Open Finance Network

Trading Real Assets on Blockchain

WHITE PAPER

Contents

Abstract 4

Background 5

Industry Overview 5

Alternative Assets 8

Product Description 11

Decentralized Securities Depository 12

Global Entity & Asset Registry 14

Decentralized Securities Depository 14

Investor Passport 14

Use Cases 15

Tokenized Trading 18

Securities Token Protocol and Issuance 18

Securities Token Trading 19

Decentralized “Street Name” Trading 19

Distributed Ledger Book Entry 20

Network Benefits 21

Technical Framework 23

Smart Contracts 23

Network Token 23

Network Adaptors 24

Zero-Knowledge Proving System 25

Team and Advisors 27

Development Team 27

Investors and Advisors 28

Conclusion 30

Appendix A: Industrial Zero-Knowledge Proving System 31

Zero-Knowledge Arguments of Knowledge 31

Proving System Architecture 34

System Roadmap 36

ABSTRACT

The emergence of Bitcoin and its associated ecosystem of blockchains and alt-coins have been widely recognized as a generational disruptive force in the financial services industry. Equally disruptive is the underlying technology behind Bitcoin, commonly referred to as blockchain or distributed ledger technology, which has greater potential applications beyond just electronic currency. In particular, within financial markets, there is a wide range of benefits of blockchain technology in the securities trading, clearing & settlement process.

Modern financial markets are saddled with an antiquated clearing & settlement process that is often slow and cumbersome, and include multiple intermediaries and redundant data sets that need to be manually reconciled on a repeated basis to complete a single transaction. The core strengths of blockchain (shared ledger, immutability and security) bring the promise of reduced transaction costs and streamlined processes to the industry, which benefits both financial institutions and individual investors alike.

In the direct participation program (DPP) market, comprised of assets such as non-listed REITs, business development companies (BDCs), Regulation A+, Regulation CF and other crowdfunded assets, the inefficiencies and problems of an antiquated clearing and settlement process are even more pronounced. The lack of a standardized process and interoperability lead to a lengthy settlement process that averages 6-8 weeks to complete, an absurd amount of time by any measure. As more and more investors enter the DPP market (led by a revitalized interest in the alternatives sector) a more robust model must be put in place in order to meet the needs of its core customer base.

OpenFinance Network, the leading trading platform in the $7.7T alternative asset market, has developed a framework to transform the trading, clearing & settlement process in the industry, leveraging distributed ledger technology to bring efficiency, transparency, and interoperability to a fragmented market. The framework contains a uniform protocol to provide standardization of assets and data within the industry. Moreover, this interoperability also applies between “traditional” alternative assets and the emerging “crypto” alternative asset class, creating a mechanism of tokenized trading to bridge the gap between off-chain and on-chain capital markets.

BACKGROUND

INDUSTRY OVERVIEW

Today's global financial markets were shaped over decades of interactions between various participants and stakeholders in the industry. Markets are comprised of complex networks of internal systems and service providers that support the processing of hundreds of millions of financial transactions each day. This mix of internal and external systems was not created through intentional architecture and design, but through a painstaking integration process that resulted in the current flow of assets, information and data across markets and regions. While not perfect, the current construct is a finely practiced dance between market participants that creates the public financial markets as we know them today.

The act of “trading” itself is very simple. At the most basic level, an individual exchanges an item of value and receives payment in return from another individual party. This action can be performed face-to-face, in real-time, with no intermediaries or other parties present. This is basically how trading was first conducted in the early days of stock exchanges. In this example, the trading and clearing & settlement occur bilaterally and at the same time. However, as the number of financial markets grew and became more complex, so too did the process of trading. As more people accumulated diverse assets, the need arose for trusted third party authorities to securely hold and manage those assets on their behalf, as well as for service providers to manage the trade processing. Over time, as more people participated in these markets, the need for investor protection from service provider fraud or unexpected financial crises led to the development of industry governance and regulation to oversee and police the processing of financial market transactions. The end result is a layered interaction of complexity and redundancy that exists today, with multiple intermediaries and redundant data sets that need to be manually reconciled on a repeated basis in order to complete a full lifecycle in a single securities transaction.

The typical securities transaction lifecycle (STL) starts with a trade initiated from an investor, either a buyer or a seller. Their broker sends the transaction to an exchange for processing, where it is matched with a corresponding counterparty. The exchange then sends this matched transaction to a central counterparty clearinghouse (CCP), where it is reconciled with the brokers to reduce default and counterparty risk. From there, the transaction is sent to settlement, where the investor’s custodians (who hold the assets and funds) work via the central securities depository (CSD) to ensure that assets and funds are transferred from one source to another. Finally, the transaction data is sent to the registrar or transfer agent of the underlying issuer in order to update their shareholder list and information.

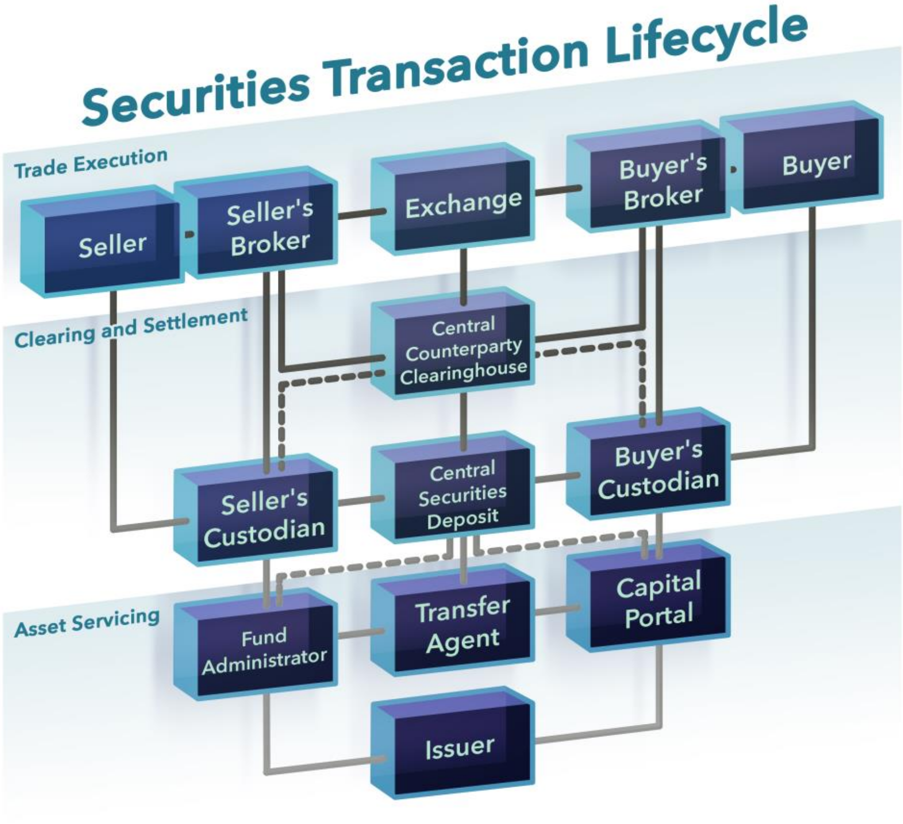


FIGURE 1 - SECURITIES TRANSACTION LIFECYCLE

Of note in this STL model are the key (central) roles that CSDs and CCPs play towards a fluid market. Generally grouped within the area of "clearing & settlement", these entities provide a coordination mechanism that is the foundation for the common framework utilized by all participants. The CSD serves as the "golden source" for shareholder ownership, while the CCPs reduce counterparty risk for buyers and sellers, keeping all participants "honest" and trusted.

The benefits of this STL model are evident: standardization of assets, interoperability between multiple participants, reduced counterparty risk, and ensured transactions verified by trusted sources. There are detriments to this type of model however, including the massive scale needed for the viability of this type of STL model (with a network of centralized industry-owned trusted entities), the cost and difficulty for smaller players to gain access to this network, the redundant repeated data stored across multiple intermediaries, and legacy systems that add complexity and inefficiency to the system.

> “The execution processes for trades includes multiple intermediaries, each which maintains its own ledger of data. While central intermediaries maintain aggregated records, the parties’ ledgers can differ quite substantially. **Therefore, no single institution has a master record of all executed transactions.”**
>
> **- Moody’s**

Given that these inefficiencies are estimated to cost the industry $80B annually, it’s no surprise that many industry participants are exploring blockchain initiatives, particularly as high compliance costs and low interest rates have kept pressure on returns for these firms. Some of the benefits that can be accomplished with distributed ledger technology are:

- Improve operational efficiency
- Increased transparency
- Simplified regulatory oversight and reporting
- Improved security
- Removal of counterparty risk
- Reduced settlement times

Concerning regulatory review and acceptance, the CFTC and Moody’s have both been outspoken about the substantial potential in applying the technology into recording trading counterparties and AML/KYC processes, going so far as to saying it may have prevented recent financial scandals and the resulting market crashes. Commissioner J. Cristopher Giancarlo has endorsed a “sandbox regulation” type regulatory model and “do no harm” approach to blockchain technology. Blockchain is thus being explored as the solution for intermediary transformation in fixing its necessary practical legal characteristics (loss of carrier, pooling and mirroring), latency issues (response times, sequenced approval process), capital markets & securities servicing limitations, solving less efficient netting & clearing and collateral management, regulatory issues (AML & KYC compliance) including interoperability with audits, and for database inefficiencies (ensuring consistency of information, security, access, utility).

The promise of blockchain technology to reduce back-office costs by eliminating various reconciliation processes and reducing capital tied up in the settlement cycle has prompted many incumbent financial institutions to actively assess its potential to improve efficiencies. At the same time, many institutions are concerned that their role in a blockchain-enabled post-trade life cycle could be significantly reduced (if not made obsolete) and may delay internal adoption, which in turn leads to lack of adoption in the industry, to the detriment of the investment community as a whole.

ALTERNATIVE ASSETS

Alternative assets are broadly defined as investment vehicles that exist outside the traditional asset space of public equities, bonds and cash. The global market size for alternative assets totals $7.7 trillion as of 2017. The asset class primarily acts as a diversifier but is also a potential source of inflation protection, income, and capital appreciation. Alternative assets can include exposure to private equity and debt, real assets, limited partnerships, hedge funds, mutual funds, ETFs, fund of funds, and emerging sub-segments such as UCITs, online capital assets and cryptocurrency assets.

While traditional assets and public listed securities benefit from greater liquidity, they are by no means superior to alternative assets in terms of returns, income, inflation protection or capital appreciation. In the past few decades these key attributes have shifted allocations away from the traditional towards alternative assets, revitalizing interest in the alternatives sector via accommodative regulation and reform, and ultimately amplifying the opportunities for both alternative assets and the infrastructure surrounding them. The market for alternative assets is booming and the case for investment into them featuring fundamental liquidity is no longer a non-sequitur for the retail investor. The table for alternative investments has turned; the asset no longer embodies crowd listlessness and high-towered goliaths but instead a ripe, crowd funded vehicle for opportunity and innovation.

Spearheaded by their collective resilience - overlooking bubbled real estate - during the global financial crisis, alternative assets in the United States have entered the spotlight this past decade. In the years between 2005 and 2007 alternative assets AUM nearly doubled from $2.9 trillion to $5.7 trillion, and during the crisis select assets took a hit due primarily to illiquidity stunted by scandals and poor performance, otherwise caused by both systematic and systemic risks. However, by year-end 2011 this AUM had rebounded to $6.5 trillion (14% compounded annual growth rate) with revitalized health and momentum.

Amid signals of a deregulatory phase in the “regulatory cycle” the momentum has been driven in part by innovative syndication mechanisms such as with the emergence of crowdfunding – the child of the Jumpstart Our Business Startups Act (the “JOBs” Act) – and more recently, the popularized Initial Coin Offerings (ICOs), including both security tokens and utility tokens. Concurrently the advents of securitization alongside smarter derivatives pricing mechanisms such as X-Value Adjustment have reinforced adoption. Together this environment has been coined the democratization of capitalism but is in fact a showcase of the intrinsic maturing of both investors and policy as it relates to the alternative assets class.

Today a wide-spectrum of new investment opportunities have emerged and grown in market share within the alternative assets space catalyzed by these drivers. Direct participation programs (DPP) including BDCs and public non-listed REITs alone comprise a $90 billion market size in 2017 with an estimated “online capital” assets market – consisting of Tier 1 and Tier II Regulation A+ crowdfunded offerings - estimated to be an additional $34 billion. Others include Regulation D 506(c) & Regulation CF, managed futures, LPs and liquid alternatives / ETF securities. The rise of the ICO in 2017 as a viable mechanism for capital raising from a broader audience has created a new asset class that challenges the construct of traditional financial markets.

In 2017 the divergence between all-time low interest rates and all-time high (priced) equity markets emphasized this point – signaling that alternatives today are uniquely attractive. For some early adopters of this market opportunity, like for the endowments of Harvard and Yale, this is no surprise. But for SME's and most retail and institutional investors these advents have only recently come to the forefront as attractive diversified opportunities and fundraising mechanisms. Crowdfunding and ICOs exemplify this opportunity; ICOs have already outpaced venture capital fundraising while on a similar long-term trajectory.

Alternative assets are becoming mainstream – today the market features emerging opportunities by way of strengthened fundamentals and accommodative policies alongside momentum of adoption by way of democratization and attractiveness.

Due to this rapid growth, alternative assets are facing growing pains, especially in the post-trade securities lifecycle. Alternative assets have less efficient netting, clearing, collateral management and clearing periods, causing further issues for trade settlement windows and causing legal considerations such as pooling, mirroring and loss of carriers that present even greater friction points. In many cases, such as with DPP assets, there are no central counterparty clearinghouses or central securities depositories – let alone standardized asset data or a uniform communication protocol. This results in a process characterized by many in the industry as opaque and paper heavy. Despite new technological advances available to the market, many incumbent industry players have been slow to adapt, and the systems remain in fragmented silos of investor data and asset data with limited external access. These legacy systems are saddled with high costs and fees that continue to make the network inaccessible to many. To worsen matters, the DOL fiduciary rule and its "good-faith" requirements of broker-dealers alongside FINRA and IRS enforced reporting methodologies, along with KYC and AML compliance, make due-diligence in this market even more timely and expensive.

On the other end of the spectrum, newer "crypto" securities suffer from the lack of a defined compliant transfer process. Confined to a regulatory framework that has not been able to keep up with the rapidly evolving state of distributed ledger technology, crypto security holders are faced with uncertainty on issues of asset custody, ownership transfer and financial reporting.

As a result of the lack of standardization and interoperability, investors cannot manage their entire portfolio in one location nor have their traditional equity positions alongside their alternative asset positions. They are further encumbered by having to duplicate the same information and documentation across multiple service providers, and in turn receive vastly different reports, documents and methods of distributions. Issuers also suffer from this lack of standardization and connectivity as they can only target the small subset of the market that is available to them via their preferred service provider. Service providers can only reach a limited audience given the lack of connectivity in the industry.

In summary, the securities transaction lifecycle in alternative assets is inefficient - lacking interconnectivity, interoperability and protocol. The existing marketplace is fragmented, expensive and archaic. While artificial frictions cause layers of distribution tolls and fees, siloed fragmentation of data results in the lack of a single satiation point to enable fundamental market efficiency for the trifecta of participation, adoption and investment driving momentum to the market today.

Prior efforts at solving this problem have faced cost-prohibition and a lack of adoption. This is because high fees and fragmented data, amid non-existent competition, plays into the interests of certain parties. One failed example was conceptualized by Prodigious LLC, as explained in their whitepaper on the subject exploring the vast benefits of such a system. Cost effectiveness is important because unlike with traditional assets whose sponsors and investors include large institutions and banks, the alternative assets marketplace is dominated by smaller shops such as broker-dealers and RIAs who do not have the operational capacity nor leverage to accommodate these systems. A low-cost, friction-less solution is needed for the industry to provide the benefits of a large-scale mature securities transaction lifecycle as seen in public markets (including clearing & settlement), while side-stepping the pitfalls and prohibitive costs of legacy system that exist today.

The alternative asset industry has a once-in-a-generation opportunity to reimagine and modernize its infrastructure to address long-standing operational challenges. However, there is a need for a driving force with the experience and capabilities to enable the integration of a financial industry distributed ledger framework and protocol with the existing financial market infrastructures in a manner that is consistent with existing regulations and that further lowers risks and costs for all market participants.

PRODUCT DESCRIPTION

The clearing & settlement process today in the alternatives asset industry is slow and cumbersome, with multiple intermediaries and redundant data sets that need to be manually reconciled on a repeated basis to complete a single transaction. The lack of standardization and interoperability further hinder this market and hurt the millions of investors who participate in this asset class.

OpenFinance Network, already a trusted player in the alternative asset industry since 2014, is leveraging the advancements in distributed ledger technology to build on its success to date to introduce an "open source" version of its own internal clearing & settlement process. The key innovation enabled by this blockchain-based approach is the creation of a decentralized securities depository mechanism by which data interoperability can be leveraged across the various intermediaries in the industry in a transparent, secure and efficient method. Moreover, this data interoperability also applies between “traditional” alternative assets and the emerging “crypto” alternative asset class.

OFN today works directly with individual investors and financial advisors to transact with the full spectrum of brokers, custodians, issuers, portals and transfer agents in the alternative asset industry. Effectively acting as a self-clearing broker, OFN touches all aspects of the securities transaction lifecycle, and deals with the antiquated clearing & settlement process of the industry; with a lack of standardization, non-interoperability and manual reconciliation across the ledgers of multiple intermediaries and counterparties.

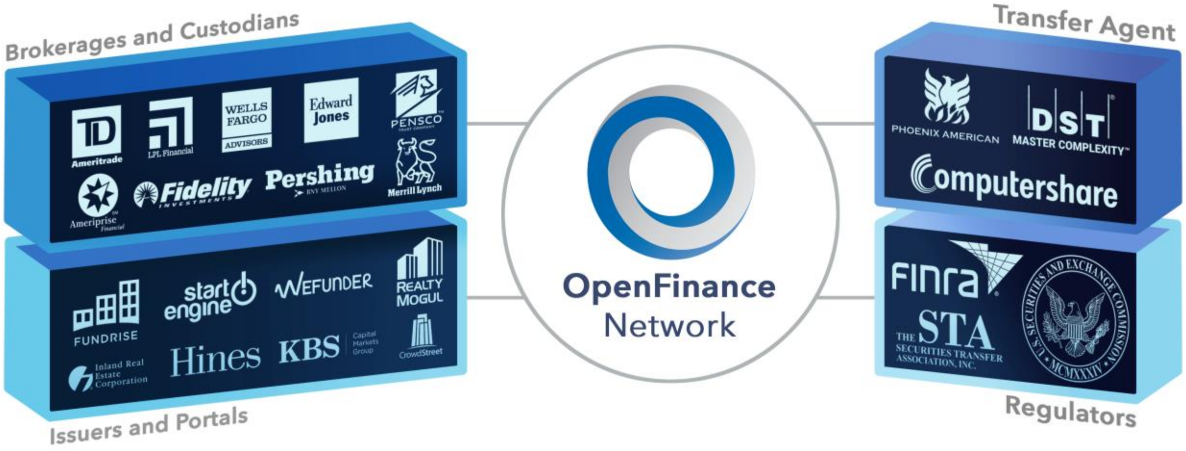


FIGURE 2 - MAP OF MARKET PARTICIPANTS

DECENTRALIZED SECURITIES DEPOSITORY

OpenFinance Network has developed a decentralized securities depository system for the alternative asset industry. The OpenFinance Network (OFN) is a protocol and framework for the processing of securities transactions, initially focused on the clearing & settlement process but intended for the entire securities lifecycle. This provides a common framework and communication protocol by which to standardize alternative assets and provide interoperability between the data silos of market participants. The standardization applies not only to the assets themselves, but also to the reporting and compliance process in the industry. The framework is built with regulatory compliance first and foremost, while bringing the strengths of blockchain to the industry.

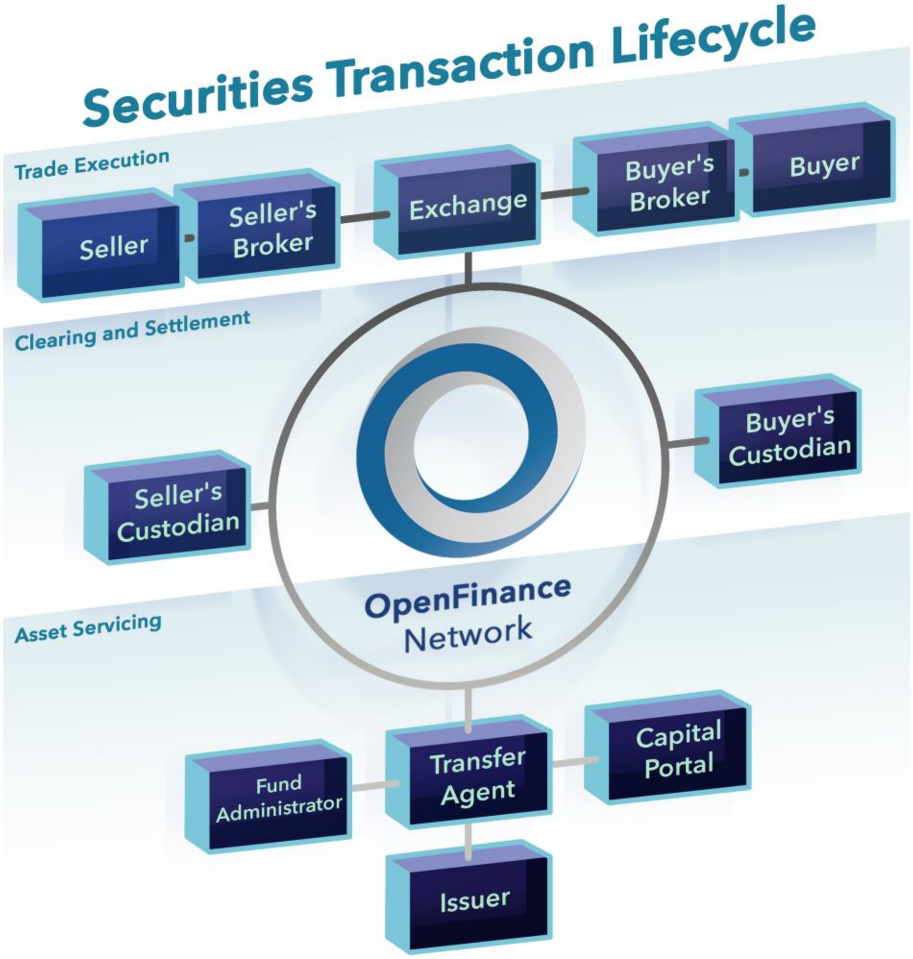


FIGURE 3 - OPENFINANCE NETWORK MAP

The OFN framework replaces the need for central counterparty clearinghouses (CCPs) and central securities depositories (CSDs) in the ecosystem. Rather than relying on manually reconciled ledgers, participants on the marketplace can conduct real-time verifications of asset ownership and fund availability in order to eliminate counterparty risk between parties. Participants can integrate directly onto this framework, or they can interface via network adaptors that are designed to provide off-chain access to the blockchain framework. In order to ensure compliance with regulatory guidelines and investor privacy laws, all sensitive private data is stored on a secure federated sidechain (SFS), which is then hashed back to the public chain to provide immutability to the SFS. A zero-knowledge proving system is utilized to bring full transparency of auditable data to the public without leaking the underlying data. The use of decentralized oracles allow for direct interaction and interoperability to existing back-end systems of market participants while mitigating the risk of single points of failure/fraud.

The framework consists of three main components:

1. A distributed ledger built on the Ethereum consensus mechanism defined by smart contracts at the Asset, Entity, Validators and Transaction level to provide a common protocol for data standardization and interoperability. Sensitive data is stored on a secure federated sidechain, with a zero-knowledge proving system utilized to bring full transparency and accountability to the public.

2. A network token (OFN token), which grants the holder a license to transact on the framework (granting a license to the system). License holders can also be granted additional authorization on the framework based on off-chain verification (e.g. for registered companies such as broker-dealers, custodians, and transfer agents).

3. Network Adaptors (web and software applications) that allow participants to directly interact with the framework off-chain. This will be the main entry point into the system for many of the legacy players in the industry.

The OpenFinance Network is a system that is designed to be used by the primary actors in a securities transaction, including broker-dealers, issuers, transfer agents, clearinghouses, custodians, fund administrators, capital raising portals, and of course, retail investors. Participants can interact directly with the OFN framework, or they can continue to work with their intermediaries who are then integrated within the OFN. Network adaptors allow for these intermediaries to connect and provide direct-to-consumer options for self-directed investors.

Broker-dealers today act as validators in the current off-chain ecosystem; on the OFN these registered entities are granted additional authorization that allow them to verify other individuals, firms and assets on the system. Once verified by a trusted Validator, all other participants can securely interact with this individual, firm, or asset on the system knowing that the broker-dealer has already performed the necessary due diligence required. Other registered entities include transfer agents, custodians, escrow agents, fund administrators and registered funding portals.

The OFN framework is designed to be open to further development and construction on top of the base model. Developers can build custom applications that interface with the network and can authenticate/authorize as needed. Existing service providers will need network adaptors to be able to on-board their assets and client base onto the network. The structure of the OFN network token is also modeled so that industry participants and developers are incentivized to build on top of the open source framework. The token effectively acts as a license to transact on the framework, and can be sub-licensed to others who wish to transact. The token transaction capacity (and frequency) are programmatically determined by the system's token capacity algorithm that adjusts the number of transactions permitted per token based on network traffic, meaning that transaction costs are dynamic and adjustable based on the needs of the network. Market participants, service providers, and developers can thus build on top of the framework and sub-license to others, whether for free or for compensation, to gain access to the broader network. This mechanism is designed to boost market adoption and creates a robust ecosystem through both competition and cooperation amongst third party providers.

The OpenFinance Network began development within the broker-dealer network, and was constructed in-line with securities regulations. The development team gathered input from the broker-dealer community and broader financial intermediary industry for desired functionality and features to be included in the base framework. Some of the key features of the framework include:

GLOBAL ENTITY & ASSET REGISTRY

The OFN system contains a public registry of qualified entities and assets on the distributed ledger. Qualified entities include broker-dealers, transfer agents, custodians, escrow agents, fund administrators and registered funding portals. Asset may also be registered with the SEC/EDGAR and that data can be referenced from the OFN as a subset of the Asset data object (via oracles). Sensitive data is stored on a secure federated sidechain (SFS). Shared asset and transactional data is provided in a standardized protocol format to provide for interoperability amongst market participants.

DECENTRALIZED SECURITIES DEPOSITORY

The global registry of qualified entities and securities creates a mechanism for a decentralized securities depository that provides a public governance model to ensure maximum transparency and protection for investors. The distributed ledger acts as the "golden source" to synchronize (and protect) data across multiple stakeholders in standard securities transactions. This provides a "trustless" clearing & settlement process that is instantly available to all market participants and removes the single points of failure/fraud.

INVESTOR PASSPORT

The global registry and decentralized securities depository allow for the creation of an Investor Passport to verify an investor's AML, KYC, suitability and accreditation verification once with a system Validator, and then utilize that passport with other service providers in the ecosystem. This creates an enhanced, secure, and global compliance process that improves investor protections and security, along with increased privacy of sensitive investor data.

USE CASES

The OpenFinance Network is a system that is designed to be used by the primary participants in a securities transaction, including broker-dealers, issuers, transfer agents, clearinghouses, custodians, fund administrators, capital raising portals, and retail investors.

The user cases below are a subset of possible use cases enabled by the OFN. Note how each use case builds on the use case before it, indicating the layered functionality that can be unlocked as adoption increases within the industry.

INVESTOR VERIFICATIONS

Investors seeking to participate in a securities offering often have to go through various forms of AML, KYC, Suitability and Accreditation verification, depending on the asset class and exemption type. Each time they invest with a new Issuer (or Service Provider), they are asked to submit the same information, even though they may have just been already verified that same day. With the OFN, Investors can instead rely on a Validator to perform the necessary AML, KYC, suitability and accreditation checks once, record the Verification data to the OFN, and then grant access for the Issuer to reference that data in their Investor Passport.

Benefits: Improved investor protection and security, increased privacy of sensitive investor data, enhanced compliance and protection for the issuer

ISSUANCE OF NEW SECURITIES

An Issuer who is seeking to offer new securities typically goes through a burdensome lengthy process to get their offering to market. There is no standardization of assets within the alternatives industry today, and the compliance and regulatory process can be confusing if the issuer is not familiar with securities law. With the OFN, the Issuer can go direct to a Validator (a qualified entity that has authorization to perform this action) to perform the necessary due diligence process to register the asset on the OFN (and other registrars). This mechanism streamlines the compliance, reporting and investment management process. Potential investors can now invest with confidence knowing that the securities are tracked on the OFN and are being real-time audited by a decentralized authority. Investors may also provide their Verification data to participate in the offering via the OFN Investor Passport.

Benefits: Boosted trust + investor confidence, investor protection and security, enhanced compliance and protection for the issuer

ONLINE PORTALS

An Issuer who works with a Portal service provider on the OFN knows that they will receive a standardized and streamlined process for compliance, reporting and investment management. These efficiencies and cost savings can be passed on the Issuer, which can reduce their cost of capital. Potential investors can now invest with confidence knowing that the securities are tracked on the OFN and are being real-time audited by a decentralized authority. Investors may also provide their Verification data to participate in the offering via the OFN Investor Passport.

Benefits: Boosted trust + investor confidence, investor protection and security, increased privacy of sensitive investor data, enhanced compliance and protection for the issuer, lower cost of capital for issuers, increased transparency and reduced fraud in the industry

SECONDARY MARKETS

An Investor who works with a Secondary Market service provider on the OFN knows that they will receive a standardized and streamlined process for compliance, transfer of ownership, escrow, and distribution of proceeds. These efficiencies and cost savings are passed on to the Investor in the form of lower fees. The Secondary Market service provider also works with the transfer agent / registrar, and if that entity is connected to the OFN, they can also query & post data to the OFN. Investors can now transact with confidence knowing that the securities are tracked on the OFN and are being real-time audited by a decentralized authority. Investors may also provide their Verification data to participate in the transfer via the OFN Investor Passport.

Benefits: Boosted trust + investor confidence, investor protection and security, increased privacy of sensitive investor data, enhanced compliance, proper escrow management, lower costs for participants, increased transparency and reduced fraud in the industry

TRANSFER AGENTS / FUND ADMINISTRATORS

Transfer agents / fund administrators who are active on the OFN receive access to a wider base of investors and assets, along with boosted efficiencies, and lower administrative and overhead costs. Issuers, portals and secondary market service providers can interface directly with the transfer agent / fund administrator, and/or communicate solely via the OFN and network adaptors. Full service firms can focus on higher value and revenue generating activities in a full service product suite (reporting, taxes, statements, etc.), and deliver them in a more efficient and cost effective fashion.

Benefits: Investor protection and security, increased privacy of sensitive investor data, enhanced compliance, lower administrative and overhead costs for all participants, access to wider base of investors and assets for client onboarding, increased transparency and reduced fraud in the industry

CUSTODIANS / TRUST COMPANIES

Custodians on the OFN receive access to a wider base of investors and assets, along with boosted efficiencies, and lower administrative and overhead costs. Issuers, portals, transfer agents, fund administrators and secondary market service providers can interface directly with the custodian, and/or communicate solely via the OFN and network adaptors. Custodians can spend less time coordinating data between them, the transfer agent, and the clearinghouse and focus on higher value and revenue generating activities. Further, escrow agents and other service providers can ride on top of the OFN to provide their services to the broader industry for issuers and transactions that need an SEC approved escrow provider or other compliant services.

Benefits: Investor protection and security, increased privacy of sensitive investor data, enhanced compliance, lower administrative and overhead costs for all participants, access to wider base of investors and assets for client onboarding, increased transparency and reduced fraud in the industry

LISTING ASSETS ON MULTIPLE PORTALS

An Issuer with an asset registered on the OFN can work with multiple portals and service providers to syndicate their offering across a broader audience of prospective investors. With the portals and partners connected to the OFN, they can easily remain in synch and ensure a consistent compliance and reporting mechanism across the board. Further, they can each mix and match different service providers as necessary. Similarly, an asset can be listed with multiple secondary market service providers without fear of “double selling” since the OFN serves as the main securities depository.

Benefits: Investor protection and security, increased privacy of sensitive investor data, enhanced compliance, lower administrative and overhead costs for all participants, access to wider base of investors, increased transparency and reduced fraud in the industry

TOKENIZED TRADING

The emergence of Initial Coin Offerings (ICOs) in 2017 has created a new asset class that challenges the construct of traditional financial markets and has put a further strain on a regulatory framework that has not been able to keep up with the rapidly evolving state of distributed ledger technology. With this new evolution of securities comes uncertainty from issuers and shareholders on issues of asset custody, ownership transfer and financial reporting.

The OpenFinance Network is designed for both traditional alternative assets and crypto/token securities, and allows for a streamlined compliant process from issuance to secondary market trading. Securities token trading is fully supported on day one and can be processed alongside other alternative assets in a standardized uniform fashion. Further, as the industry shifts towards a distributed ledger based book-entry process, issuers can leverage the system to connect to the “on-chain” crypto capital markets. OFN also provides mechanisms for a securities token protocol, S3 (Smart Security Standard), and issuance, bringing a full end-to-end solution for securities token issuance and trading.

While some may see “traditional vs crypto” as two different markets, we see a natural convergence of the off-chain and on-chain capital markets as the adoption of blockchain technology expands. From initially seeking to reduce back-office costs to accessing broader capital markets, the strengths of blockchain technology will ultimately create an environment for “smart securities” that is not only more efficient but will also provide increased access and improved service to the investing public at large.

SECURITIES TOKEN PROTOCOL AND ISSUANCE

In 2018 we see the eventual shift to security tokens as the primary vehicle for crypto investment. We have seen a few notable projects arise over the past year as security tokens, and expect a boom in adoption in the coming months. One of the main aspects of the securities transaction lifecycle is the process of issuance, and doing so in a compliant fashion is of the utmost necessity.

To best serve new issuers entering the space, we recommend two solutions to this problem. The first is working with an issuance platform on which a user can raise capital for their company under full compliance, ideally also connected to a secondary market platform such as OFN. The second is working with a standardized security token contract (such as OFN’s S3 security contract structure), to ensure that the primary and secondary market activities are conducted under full compliance. We believe that by making a protocol standard across the industry, we can create a thriving ecosystem in which all players are operating in a uniform standard.

SECURITIES TOKEN TRADING

When we look at “crypto” security tokens, we see financial instruments with familiar exemptions to other alternative assets, including Regulation D (506c), Regulation A+, and even Regulation CF. However, the actual issuance and transfer of these securities currently suffers from a lack of a defined process. While it is understood that AML/KYC checks must be conducted on the initial security token offerings (and accreditation checks for Reg D tokens), beyond that there is not much else done by issuers and portals today.

Many of these securities must adhere to SEC Rule 144 when transferring, which apply to selling restricted and control securities. Restrictions such as holding periods or AML/KYC checks on the new buyer are expected for compliant transfers of ownerships. Current Reg D token offerings resort to simply implementing methods for **Freeze()** and **UnFreeze()** at the asset level which take effect for all token holders and does not provide any specificity beyond allowing for an asset to be traded or not.

For investors seeking to sell their security tokens (or buy security tokens on the secondary market), there is a lot of uncertainty around transfer of ownership and whether updates to a distributed ledger truly reflect a compliant transfer under the eyes of the SEC and FINRA.

However, many of these concerns are resolved for security tokens within the OFN system. The Global Asset Registry maintains a distributed source of data around the specific assets and exemption types, ensuring that transfer restrictions are properly adhered to when attempting a change of ownership. Each investor participant can properly verify their AML/KYC data (and accredited status) using their Investor Passport. Transfer agents (required for Regulation A+ tokens) can also interface directly via network adapters to this broader decentralized securities depository and ensure compliant issuances and secondary market transfers.

DECENTRALIZED “STREET NAME” TRADING

When you buy public equities through a brokerage firm, most firms will automatically place your securities into “street name”. A street name is when securities are held in the name of a broker, custodian, bank, or some other nominee as opposed to being held in the investor's name. Public equities are largely held in street name because it makes transferring the securities easier, especially in the world of electronic trading. Before the introduction of electronic trading, all shares were held in a paper certificated form, either as registered shares (where the company maintains a register of owners of shares as well as issuing share certificates) and changes of ownership are registered, or as bearer shares where ownership was transferred simply by handing the bearer share certificate to the new owner. By holding securities in street name, it eliminates the step of physically transferring the securities to the investors and significantly speeds up the trade settlement. Public equities today are held in electronic form, making the need for physical transfers obsolete, but holding securities in street name still facilitates speedy trading.

Alternative assets don’t have the mechanism or infrastructure in place to support street name trading. With the advent of the OFN system though, these assets can be held in “distributed custody” by the network and its consortium of broker-dealers, custodians and banks in a method compliant with the Uniform Commercial Code (UCC). While the street name mechanism does have its flaws, we see blockchain as addressing some of the underlying issues of property rights, settlement and needless counterparty risk. In public equities one of the largest direct holders is Depository Trust Co. (DTC), a depository that holds securities for some 600 broker-dealers and banks (via its nominee Cede & Co.), but in a distributed ledger model the assets can be held by the broader consortium to minimize these issues. The act of placing an asset into distributed custody (also commonly referred to as “tokenization of assets”) allows for these "real" assets to be traded on blockchain with instant settlement times.

The distributed custody mechanism provides a bridge for certificate and traditional book-entry records to access a new form of distributed ledger book-entry recordkeeping and all the benefits that come with it.

DISTRIBUTED LEDGER BOOK ENTRY

We’ve covered the introduction of new crypto securities and the concept of decentralized “street name” trading as new capital market mechanisms allowed by blockchain technology. However, these are just bridging mechanisms to connect the worlds of traditional capital markets and crypto capital markets. As the benefits of distributed ledger technology become more evident to market incumbents, there will be a full migration toward a distributed ledger book-entry recordkeeping mechanism for the issuance and trading of all alternative assets.

In fact, we strongly believe that in three years’ time, we will see a massive shift from traditional off-chain electronic book-entry, to a recording of ownership entirely on the distributed ledger. We refer to this new process as “ledger-entry” to distinguish between not only between the location where the “book-entry” data is located but also to the newfound functionality and capabilities that this new system entails.

Leveraging our decentralized securities depository system, the industry can perform the full scope of the securities transaction lifecycle entirely on blockchain. Our Investor Passport allows for broker-dealers and online portals to securely perform all the necessary AML/KYC checks, along with accreditation and/or suitability reviews. The Global Asset Registry provides full transparency to the registered securities to boost investors’ confidence in the issuance. Direct integrations with financial institutions such as broker-dealers, custodians and transfer agents enable trusted intermediaries to play their necessary roles within the broader ecosystem in a frictionless format.

NETWORK BENEFITS

The primary benefit of the OpenFinance Network to the industry is the capability to leverage the strengths of blockchain technology (e.g. security, transparency and efficiency) in a compliant fashion that is in-line with the regulatory framework of financial markets. The standardization and interoperability that is provided by the OFN system creates a broader capital market that network participants can easily access and integrate with in their current capacity. The resulting unification of a fragmented marketplace creates new opportunities for incumbents and new entrants alike.

Above all, investors gain access to a wider universe of alternative assets, have full transparency to the entirety of their portfolio and the investment process, and benefit from the efficiencies, cost reduction and flexibility in the securities transaction management process. The brokers and financial advisors who service this community can also provide better access, reporting and insights to their clients across the spectrum of their portfolio.

The general benefits to participants on the OpenFinance Network are as follows:

- Improved operational efficiency
- Increased transparency
- Simplified regulatory oversight and reporting
- Reduced settlement times and associated risks
- Increased standardization and interconnectivity
- Access to broader capital markets and investor base for alternative assets

Specific benefit details can be broken out by participant type:

Participant	**Benefits**
Investors and Financial Advisors	• Investor protection • Privacy of sensitive data • Lower transaction costs • Trust and confidence in issuers, the assets and the system • Access to a wider selection of quality investment opportunities
Issuers and Sponsors	• Access to broader capital markets and wider base of investors • Lower capital raising costs • Efficiencies and lower costs in investor relations management • Ensured compliance with regulations • Provide higher levels of trust and confidence to potential and current investors

Participant	Benefits
Broker-Dealers and Service Providers	• Provide investor protection • Access to wider base of investors and assets • Efficiencies and lower administrative and overhead costs • Ensured compliance with regulations • Scalability for institutional player participation • More efficient way to place capital across a standardized basket of assets
Industry and Regulators	• Investor protection and security • Standardize the issuance, reporting, compliance and management of alternative assets • Reduce fraud and bad actors in the system • Bring higher level of transparency and oversight to all participants • Boost trust and confidence in alternative assets • Increased efficiencies in capital markets

TECHNICAL FRAMEWORK

SMART CONTRACTS

OpenFinance Network smart contracts are primarily defined at the Entity and Asset level to encapsulate the key data being recorded on the ledger. Certain actions and activities on the OFN system are permitted only to authorized Entities, such as Investor Validations.

The OFN Asset smart contract is the core contract which stores data about all assets in the system, as well as their relationships, transactions and events. It holds three main data structs: Relationships, Transactions and Activities. Relationships tracks the relationships between the Asset and other Entities in the system. Relationships can be of different types, such as owner, validator, and registrar. When an Asset is first created, certain relationships (such as owner) must be present, while others are indicated over the course of the Asset's lifecycle. Relationships can also track pending relationships, as Entities are required to confirm relationship requests from the Asset. Transactions keeps track of transactions between one Entity and another for the Asset. It executes tasks like recording transactions, validating transactions between related Entities, and maintaining state of the transaction over the transaction lifecycle. Activities keeps track of events and activities that occur at the Asset level. It records activities such as corporate actions and changes to the relations of the Asset.

The OFN Entity smart contract is the core contract which stores data about all entities in the system, as well as their verifications and transactions. Entities can be individuals, businesses, or other corporate structures. It holds two main data structs: Verifications and Transactions. Verifications keeps track of the validated verifications given to the Entity, along with the Validator that provided that verification. Transactions keeps track of transactions between the Entity and other Assets. Several other smart contracts inherit from the Entity contract, including the Investor, Service Provider, Issuer, and Regulator smart contracts, which each contain attributes specific to the entity sub-type.

NETWORK TOKEN

The OFN token is needed to transact on the network and acts as a license to use the system. License holders can also be granted additional authorization on the framework based on off-chain verification (e.g. for registered companies such as broker-dealers, custodians, and transfer agents). The structure of the network token is modeled so that industry participants and developers are incentivized to build on top of the open source framework. The license can be sub-licensed to others who wish to transact. The token transaction capacity (and frequency) are programmatically determined by the system's token capacity algorithm that adjusts the number of transactions permitted per token based on network traffic, meaning that transaction costs are dynamic and adjustable based on the needs of the network. The system is designed to expand network capacity once it exceeds 85% of current capacity. This mechanism guarantees that available transaction capacity will grow with increasing network usage, and rewards the early system adopters with increased license capacity. It is akin to the expansion of broadband capacity as network usage increased with the popularity of online digital video and gaming. A reserve of licenses will be held for regulatory entities to grant them access for real-time audits and reports.

NETWORK ADAPTORS

Network adaptors are technology applications that allow participants to directly interact with the framework off-chain. Most commonly, an adaptor is a website, mobile app or API that allows for legacy system to communicate with the OFN. This will be the main entry point into the system for many of the legacy players in the industry. Network Adaptors in turn interface with the system via decentralized oracles, which allow for off-chain data to be recorded on-chain. In order to mitigate the issue of single points of failure/fraud, this transport mechanism is accomplished via a network of multiple independent oracles responding to the same queries to reach a consensus.

A typical securities transaction lifecycle on the OFN framework is as follows:

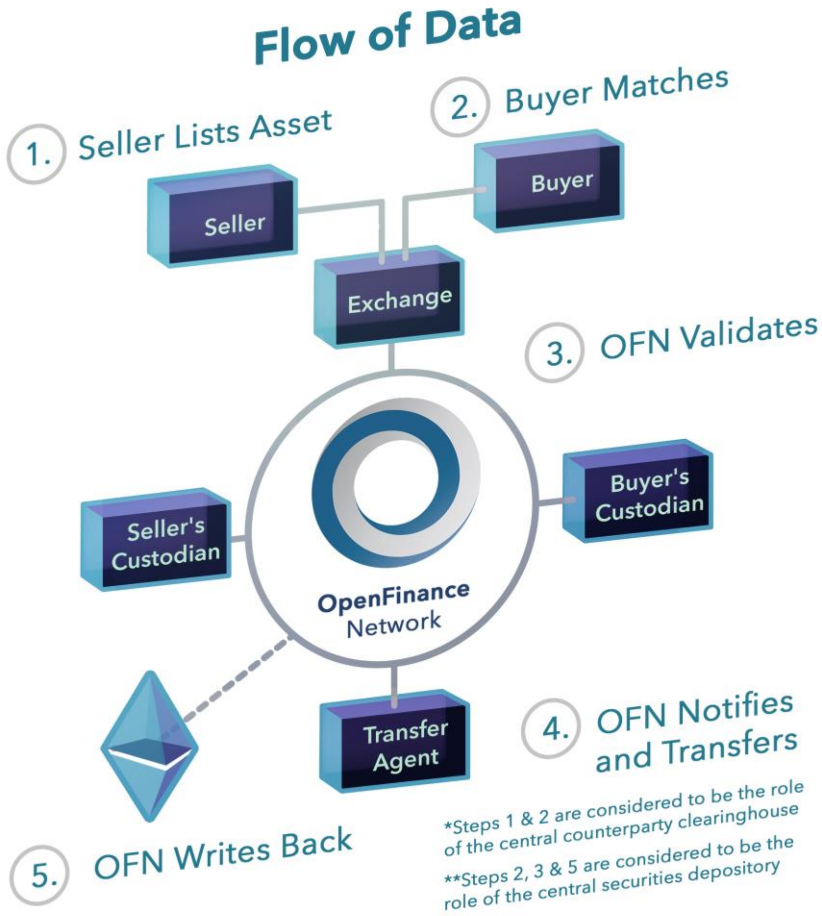

Flow of Data
1. Seller Lists Asset
2. Buyer Matches
Seller
Buyer
Exchange
3. OFN Validates
Seller's Custodian
Buyer's Custodian
OpenFinance Network
Transfer Agent
4. OFN Notifies and Transfers
5. OFN Writes Back
*Steps 1 & 2 are considered to be the role of the central counterparty clearinghouse
**Steps 2, 3 & 5 are considered to be the role of the central securities depository

FIGURE 4 - FLOW OF DATA

The typical flow for the Investor Passport:

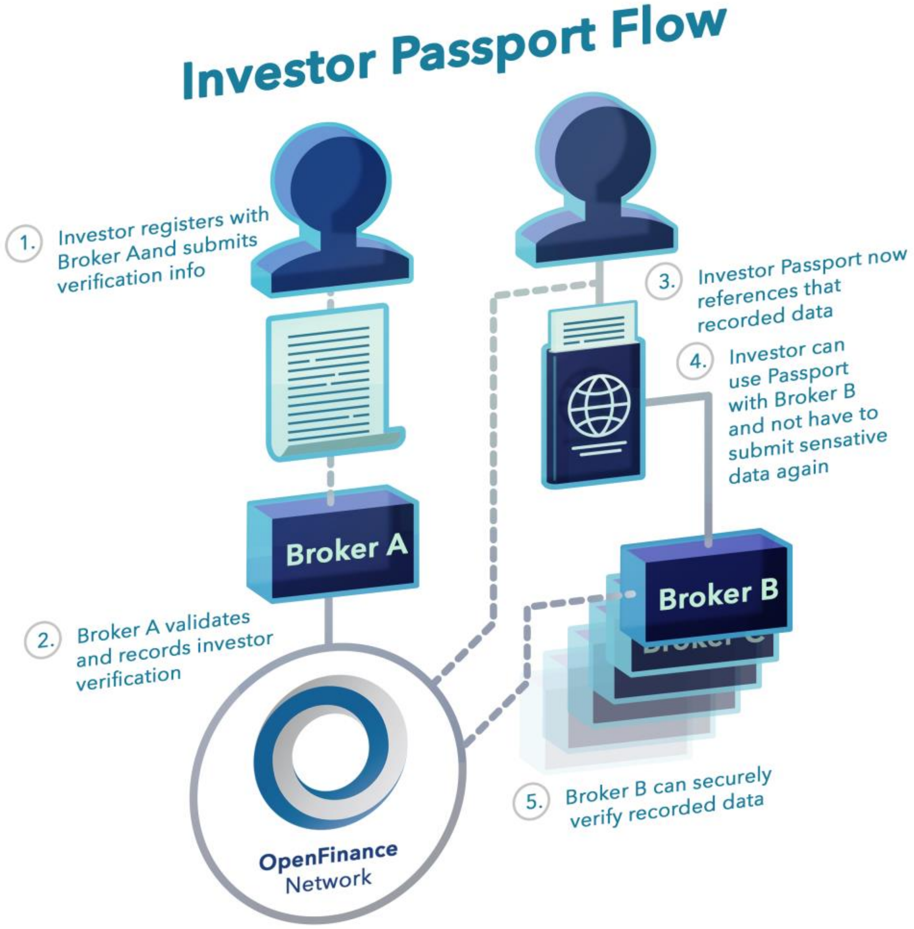

Investor Passport Flow
1. Investor registers with Broker Aand submits verification info
Broker A
2. Broker A validates and records investor verification
OpenFinance Network
3. Investor Passport now references that recorded data
4. Investor can use Passport with Broker B and not have to submit sensative data again
Broker B
Broker C
5. Broker B can securely verify recorded data

FIGURE 5 - INVEST PASSPORT FLOW

ZERO-KNOWLEDGE PROVING SYSTEM

In order to ensure compliance with regulatory guidelines and investor privacy laws, all sensitive private data is stored on a secure federated sidechain (SFS), which is then hashed back to the public chain to provide immutability to the SFS. All data transmitted via the OFN is encrypted and stored in a hierarchical format, and then organized into a Merkle tree, where each node in the tree contains a hash of its content and a hash of the hashes of its child nodes. The end hash of the root of this tree (commonly referred to as the Merkle Root, or the “root hash”) can then later be used as a validation signature to ensure the private data being referenced has not been tampered or altered in any fashion. The root hash is the value that is ultimately stored on the public blockchain, to remove the risk of private data being leaked.

While the underlying data on the SFS is immutable and auditable on a real-time basis, the question remains: how can the OFN be fully transparent to the public while maintaining data privacy? **How does an organization, motivated by the competing aims of transparency and privacy, publish verifiable statements about sensitive data without leaking the underlying data?**

For that we turn to an industrial zero-knowledge proving system, which allows for full transparency of auditable data to the public without compromising data privacy. A zero-knowledge proof is a mechanism by which one party (the “Prover”) can prove to another party (the “Verifier”) that a given statement is true, without conveying any information about the underlying statement apart from the fact that the statement is indeed true. In this scenario, the Prover is the OFN, while the Verifier is the general public. The OFN system provides secure cryptographic proofs that allows Verifiers to audit any transaction statement on the network. An audit can be thought of as a program that runs on the distributed ledger and returns whether or not the dataset is valid, consistent with previous versions, etc. By using a zero-knowledge protocol the OFN can prove that such an audit truly produced a reported result without revealing what the data was. This level of transparency brings additional trust and confidence to the OFN system, while increasing privacy of investor data and reducing fraud in the industry. For more details on the OFN zero-knowledge proving system, please refer to **Appendix A** for a detailed summary on the protocol and system.

Additionally, because only secure hashes are transmitted across the system, the OFN protocol is compliant with the statutory language of Section 4A(a)(9) of the Securities Act, which requires that intermediaries protect the privacy of information collected from investors. The SEC adopted rules to clarify that broker-dealers and funding portals are required to comply with Regulation S-P, Regulation S-ID, and Regulation S-AM. Taken together, these regulations obligate intermediaries to have policies and procedures in place to protect nonpublic information about investors, prevent identify theft, and limit the information shared with affiliates.

TEAM AND ADVISORS

DEVELOPMENT TEAM

Our team consists of exchange technologists, blockchain developers, mathematicians, securities lawyers, and trading industry veterans. The core team has been working together since 2014 in the alternatives asset industry.

JUAN M. HERNANDEZ – CEO

A serial entrepreneur, Juan has built multiple start-ups, including PeerRealty, Endurance Commerce, and the Pop Stock Exchange. Prior to entrepreneurship, Juan spent his career designing and developing financial exchange platforms, algorithmic trading systems and healthcare security networks. Juan holds a CS degree from Northwestern University and an MBA from the Kellogg Graduate School of Management.

TOBIN MCCOMAS – HEAD OF SALES

Tobin leads the institutional sales team. Prior to OFN, he worked in the Institutional Equities space for CLSA Americas and Sanford C. Bernstein & Co. While at CLSA, Tobin was responsible for the equity research sales effort for the US Midwest. Prior to that, he led US equity research sales in the London, UK office for Sanford C. Bernstein after covering institutional asset managers in Boston.

JORDAN FISHFELD – GENERAL COUNSEL

Prior to OFN, Jordan worked as a finance attorney for Katten Muchin Rosenman, LLP, and assisted in the rule development of the JOBS Act. Jordan holds a JD and MBA from the University of Miami.

KAEL SHIPMAN – HEAD OF TECHNOLOGY

Kael has over 12+ years of experience and is a veteran of the financial services software industry. Kael is a regular contributor to many open source projects across the web.

THOMAS MCINERNEY – HEAD OF BLOCKCHAIN DEVELOPMENT

Thomas has extensive blockchain experience, previously working on an Ethereum Network Streaming Music Distributed Application. Thomas has a finance degree from the University of Illinois and was previously involved in the financial services industry with UBS.

IAN SHIPMAN PH. D. – HEAD OF R & D

Ian holds a Ph. D. from the University of Chicago in algebraic geometry, which includes the study of elliptic curves. Ian is a functional programmer whose interests range from distributed systems to type theory. Prior to OFN, he was a Postdoctoral Researcher at Harvard University.

DAN BREEN – HEAD OF OPERATIONS

An industry veteran with over 25 years of experience, Dan has executed over 25,000 transactions in over 900 uniquely named assets totaling over $250 million of volume in the secondary market for alternative assets.

RAYMOND COTI – FRONT-END DEVELOPER

QUSAI FARRAJ – SOFTWARE ENGINEER

JACOB REGAN – SOFTWARE ENGINEER

KUNAL PATEL – SOFTWARE ENGINEER

INVESTORS AND ADVISORS

BK CAPITAL MANAGEMENT

POLYNEXUS CAPITAL

WEST LOOP VENTURES

INOVIA CAPITAL

M25 VENTURES

SIXTHIRTY

HARVARD ANGELS

ORIGAMI CAPITAL PARTNERS

TRIBAL VENTURES

WILLIAM MOUGAYAR

William Mougayar is a renowned enterprise blockchain expert, author of the Business of Blockchain, and a board member of the Ethereum Foundation.

DAVID KRELL

David Krell co-founded the International Securities Exchange, a leading U.S. equities options exchange, in 2000 and served as President and CEO at the firm. The ISE was the first fully electronic U.S. options exchange, and was acquired by NASDAQ in 2016.

JOHN KELLY

John K. Kelly served as the COO at Liquidnet until 2014. Liquidnet is a global institutional dark pool trading network that connects asset managers with liquidity. Liquidnet trades in 45 equity markets for asset management firms who collectively manage US$15 trillion.

JEFF CARTER

Jeff Carter is the founder of West Loop Ventures, a venture capital firm that invests in B2B financial technology startups that solve problems in institutional finance. Prior to that, Jeff formed the Hyde Park Angels, one of the most active angel groups in the United States, in 2007, and was also a former CME member & trader.

CONCLUSION

The securities transaction lifecycle in alternative assets suffers from an antiquated process and rampant inefficiencies - lacking interconnectivity, interoperability and protocol between multiple intermediaries. The promise of blockchain technology to streamline this process and reduce costs by eliminating various reconciliation processes and reducing capital tied up in the clearing & settlement cycle has prompted many incumbent financial institutions to actively assess its potential to improve efficiencies. However, there is a need for a driving force with the experience and capabilities to enable the integration of distributed ledger technology with existing legacy back-office systems.

OpenFinance Network, the leading trading platform in the $7.7TB alternative asset market, has developed a framework to solve this clearing & settlement problem in the industry, leveraging distributed ledger technology to bring efficiency, transparency, and interoperability to a fragmented market.

The OpenFinance Network is a protocol and framework for the processing of securities transactions, initially focused on the clearing & settlement process but intended for the entire securities lifecycle. This provides a common framework and communication protocol by which to standardize alternative assets and provide interoperability between the data silos of market participants. The system has several integration routes that can be leveraged across the various intermediaries in the industry in a transparent, secure and efficient method. Above all, the system allows for investors to gain access to a wider universe of alternative assets, have full transparency to the entirety of their portfolio and the investment process, and benefit from the efficiencies, cost reduction and flexibility in the securities transaction management process.

There is a once-in-a-generation opportunity within the alternative asset industry to reimagine and modernize its infrastructure to address long-standing operational challenges. The OpenFinance Network will not only make the alternative asset industry more efficient but will also provide increased access and improved service to the investing public at large.

OUR CORE PHILOSOPHY

- Our fundamental belief is that wealth creation should be available to all, not just the elite few
- Better financial tools are needed for shareholders and issuers alike
- Legacy systems are saddled with high costs and fees that make this network inaccessible to many
- Fraud is too often prevalent and commonplace, which creates a lack of confidence for investors
- Financial markets need light regulation to provide protection for all shareholders
- We are bringing increased access, transparency and efficiency to the alternative asset industry

APPENDIX A: INDUSTRIAL ZERO-KNOWLEDGE PROVING SYSTEM

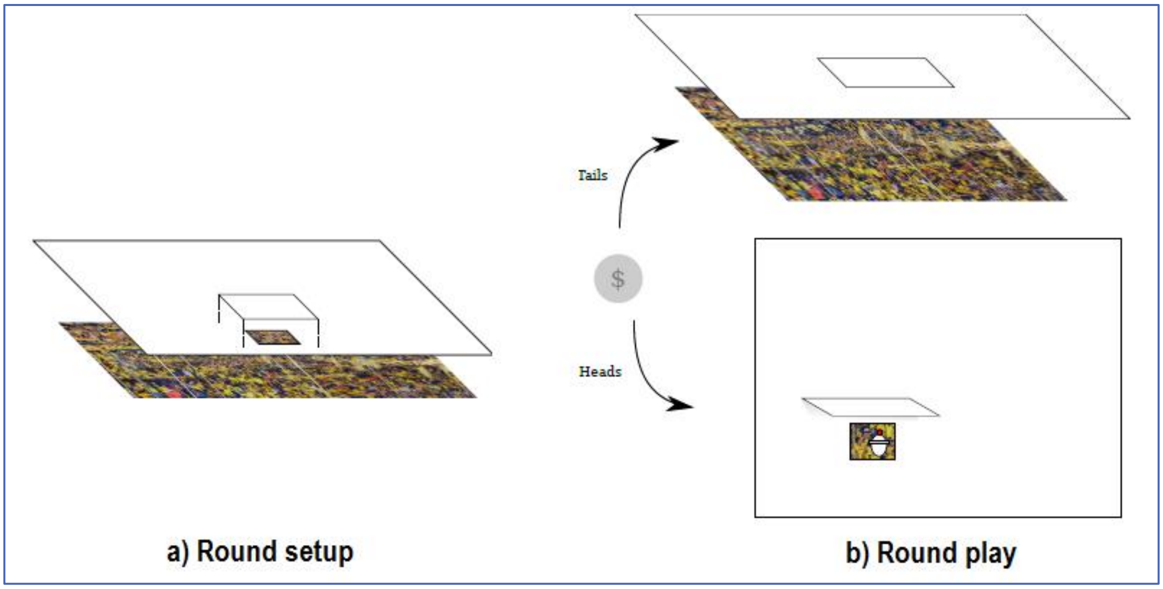
INTRODUCTION

Consider what we might mean by the term “industrial proving system”. The broad functionality is clear. An organization, motivated by the competing aims of transparency and privacy, wants to publish verifiable statements about sensitive data without leaking the data. While it may seem strange at first, it is actually possible to achieve this goal. In this appendix item, we will briefly introduce the concept of a zero-knowledge protocol. Such protocols can be used to build proving systems. We then explore how a proving system might look more concretely, and propose a sensible roadmap for building the OpenFinance Network zero-knowledge proving system.

ZERO-KNOWLEDGE ARGUMENTS OF KNOWLEDGE

Zero-knowledge (ZK) protocols are useful when one party, Alfred, wishes to convince another, Brenda, about the truth of a statement without revealing the evidence. ZK protocols were first examined in [GMR89] and a universal protocol was first proposed in [GMW91]. Suppose that there is a puzzle to which Alfred claims he knows a solution. He may want to convince Brenda he knows a solution, perhaps to sell it, without revealing what the solution is. It turns out that there are many things that can be viewed as a puzzle for the purposes of a ZK protocol.

- **Cryptographic digital signatures.** In a digital signature scheme, identity is tied to a public key. The public key is derived from a secret key that only the signer knows. The signer wishes to prove that the signer knows the private key without revealing it. The signatures used by schemes such as GPG, SMIME, and cryptocurrencies can be viewed as ZK proofs of secret key ownership.
- **Anonymous transactions.** One way to achieve financial privacy is to set up a payment system with a “pot” that anyone can pay into. To make an anonymous payment of amount *x* from the pot, a user needs to prove that they have paid at least *x* into the pot (less previous withdrawals). However, to remain anonymous they cannot reveal which incoming payment was theirs. Zero knowledge protocols can unlink payments into and out of the pot. An elaboration on this idea is used by the cryptocurrency ZCash.
- **Verifiable database audits.** A company can use ZK protocols to improve transparency. An audit can be thought of as a program that runs on a database, possibly with some other inputs, and returns whether or not the database is valid, consistent with previous versions, etc. Using a ZK protocol a company can prove that such an audit truly produced a reported result without revealing what the data was.



Let us walk through a detailed example of a ZK protocol. In this example, Alfred and Brenda are playing the game "*Where's Malbo?*". Alfred claims to have located Malbo. How can Alfred prove this to Brenda without giving away Malbo's location? To make sense of this, should have an idea of what it means to give away Malbo's location or equivalently: for one to not know Malbo's location. The standard way to think about this is point out that regardless of what else she knows, Brenda can always randomly guess a location. She has a small chance of guessing correctly, so even in a state of complete ignorance, Brenda might get lucky and find Malbo by guessing. Therefore, when we say that the protocol does not give away Malbo's location, we mean that after the protocol runs, Brenda's best strategy (short of solving the puzzle herself) remains random guessing.

The protocol that follows is an interactive protocol. It requires Alfred and Brenda to perform some, possibly large, number of rounds. To implement the protocol, Alfred and Brenda need a large stack of sheets of paper large enough to cover the Where's Malbo book they are using. They also need a fair coin.

A single round:

1. Alfred takes a sheet of paper and cuts out a Malbo-shaped hole from it.
2. Alfred places the paper with the Malbo-shaped hole over the book in such a way as to reveal Malbo, but cover the rest of the book.
3. Alfred tapes a small flap over the Malbo-shaped hole.
4. Brenda flips the coin:
    - **Heads.** Alfred lifts the flap, revealing Malbo through the hole.
    - **Tails.** Alfred lifts the large sheet, revealing the puzzle underneath.

For an illustration of the setup see figure (1a) and play see (1b). Let us consider the idealized situation where the book is perfectly flat so that Brenda cannot see its outline under the paper. To understand this protocol, we should think about the odds that Alfred can successfully complete many rounds of the protocol without knowing where Malbo is. Suppose that Alfred has complete ignorance about the location of Malbo. On a given round, either Alfred uses the true puzzle or not. If Alfred uses the true puzzle, there is a 50% chance that Brenda will ask Alfred to lift the flap. Given that Alfred does not know Malbo's location the chance that the hole shows Malbo (and not some random swath of the puzzle) is negligible.

In this case Brenda will discover that Alfred cannot find Malbo. Alfred could replace the true puzzle with a forgery in which he knows the location of Malbo. Then there is a 50% than Brenda will have Alfred lift the covering paper and discover the fake. In order for Alfred to go many rounds in this protocol, he must get very lucky: Brenda has to flip heads *every time* Alfred uses the true puzzle and tails *every time* he uses a fake. Since Alfred cannot know in advance the result of the coin flip, the odds of success are 2^{-N} where N is the number of rounds. (With 20 rounds, the odds of successfully lying are worse than 1 in a million.) So we see that by tuning the number of rounds, Brenda can be sure Alfred is being truthful with as a high a probability as she likes. (If Alfred has some rough idea where Malbo is, his odds of completing the protocol do improve for any given number of rounds.)

At this point, Brenda can be satisfied with the protocol. However, Alfred may have some reservations. To convince Alfred, we have to argue that after N rounds of the protocol, Brenda still cannot find Malbo more effectively than random guessing. The key observation here is that the only thing Brenda can see is the sequence of outcomes. While unlikely, it is *possible* that Alfred was totally ignorant, but lucky. This means that if Brenda could reliably extract useful information about the location of Malbo purely from a successful transcript, then she would be able to do so *even in the rare cases where Alfred is totally ignorant*. Thus the protocol does not leak information.

One drawback of a protocol such as this is that it requires Alfred and Brenda to interact over many rounds. It is possible to convert a broad class of ZK protocols into non-interactive ZK protocols. We can even do this (in an elaborate way) in our charming real-world example. First, Alfred and Brenda need to settle on a random beacon. Suppose that there is a trustworthy service that publishes the outcome of a fair coin toss every second over the radio. Alfred and Brenda can both refer to these coin tosses by the time they occurred. Next, Alfred will need N copies of the puzzle, scissors, tape, and patience. Alfred sends two messages to Brenda.

1. Alfred cuts each of the N puzzles into tiny squares and reassembles them randomly, keeping track of the mapping from original square locations to final square locations. Alfred sends Brenda the stack of scrambled puzzles.
2. Starting at an agreed upon time, Alfred and Brenda note the next N coin tosses from the random beacon. For each outcome:
   - **Heads.** Alfred sends Brenda the location of Malbo in the corresponding scrambled puzzle.

- **Tails.** Alfred sends Brenda the instructions to unscramble the corresponding scrambled puzzle.

Both Alfred and Brenda can be satisfied with this protocol for reasons similar to those given above, although at this point they are likely itching to digitize their system! While general purpose ZK proving systems are much more complex, almost all of the central ideas are represented in this sketch. Modern systems have one additional ingredient. The messages that Alfred has to send above are enormous. It is possible to use clever algebra to design *succinct* non-interactive ZK proving systems which have reasonably small messages. Unfortunately the ideas used to achieve succinctness are outside the scope of this summary.

PROVING SYSTEM ARCHITECTURE

In this section, we discuss some of the properties that a proving system would have to have to be used in production. The term private unambiguously refers to information that should only be known to (some) members of the organization. Public can have a broader range of meanings. For example, in some contexts public information is information that can be known to certain specific parties outside the organization rather than the general Public.

SYSTEM DATA

Computations. A reasonable candidate for the fundamental object in the proving system is the computation, which expresses a function, input types, and an output type. The output type has public designation, but some input types can be private. We expect that computations will be expressed in a special-purpose language.

Proofs. A proof is a data structure that corresponds to a computation, a particular instance of the public inputs, and the output. If valid, a proof implies that there is some value of the private inputs so that the computation transforms the input set to the given output.

Provers. A prover is an algorithm, corresponding to a computation that transforms input values and their output values under the computation into a proof. The prover has access to both public and private data.

Verifiers. A verifier is an algorithm, corresponding to a computation, which validates proofs. The verifier only has access to public data.

While provers and verifiers are algorithms, they are derived from computations. We expect that computations will typically have boolean output, where we would regard them as logical propositions. The central task from the organization point of view should be to declare the computations and logic for conditions under which to generate proofs. All other elements should be derived and distributed automatically.

COMPONENTS

Proof engine. The proof engine provides two services. It compiles computations into a pair consisting of a prover and a verifier. After compilation the verifier can be distributed to end users. However, construction of proofs, using the prover will probably be an online process. The second service provided by the proof engine is reactive construction of proofs using a stable of provers.

Verification engine. The verification engine will likely have several software representations. In an industrial setting, the verification engine reactively verifies proofs coming over the wire from other organizations. For end users, it is reasonable to compile individual verifiers into e.g. JavaScript for in-browser proof verification.

FEATURES

Automation. Construction and distribution of proofs should integrate seamlessly into the existing technology stack. In an event driven setup, other components can safely ignore the proof engine unless they require a verification or a proof.

Distribution. The distribution model should include specification for provers and verifiers in addition to proofs. All should be treated as versioned data in an ecosystem where several versions (or even standards) may exist.

Modularity. Computation reuse has not been a priority in the academic world. However, it is important to maintain libraries of computations, and provide a means for aggregating computations as much as possible. A growing library of computations and their compiled provers and verifiers that can easily be arranged into pipelines will significantly encourage adoption.

Development. Development in a system with proving has two prongs. First, developers must specify computations. The options for proof specification at the time of this writing are by using a subset of C or by directly expressing the computation in one of several arcane algebraic forms. Neither method has the kind of safeguards one would like to see in a secure computing development environment. Second, developers manipulate proofs by including proof generation and verification into the business logic. In the long term, this would likely be achieved by adding markup to source files indicating whether a proof should be published for a certain function or whether some kind of proof should be requested for a value coming over the wire from an outside system. Then as part of the build/deployment process the markup would be parsed and the proofs automatically made available or requested and verified.

Scalability. The system should make it possible for an organization to provide selective transparency at an extremely granular level. We imagine systems exposing tens, if not hundreds of verifiable, partially blinded computations on their internal data, updated as frequently as technology allows.

SYSTEM ROADMAP

There are already a handful of libraries which implement "research quality" proof systems. The best known of these are libsnark (SCIPR Lab based on [BSCG+13]) and pinocchio (Microsoft Research, [PHGR]). It is an open question whether or not a production ready proving system could be built. However, it is clear that limited versions of the system are possible.

PHASE I: INFRASTRUCTURE

The operating assumption in (I) is that the specification of computations and production of provers and verifiers is an expert task. So it is only possible in this phase to produce a small number of computations using a package like libsnark or pinocchio by ad hoc means. In this situation, the focus is on the system for integrating prover and verifier binaries into the stack. For the most part, development in this phase does not require more than one developer with the sophistication to use and patch the academic libraries.

Construct prover and verifier. Settle on one important and tractable proving task. Devote at least one qualified developer to configuring one of the academic libraries to generate a prover and verifier.

Provisional proof engine. The first implementation of the proof engine can be a wrapper around binaries generated in the previous stage. To the greatest possible extent, the proof engine should be constructed by combining existing task schedulers and event clients.

Provisional verification engine. As in the case of the proof engine the verification engine can also be a wrapper around verification binaries. There must be an emphasis on deterministic program generation. Users must be able to obtain everything they need to build the verification engine from the source code and computation specifications.

Proof exchange protocol. Ultimately zero-knowledge computation is about interactions between several parties. The team should specify a minimal extensible protocol for specifying proofs. This protocol can be used in communications between the proving and verifying engines at different organizations.

Deployment/build tool. Build a tool which analyzes sources in a target language for markup that associates certain computations to certain functions, marks values as private, etc. The tool should generate configuration for the proving engine such that appropriate proofs are generated.

Verification library. A common element of proof-aware programs will be blocking calls to the verification engine which continue upon receipt of some valid proof. So an API must be built which exposes the verification engine to the target language.

PHASE II: DSL AND OPTIMIZATION

The objective of (II) is to provide tooling to *correctly* specify computations and compile provers and verifiers at scale. This probably includes creating a domain-specific language to declaratively represent computations. These representations can then be compiled either to C, then to a prover and verifier using pinocchio, or directly to a prover and verifier. The domain language should sacrifice expressiveness for correctness. Some time should also be spent looking for a way to bootstrap proofs, transforming an existing set of proofs into a new one. An important example is proof updating to reflect dataset updates.

CONCLUSION

We now have a clear idea of the nature of a zero-knowledge protocol. The ability to selectively hide inputs to a computation makes it possible for an organization to become more transparent without compromising confidential data. With a general purpose zero-knowledge proving system, the OpenFinance Network could prove any statement about their transaction database that can be verified by a computer program. Beyond digital signature schemes, no such system currently exists. We have described some of the features that would be desirable in an industrial proving system and offer a vision for how to put one together. We are at the beginning of an exciting time as advances in cryptography and computer science make unprecedented levels of trustless coordination possible. The dream of verifiable self-regulation is certainly on the horizon.

REFERENCES

[BSCG$^+$13] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza. SNARKS for C: Verifying program executions succinctly and in zero knowledge. 2013.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. Knowledge complexity of interactive proof systems. 1989.

[GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity. 1991.

[PHGR] B. Parno, J. Howell, C. Gentry, and M. Raykova. Pinocchio, nearly practical verifiable computation.