT

Sixty-four per cent of respondents believe that “The cost of responding to regulatory pressures and the cost of maintaining legacy systems is the major challenge their financial institution faces.” This graph shows that the **two most commonly reported areas that are a problem for financial institutions** are the two areas to which FINPASS looks to add the most value.

Digital Delivery is Currently Not Suitable for Today’s Needs

Digital delivery is the act of transferring virtual content or value on the Internet to a specific destination. [vii]

Today, it costs time and money for a bank to manually prep, deliver or review their customers’ financial data when completing a credit application and an adjudication for credit products. New technologies would enable the bank to gather the relevant client information far faster and with lower expenses.

As mentioned in the previous section of this paper, what hinders the banks from harnessing these technologies are their existing ‘Core Banking Systems’ and the resulting processes that accompany these legacy systems. Multiple Core Banking Systems (CBS) underpin nearly every major banking process. Think of them as the information technology that runs a bank’s central nervous system—the software and infrastructure that link services to business units, customers, and back-office functions. These systems not only drive the banks’ day-to-day operations, but also serve as the core IT platform for new capabilities and growth. Yet many banks are burdened with underperforming systems and outdated architectures that barely support key processes. This is at a time when these institutions are facing renewed pressure to rein in costs and adjust to volatile conditions in an increasingly competitive financial system.[viii]

Over the last decade, banks and other financial institutions have failed to keep up with the ability of new technologies to deliver data. They have specifically failed to compete against the advent of 3rd party Software-as-a-Service solutions that offer accounting and other financial management tools like payment solutions and ecommerce plugins. These new software vendors have captured a large segment of the financial reporting and bookkeeping market, allowing business and consumers to keep track of their financial activity more efficiently and with greater online accessibility.

These new solutions have enabled a new generation of data analysis and specifically, credit analysis tools that financial institutions should be utilizing, since they grant immediate access to the key financial details used in credit analysis. This would translate into significant cost and time savings, as well as the ability to complete enhanced customer due diligence in a fraction of the time it takes today.

Banks have been slow to recognize the opportunities presented in connecting to 3rd Party technology services that empower businesses to manage their day to day operations, and the additional access channels that API’s would offer. To use an earlier example, if a bank were to connect to the QuickBooks Online API, it would allow them immediate access to the financial data that drives their risk adjudication. These new API focused solutions enable a new generation of data analysis and specifically, credit analysis tools that financial institutions should be utilizing. This would translate into significant cost and time savings, as well as the ability to complete enhanced customer due diligence in a fraction of the time it takes today.

4. FINPASS OVERVIEW

FINPASS is a global, decentralized identity verification and financial history record.

FINPASS is a simple technological solution that is easy to implement and understand, which responds to the industry challenges in both KYC and credit scoring. The passport is a one-stop solution for financial institutions to receive the overarching benefit of having the KYC/AML verification and credit adjudication powered by the world's most secure digital delivery system, called the blockchain. This means that verification is already completed when a passport carrying customer **(re)enters** their sales chain, bringing tremendous value to all financial institutions involved.

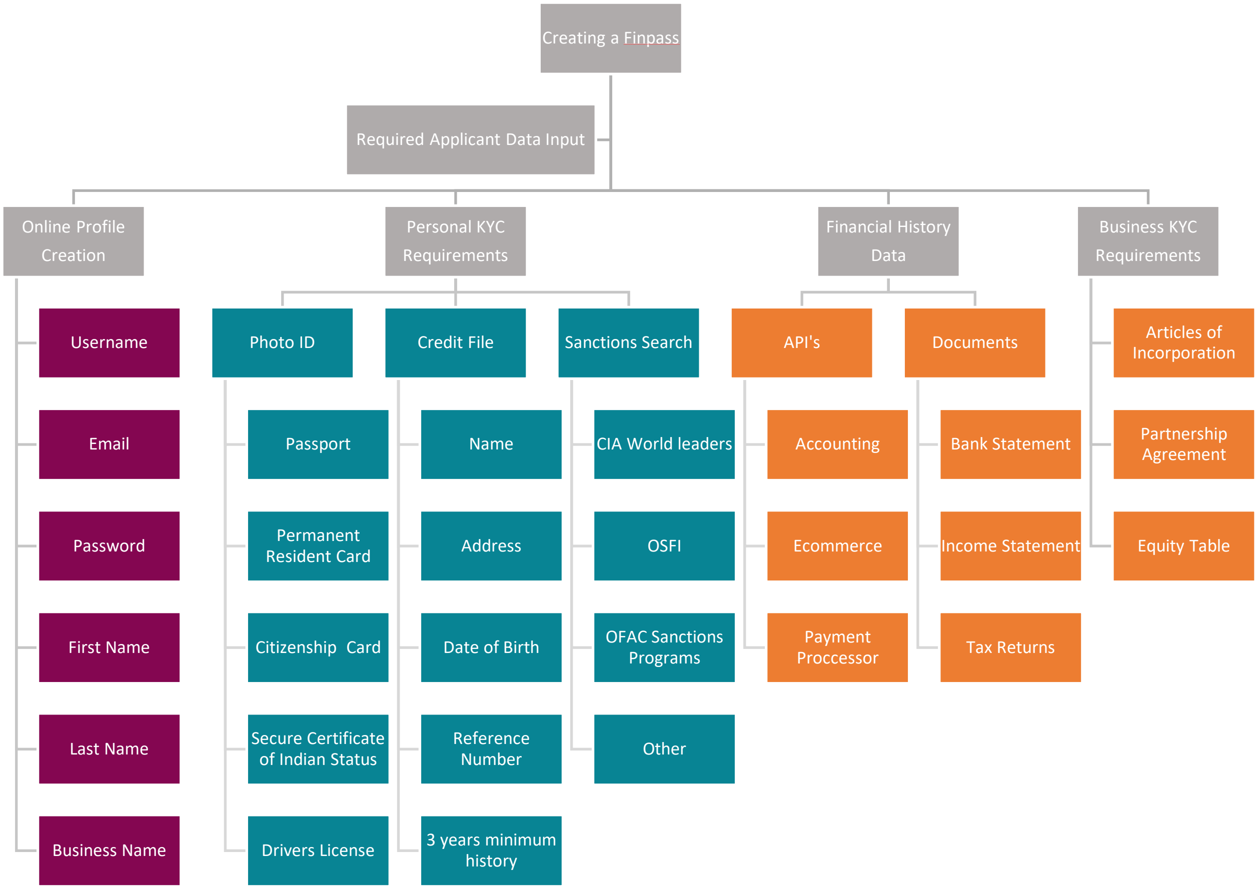
The passport is broken down into two core competencies, representing the different data sets that a business or consumer may need to provide when looking for banking products (credit/bank accounts etc.):

1) verification that the customer presenting the passport has been KYC/AML verified
2) credit adjudication of either the customer or business.

Exhibit 4 shows the entire data contents needed for a complete FINPASS. The below diagram lists the following:

- Web based Customer Profile, onboarded then accessed from the FINPASS website
- The KYC requirements
- Credit Adjudication data that is needed, split into two parts
    - Business scoring
    - Personal scoring

EXHIBIT 4 – FINPASS DATA COMPONENTS



Using the data inputs from these different categories, the results that are generated are as follows:

- Pass/Fail (KYC/AML)
  - Details if the KYC/AML has been obtained and met government set standards
- Credit score (credit bureaus)
- Commercial loan credit limit
  - Value under x for instant approval
- Image of the business owner
  - for in person verification the account does belong to this person
- ID Key

This paper will now discuss in further detail how the FINPASS works in terms of the customer profile, the verification requirements, and the personal and commercial credit adjudication techniques.

Verification & FINPASS - Why the Blockchain is the Most Secure and Universally Trusted Means of Verification Today

The fundamental process of applying for and being approved to receive credit or other banking products relies on the financial institution's ability to establish a clear and concise understanding of the individual or business. The identity must be verified, and so too must the fact that the financial product will not be used for illegitimate purposes (money laundering, criminal activity, terrorist financing etc.).

The Financial Passport therefore needs to verify and attest that the passport carrier is exactly who they claim to be, and that the regulatory guidelines for customer identification have been followed, in accordance with the governance of financial institutions. The process is successful when the basics of the KYC/AML regulations are met, resulting in a highly effective system of fraud prevention.

Governments, and private companies like credit bureaus, currently hold most of the identity data in the world. These organizations play a critical role in the customer identity and credit-worthiness checks on which financial institutions rely. Their role in the financial world has not diminished and will continue to be of value to both the passport holder, as well as to financial institutions. By accessing government sources like database searches and corporate registries, the Financial Passport will hold the necessary customer identity information and individual credit scores, to deliver further value to the financial institution, with the added benefit of a secure blockchain network.

The initial customer identification and verification procedures will be completed by the parent company Sqirl. During the signup process for the Financial Passport, a customer is asked to provide the necessary documentation to allow Sqirl to satisfy the KYC/AML concerns. Once verified, the customer is awarded the Financial Passport that will hold this information.

Blockchain and Digital Ledgers Explained

"The blockchain is an **incorruptible** digital ledger of transactions that can be programmed to record not just financial transactions but virtually everything of value." [ix] At its root, a blockchain is a growing list of records/transactions, called blocks, which are chained together and secured using cryptography, hence the name blockchain.

To understand the blockchain's specific verification advantages, and more importantly, the FINPASS and its underlying technology advantage in the financial market, we must understand the basics of what a digital ledger is, and how a digital ledger is different from blockchain.

A digital ledger, also called 'distributed ledger technology', replicates, shares and synchronizes digital data, that is then distributed across multiple computers. A blockchain based distributed platform is only one type of distributed ledger technology. Simply, all blockchain based distributed platforms are distributed ledgers, but not all distributed ledgers are blockchain based.

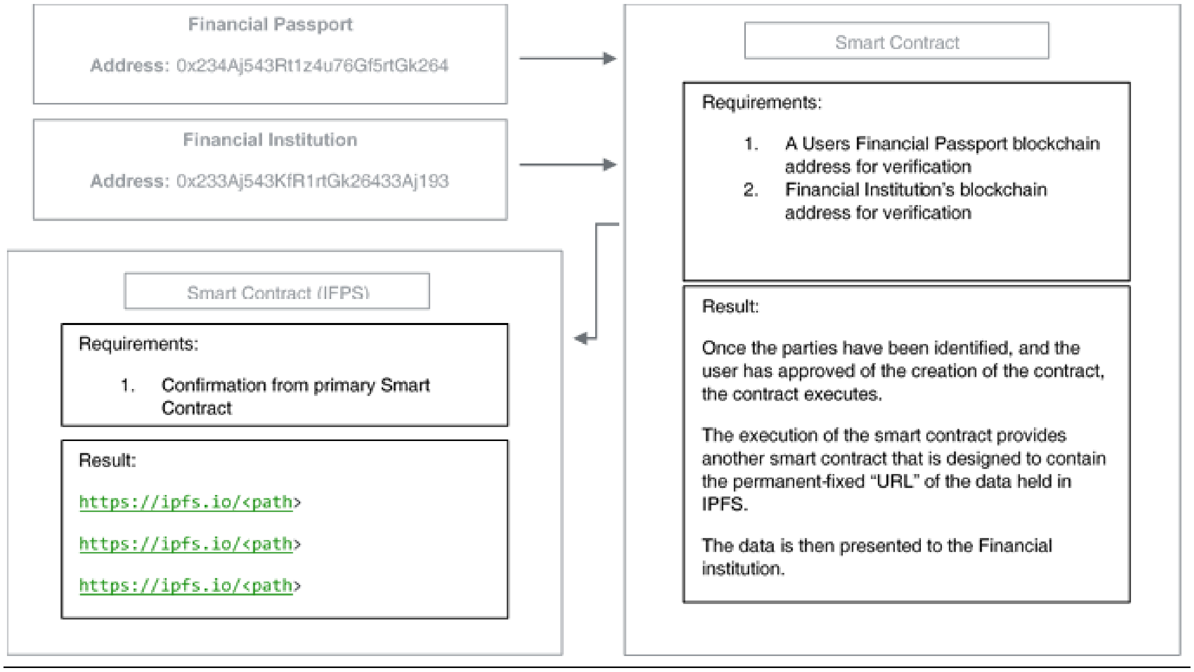
There are many types of blockchain based distributed platforms, like Komodo, Iota's Tangle and Ethereum. Ethereum was created as a peer-to-peer system used to keep track of state changes to a decentralized database. [x] Ethereum also has a growing list of blocks tracking activity, but instead of transactions, each block contains a set of state changes managed by Smart Contracts.

Smart Contracts & FINPASS

Managing these state changes are what we value with FINPASS. Smart Contracts, like those used by Ethereum, are made to facilitate, verify or enforce the negotiation or performance of a contract. Since the Smart Contracts can be written by Sqirl's engineers, choosing the conditions of the contracts makes it easy to record the digital delivery of verified data. [xi]

The primary objective of the Smart Contract for FINPASS is to facilitate the transfer of data between a passport-carrying customer and the financial institution or 3rd party requesting the data. The Smart Contracts are automatically generated and provided to the financial institution when an applicant enters a branch or utilizes online facilities.

EXHIBIT 5 – SMART CONTRACT CREATION PROCESS



Financial Passport
Address: 0x234Aj543Rt1z4u76Gf5rtGk264
Financial Institution
Address: 0x233Aj543KfR1rtGk26433Aj193
Smart Contract
Smart Contract (IFPS)

Requirements:

1. A Users Financial Passport blockchain address for verification
2. Financial Institution's blockchain address for verification

Result:

Once the parties have been identified, and the user has approved of the creation of the contract, the contract executes.

The execution of the smart contract provides another smart contract that is designed to contain the permanent-fixed "URL" of the data held in IPFS.

The data is then presented to the Financial institution.

Requirements:

1. Confirmation from primary Smart Contract

Result:

https://ipfs.io/<path>

https://ipfs.io/<path>

https://ipfs.io/<path>

Smart Contracts can:

- Function as 'multi-signature' accounts, requiring two party consent for a transaction to take place
- Manage agreements between users—for example, if one buys insurance from the other the Smart Contract system helps facilitate the process
- Provide useful information to other contracts (like how a software library works)
- Store information about an application, such as domain registration information or membership records.

The Smart Contract can be auto generated within a mobile application, a web-front end or pre-authorized and sent as a "invitation" to transact based on the data.

"Incorruptible" Verification

What makes the blockchain "incorruptible" is the proof of work concept on a distributed network of nodes. [xii] The blockchain's security is derived from a proof of work problem. A proof of work is a piece of data which is difficult (costly, time-consuming) to produce, but easy for others to verify. It relies on two major pillars:

- consensus
- distribution

If a user wants to alter the blockchain, they must produce a "proof of work". This framework is designed to take a large amount of computational power to access and thus, for a single person, completing it may take years. But it may only take minutes for a network of computers, making it impossible to produce fraudulent data. "Proofs of work that are tied to the data of each block are required for the blocks to be accepted. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes." Thus, the chain can be continually added to, and transactions are still processed in a timely manner while securing the data from tampering. [xiii]

a. Consensus

The nature of this problem makes it mathematically impossible for someone to change the blockchain. "Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain." Changing the block could theoretically be done given enough time, but the formerly mentioned public ledger is chosen by consensus, where the network of users agrees that the longest blockchain will be the recognized chain. This makes up the first pillar of the blockchain. As other systems on the network only recognize the longest blockchain, the only way for a user to successfully alter the chain would be to alter a block and then generate subsequent transaction blocks to make a new, longer chain. However, the usage of a proof-of-work problem makes this mathematically impossible, because the network of users will be adding blocks at a much faster rate than any single person could. Thus, the security lies in the nature of the protocol, which prevents malicious parties from doing harm without having to authenticate a transaction.

b. Distribution

Finally, the ledger is distributed across all network nodes, meaning that every user stores the current ledger, preventing someone from altering a single point of truth. In traditional cryptography, a single point of truth could be a certificate authority. However, if that certificate authority was to be breached, an attacker could replace the stored keys with their own keys, thus enabling them to masquerade as a plethora of users. Furthermore, there are security measures in place to prevent the "address/key" from being stolen. The key on its own **is useless** as the **transaction has to be created before the key**

becomes "active". Thieves would need to steal more than someone's key to obtain access to vital information.

Additionally, due to the distributed nature of the ledger, an attacker would have to breach every member node and replace the blockchain with their own block, making it functionally impossible for the attacker to alter the chain.

By distributing a ledger among all members of the network, blockchain authentication eliminates the possibility that someone will alter the ledger. Every time a 'transaction' or block of data is added to the chain, a majority of the network must verify its validity. This guarantees the integrity of the ledger. One could then use public key encryption, such as the extremely secure RSA encryption, to send their credentials. The recipient could then verify this against an entry in the immutable blockchain, resulting in an incredibly secure and reliable way to handle verification of identity.

The CIA Triad – Blockchain, Cybersecurity and FINPASS

Confidentiality, Integrity and Availability (CIA) are three key principles that are guaranteed with FINPASS and the blockchain.

a. Confidentiality

According to the National Institute of Standards and Technology (NIST), confidentiality refers to "the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes"[xiv]

Today, if an attacker gains access to a blockchain network, this does not necessarily mean the attacker can read or retrieve sensitive information. Due to the use of a public/private key, and the full encryption of the data blocks transacted, the blockchain effectively guarantees its confidentiality.

It is important to note that keys are used for several purposes in the blockchain ecosystem: protection of user information, confidentiality of data, and authentication and authorization to the network.

b. Integrity

Integrity is defined as the "guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity" according to NIST. [xv]

Maintaining data consistency, and guaranteeing integrity, during its entire life cycle is crucial in information systems. Data encryption, hash comparison (data digesting), or the use of digital signing, are some examples of how system owners can assure the integrity of the data, regardless of the stage it is in, whether it be in transit, at rest or in use storage. Blockchain's built in characteristics, immutability and traceability, already provide organizations with a means to ensure data integrity.

As mentioned, FINPASS leverages Ethereum's Smart Contracts. This type of program can be used to facilitate, verify, or enforce rules between parties, allowing for straight through processing and interactions with other Smart Contracts.

c. Availability

NIST defines availability as "ensuring timely and reliable access to and use of information"[xvi]

Cyberattacks attempting to impact the availability of cyber services continue to increase. Denial of service attacks, or DDoSs for short, being one of the most common type of attacks, can cause disruption to internet services and hence blockchain enabled solutions. The resulting implications are that websites get disrupted, mobile apps become unresponsive, and this can generate ever increasing losses, and costs, to businesses.

Blockchains have no single point of failure, which highly decreases the chances of an IP-based DDoS attack disrupting the normal operation. If a node is taken down, data is still accessible via other nodes within the network, since all of them maintain a full copy of the ledger at all times. The distributed nature of the technology solves the problem of false consensus.[xvii]

The combination of the peer to peer nature and the number of nodes within the network, operating in a distributed and 24/7 manner, make the platform operationally resilient. Given that both public and private blockchain consists of multiple nodes, organizations can make a node under attack redundant and continue to operate as business as usual. So, even if a major part of the blockchain network is under attack, it will continue to operate due to the distributed nature of the technology.

Credit Adjudication & FINPASS Profile

FINPASS is designed to run credit scoring on both the individual FINPASS holder and the individual's business, if they have one, through the FINPASS 'network'. 'Network' in this context represents the FINPASS and the Sqirl technology that helps make it run. FINPASS allows Sqirl to be always connected to the user's financial data, so when a bank needs to update their financial information, it is as easy as a simple click of a button to obtain the data needed.

Specifically, the Financial Passport has been designed to include the reporting and tracking of current and historical debt obligations, as well as the associated risk scoring that has been completed, and continues to be updated as the passport holder interacts with the FINPASS network.

The goal of the network is to fairly and securely track the use of, and contribution to, the data that the Financial Passport holds.

Ultimately, the Financial Passport is designed to bring the wealth of pre-existing data and comprehensive credit history, and associated credit scoring to the blockchain.

The FINPASS Customer Profile

The Financial Passport operates as a primary data source that will include the customer's relevant information (business/individual) and will enable financial institutions to quickly and efficiently create a customer file, onboard accurate credit scoring for both businesses and individuals, and ultimately satisfy their need to complete KYC/AML verification and credit adjudication. The blockchain will ensure that the information provided is accurate and secure.

By distributing a ledger among all members of the network, blockchain authentication eliminates the possibility that someone could alter the ledger. Every time a 'transaction' or block of data is added to the chain, a majority of the network must verify its validity. This guarantees the integrity of the ledger. One could then use public key encryption, such as the extremely secure RSA encryption, to send their credentials. The recipient could then verify this against an entry in the immutable blockchain, resulting in an incredibly secure and reliable way to handle verification of identity.

Consumer Scoring

Existing data services provided **by credit bureaus** will initially provide the necessary risk categorization of customers when they are applying for personal banking products. The Financial Passport will continue to update and carry forward a history of the credit score provided and allow financial institutions to understand and verify the customer's track-record of credit performance.

The Financial Passport's privacy model puts loan recipients at the center of all transactions involving their private information and credit history. Passport carriers are empowered to view and review their information before it is shared with any company performing a risk assessment.

Business Scoring using 3rd Party APIs

Sqirl makes use of 3rd-party application program interfaces (API's) that gather the financial data from multiple software solutions. Each API provides us with the applicant's financial data, which is consumed by the analysis engine. Below is a non-exhaustive list of 3rd-party data providers from whom the Sqirl engine can collect data.

- **eBay**
- **Xero**
- **Shopify**
- **Amazon**
- **Square**
- **PayPal**
- **QuickBooks**
- **Experian**
- **FreshBooks**
- **Facebook**
- **Etsy**
- **Stripe**
- **Equifax**
- **TransUnion Canada**
- **Certn**

If multiple sources are available, the applicant may choose to connect them, which would allow the system to run the algorithm against each of the data sets and average out the results.

We also incorporate optical character recognition (OCR) for quick reading of documentation like business plans, T4 notice of assessments, credit rating reports and anything else that may need to be scanned and read automatically, and that will help with the adjudication of the businesses credit worthiness.

Calculating Credit Worthiness

The Sqirl score for commercial loan adjudication takes far more variables related to the predictive performance of a business into consideration than current financial adjudication protocols today. A probability of default (PD) might be based on a single set of parameters, whereas the Sqirl Score is an amalgamation of financial performance analytics, predictive models and time-tested ratio analysis.

Depending on the methodology, you can compare the Sqirl score to your own, internally generated probability of default.

The Sqirl Score continues to learn over time. As the system interacts with live market data, and ongoing applications – the performance of the score and loans adjudicated are constantly monitored and adjusted, to ensure the Sqirl Score is as accurate as possible

The Chartered Financial Analysis curriculum is used to further and continually analyze a business's financial performance and its relative strength to afford new debt.

The following areas are taken into consideration when Sqirl evaluates the credit worthiness of a business:

Quantitative Methods

This topic area is dominated by statistics: the topics are broad, covering probability theory, hypothesis testing, (multi-variate) regression, and time-series analysis. Other topics include time value of money—incorporating basic valuation and yield and return calculations—portfolio-related calculations, and technical analysis.

Financial reporting and analysis

This includes analyzing financial reporting topics (International Financial Reporting Standards and U.S. Generally Accepted Accounting Principles), and ratio and financial statement analysis.

Financial Ratios – Business

Business risk is defined as the risk related to a company's income variance, the possibility that the company might make less money through a decrease in sales, or worse, the company starts to lose money. It is important to assess the business risk to further determine whether any debt or loans could be at risk if the company were to start making less money.

Industry Analysis

Understanding a business's financial performance relative to the companies in the same industry can provide an excellent indication of the company's financial health. The ability to take on new debt, and ultimately repay it in a timely fashion is heavily reliant on a company's historical financial performance. The industry related risk and credit scoring are considered when deciding on a company's credit worthiness.

5. TECHNOLOGY ROADMAP

The purpose of the technology roadmap is to indicate major milestones for Sqirl's development team to achieve for the successful release of the Financial Passport.

Phase 1: KYC/AML Individuals (Complete)
Identification of the necessary measures to have in place for document capturing and storage when determining a customer's identity and their completion of governance for KYC/AML.

Implementation of business processes and technology to aid in the data verification and establishment of an individual's identity.

Phase 2: KYC/AML Businesses (Complete)
Identification of the necessary measures to have in place for document capturing and storage when determining a business customer's corporate identity and their completion of governance for KYC/AML.

Implementation of business processes and technology to aid in the data verification and establishment of an individual's identity.

Phase 3: Individual Creditworthiness Assessment (Complete)
Established data partnership with a credit bureau to provide credit scoring of individuals to be included in the Financial Passport.

Complete the technological requirements of implementing an automated connection and receipt of credit files, and reports from the credit bureau.

Phase 4: Commercial Creditworthiness Assessment (Complete)
Identify the 3rd party software solutions that offer API's for the collection of financial performance data of a business.

Implement the use of a credit scoring and decisioning engine to determine the creditworthiness of a business utilizing the data sources available.

Continue the optimization of the risk categorization and determination score using a regression-based machine learning algorithm.

Phase 5: Blockchain Delivery Network (Complete)
Smart Contracts and the Ethereum Network will be utilized to create and finalize the functioning processes of the Financial Passport.

The network will be responsible for the issuing of the Financial Passport keys, as well as the delivery mechanism of the Financial Passport to the financial institutions. The network will include the ability for data providers to contribute to the Financial Passport.

Phase 6: Data Partners and Modeling

With an increase to different data partners and data sources, additional types of modelling can be added to the Financial Passport. As an example: social profile scoring (Facebook, LinkedIn, Twitter) can be utilized in consumer credit adjudication.

6. TEAM

Founding Team

Kyle Boyko

A lover of all things innovative, Kyle has had a seasoned career in strategy and technology.

Kyle worked at the C.D. Howe Institute, a macro-economic and banking research facility, or ‘think-tank’, that is widely viewed as Canada’s premier institution for economic policy opinion.

Kyle also worked as a strategist in a management consultant role for the Swedish Trade Council, an extension of the Swedish Consulate, participating multiple high-profile strategy assignments for fortune 500 companies and SME’s.

While Kyle was working with small businesses, he noticed the out dated underwriting practices used for small business lending. In his view, the solution would come from a technology enabled overhaul of underwriting processes used by F/I’s. The solution Kyle and Andre conceived is Sqirl, a technology that helps people interact and obtain banking products with ease.

A veteran of the start-up world, Kyle has been part of 2 other startups — one of which sold in the retail hologram technology world.

He is currently authoring a 3-part series in finance and financial technology.

Andre-Ivor Wills

An avid technology enthusiast and full stack developer, Andre-Ivor Wills started his educational and professional career in South Africa, before being selected as a Fellowship Winner at the Ryerson DMZ business incubator in 2014, which saw him come to Canada and continue his career as an entrepreneur.

Andre-Ivor has been responsible for the design and construct of the Sqirl the technology that powers the current business solutions. Prior to this, he built and maintained a marketing intelligence platform for Africa’s largest Fixed-Line Telecommunications Provider – a system still in use today.

Andre-Ivor started his IT career, working for a company that specialized in Debt Collection Management. He was responsible for maintaining and improving the software that clients would interact with when building new Debt payment schedules.

Advisors

Robert French

Robert is a seasoned developer who has been programming applications for just over three decades.

He spends his evenings as a Professor in video game development in Toronto at Trios College where he has an impressive 85% employment rate for his graduates (in the field) over the last 8 years. He also alternates between teaching cyber security at Fleming College in beautiful Peterborough, Ontario where he resides and video game design at Humber College's north campus.

Vitaly Kontishev

A visionary senior executive with verifiable year-after-year success achieving revenue, profit, and business growth objectives in start-up, turnaround, and rapid-change environments.

A corporate leader executing multi-million-dollar international strategic business development deals. Offers over 20 years of business development acumen, leadership an operational expertise. Individually selected by the Mayor of Penza, Russia as a Chief Economic Advisor since 2005.

A published scientist with 18 patents and 20+ years expertise in the machine vision and robotics industry developing and testing products for military and private use. With one Ph.D. and three Master's degrees to his name, Vitaly is a former Assistant Professor of Mathematics, Simulation and Artificial intelligence with an emphasis on machine vision and robotics.

7. References

[i] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[ii] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[iii] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[iv] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[v] https://mapr.com/blog/top-10- big-data- trends-2016- financial-services/

[vi] http://www.gartner.com/newsroom/id/3303517

[vii] http://dictionary.reverso.net/english-definition/digital%20delivery

[viii] http://www.gartner.com/newsroom/id/3303517

[ix] Don & Alex Tapscott, authors Blockchain Revolution (2016)

[x] https://hackernoon.com/what-on-earth-is-a-smart-contract-2c82e5d89d26

[xi] https://cointelegraph.com/explained/smart-contracts-explained

[xii] http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf

[xiii] http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf

[xiv] http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[xv] http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[xvi] http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[xvii] https://ice3x.co.za/byzantine-generals-problem/

https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

https://themerkle.com/distributed-ledger-technology-vs-blockchain-technology/

https://blockgeeks.com/guides/smart-contracts/

https://www.cnbc.com/2015/05/05/credit-invisible-26-million-have-no-credit-score.html

https://bitsonblocks.net/2017/02/20/whats-the-difference-between-a-distributed-ledger-and-a-blockchain/

https://bitsonblocks.net/2017/01/09/distributed-ledgers-shared-control-not-shared-data/

https://globenewswire.com/news-release/2018/01/29/1313374/0/en/Evernym-and-R3-partner-to-apply-self-sovereign-identity-to-financial-services.html

https://www.r3.com/research/

https://medium.com/startup-grind/gentle-intro-to-blockchain-and-smart-contracts-part-1-3328afca62ab

https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

https://hackernoon.com/what-on-earth-is-a-smart-contract-2c82e5d89d26

https://kyc-chain.com/

https://www.coindesk.com/information/ethereum-smart-contracts-work/

https://www.lexisnexis.com/risk/downloads/whitepaper/anti-money-laundering-risk-assessment-and-customer-due-diligence-study.pdf

http://www.jstor.org/stable/3666266?seq=1#page_scan_tab_contents

http://amj.aom.org/content/40/5/1063.short

https://muse.jhu.edu/article/209037/summary

http://www.sciencedirect.com/science/article/pii/S0378426697000101

https://www.central1.com/about-us/credit-union-system

https://cba.ca/Assets/CBA/Files/Article%20Category/PDF/bkg_consumers_en.pdf

https://www.cba.ca/Assets/CBA/Files/Article%20Category/PDF/bkg_technology_en.pdf