Financial Securities Protocol

Eduard Silantyev

November, 2018

`fsp.network`

Abstract

Issuance, transaction, maintenance and settlement of financial securities costs hundreds of billions of dollars every year in form of legal, operating and monitoring overheads. Financial institutions, intermediaries, regulators and governments are forced to adhere to fragmented and ambiguous standards that lack transparency and determinism. Cross-border security transactions are even more opaque - complexity compounds when lack of mutual clarity is combined with legal debris. Financial Securities Protocol (FSP) offers an mechanism built on top of EOS blockchain for issuing and managing life-cycle of compliant and auditable securities. Securities of any type that successfully implement the protocol will enjoy a significantly lower all-round cost footprint, while adhering to relevant regulation. Beyond immediate benefits enumerated, FSP-enabled securities will enhance the transparency and efficiency of primary and secondary financial markets.

Contents

1 The Problem

In its current state, operations involving financial instruments are cluttered with various inefficiencies across many levels of an organisation. From issuance of securities, through to intermittent clearing, settlement and maturity, organisations generate massive overheads due to industry-wide embrace of outdated conventions. During various life-cycle stages of a security, the costs accumulated can be well in excess of 10% of nominal issue volume. Privately issued securities, on the other hand, lack price discovery, liquidity and sovereignty mechanisms. Below is an elaboration upon the spectrum of inefficiencies from standpoints of multiple economic participants - firms, regulators, central banks and financial institutions.

1.1 Primary Market

Issuance processes, such as IPOs and debt issues, are very complex processes, often involving consensus of multiple parties and satisfaction of a given set of objective conditions. To this day, investment banks are the biggest benefactors from primary capital market intermediation. Frictionless primary markets are vital to the health of an economy, as they represent the mechanisms responsible for capital allocation. Primary capital markets are arguably the most heavily regulated financial structures.

1.1.1 Issuance

While regulation in and of itself generally improves market integrity and compliance, it also requires issues of various securities to abide to certain standards. Among other rules, parties involved in the issue usually must comply with the highest standards of non-disclosures in order to lower the possibility of insider dealing and therefore, price manipulation. Moreover, regulations are non-stationary and are subject to constant revisions. Private issues are less constrained by regulation, however, lack of liquidity is a serious concern in such scenarios.

Year of 2017 has seen ICOs emerge as a new vehicle of capital raising. ICOs have revolutionised access to capital and subsequent transition to secondary markets - never before could an issuer reach a global audience and get listed on a dozen of venues within months of conceiving a fund raising process. ICOs are not without their downsides. ICOs, which usually entitle an investor to an ERC-20 token, do not grant any rights or claims to an investor that can be exercised in any event of governance (i.e. voting) or dissolution (ERC-20 token does not have a claim on underlying assets of a business). At a higher level, aggregate money raised by traditional fund raising activities such as IPOs and debt issuance has been in excess of $4 trillion in 2017 and belittles the $4 billion figure raised by ICOs in 2017 and $6.8 billion in 2018 (Conley et al. 2017). Transaction fees associated with raising funds in a traditional market place, however, are unjustifiable, amounting to roughly 7% of the amount raised. Convergence of the two methods has a potential to unlock value by making fund raising more streamlined and cost-efficient.

1.1.2 Price Discovery

Primary market price discovery involves polling market appetite for a given security. Price discovery is an asset-specific process. For example, fixed income securities and equities usually go through completely different pricing journeys; former usually discovers its price from the amount of money that is syndicated, the latter discovers its fair price from secondary market forces. Establishing a fair price of a security is usually an error-prone process that is driven by asymmetry of information and can result in market inefficiencies. In the case of privately held securities, such as shares of limited liability companies, it is often impossible to find and match buyers and sellers. For example, if you wanted to buy or sell a stake in Revolut Ltd., you would either do so via a funding round and / or by physically locating an entity with a complimentary interest. Such transactions usually take place through one's own professional network or a private equity fund.

1.1.3 Listing

Listing, also known as a process of transition to a secondary market, plays a big role in a life cycle of a security. In order for a security to be listed on a venue such as NYSE, for example, it once again needs to satisfy venue and jurisdiction specific rules and regulations, a process that can take anywhere from 6 months to 2 years (Bodie et al. 2012). In US, security offering exemption rules such as Rule 504 and Rule 506 (b, c) under Regulation D allow capital fund-raising and securities sale of privately held securities under certain investor / capital constraints. Regulation S, on the

other hand, allows for uncapped raising of equity and / or debt as long as U.S. persons are not being sold the securities. As such, securities complying with these rules do not have to be publicly listed to be sold to general public, but can effectively be traded between holders and authorised investors under certain constraints (Coffee Jr et al. 2015). The idea of embedding such regulation into computer-executable code will be explored in subsequent sections.

1.2 Secondary Market

In 1999 SEC allowed the use of electronic messaging when dealing in various types of securities. This has began a great paradigm shift that is still developing to this day (Barclay et al. 1999). Markets have started handling hundreds of times the volume they did prior and thousands of jobs have been transformed to reflect that changing landscape of market structure. Whilst technological capabilities of secondary markets have been advancing, supporting functions, such as booking, clearing and settlement, have remained largely unchanged. Such functions generate considerable costs for back offices of large financial institutions and regulators alike. In addition, lack of transparency, which is especially pertinent to cryptocurrency venues, is a big concern for regulators as well as market participants (Baker 2015).

1.2.1 Market Transparency

Recent survey conducted by Office of the New York State Attorney General Virtual Markets Integrity Initiative has shown that numerous cryptocurrency venues trade against their client trading flow, putting their transparency under a question mark (Underwood 2018). The survey uncovers that venues including Coinbase, Bitfinex and Poloniex are among the ones that trade against their clients. Other sources speculate that Bitmex, a Seychelles domiciled venue, that has the biggest dollar turnover in the industry, not only trades against their clients, but also uses covert front-running and deleveraging techniques that prey on their clients' orders and positions / risk limits (Hasu 2018). Such practices violate security exchange laws of more than one jurisdiction and are generally deemed inappropriate by regulatory bodies worldwide.

Traditional markets also deserve their fair share of criticism. Over the last few decades, volumes on electronic venues have skyrocketed but the number of participants have been reduced to a handful. Establishment of high barriers to entry has perhaps been the single most important factor in formation of such oligopolies. Currently, direct market access to Chicago Mercantile Exchange matching services costs a fee of at least $600,000 and purchase CME shares at a set rate (CME 2018). Introduction of exotic order types has led to even further information asymmetries, which adversely reflected in market microstructure. The demonstration of consequences of all these side effects has unfolded in 2010 Flash-Crash when liquidity has effectively evaporated from numerous markets due to inter-dependency of trading algorithms (Kirelenko et al. 2011).

Enabling a single executable standard for a fair electronic trading venue, therefore, becomes essential for transparent functioning of secondary markets.

1.2.2 Market Surveillance

Market surveillance is an expensive responsibility of financial regulators that ensures legitimacy as well as risk monitoring of financial transactions which take place via exchanges as well as OTC. In recent years, market surveillance has been aided by Machine Learning techniques such as Anomaly Detection, but the activity remains a very costly operation for regulators and law enforcement agencies (Fiore et al. 2013).

As mentioned in the previous section, major cryptocurrency markets remain voluntarily exempt from market regulation by choosing opportunistic jurisdictions to conduct their business in. New York State Attorney General Virtual Markets Integrity Initiative has hinted that lack of proper surveillance measures across cryptocurrency markets will hinder institutional adoption of the asset class (Underwood 2018).

Defining a protocol for markets to implement, market surveillance has a capacity to be embedded into computer code, such that resulting operations will only be executed if they are within the legal bounds defined by a regulator, a central bank or a government. Such solution, explored further in Section 3.3, has a potential to (i) reduce costs and (ii) establish confidence and transparency across various markets.

1.3 Security Administration

A full life cycle of a security consists of various auxiliary processes without which it would not be possible to facilitate well-functioning primary and secondary markets. Such functions include, but not limited to, transfer of securities, custodianship, voting, dividend / coupon payments and communication channels (Baker 2015). Future sections explore how security life-cycle tasks such as booking, clearing and settlement will become automated and self-regulating, because the business logic that guides such activities will be embedded into the protocol. Large financial institutions currently employ thousands of people in middle and back offices for such tasks to be performed and potential cost saving from implementing the protocol cannot be overstated.

2 Current Landscape

Having established the inefficiencies of the current handling of securities life-cycle, this section examines the validity of blockchain as a potential solution to these problems. Being a very nascent field, there are a few solutions that have been offered up. Some of them are implemented using blockchain and some are implemented using a classic (centralised) server business model. Further, the section provides an evaluation of current solutions to the problem of digitisation of financial securities and examines the benefits of employing blockchain to solve the problem.

2.1 Blockchain

Advancement of blockchain technology has gifted us an ability to unambiguously define business logic and deploy it directly onto a verifiable ledger. Blockchain, in turn, provides its users with certain properties and guarantees that are essential to solving the posed problem. There have been many implementations of the blockchain technology all varying, among other properties, in consensus mechanisms, reward structure and scalability. FSP defines a protocol for issuing, transacting, monitoring and settling financial securities; hence, it requires a scalable infrastructure to execute the required computations.

2.2 Blockchain Properties

Blockchain combines important properties and guarantees that are essential for core FSP functionality. Under normal conditions, these properties include, but not limited to, immutability, auditability, determinism and transparency. Among other benefits, these properties of blockchain enhance *asset sovereignty* of a security (Shapiro 2018).

2.2.1 Asset Sovereignty

Asset sovereignty refers to creating technological environment where securities can be held, exchanged and other wise transacted in a trust-minimising manner, while providing a high level of security. The term also preempts some of the benefits derived from features of a token (increased audience of fund raising, liquidity and life-cycle management) that were discussed in previous sections. Embedded regulatory features also mean that a security is effectively self-regulated, adding to its sovereignty, as it minimises the amount of 3rd party interactions required. Sections below explain how various properties of blockchain contribute to self-sovereignty of a security.

2.2.2 Immutability

We live in the world where data determines business decisions and business decisions determine data. Deliberately or otherwise, someone could change or delete past data, thus rendering this data less useful or completely useless for future use. Financial Services industry is one of the biggest data emitters and consumers in the world and is especially vulnerable to data corruption and mutation. Blockchain guarantees immutability by linking cryptographic hashes of data into a sequentially dependent chain of blocks that contain the data in question. In order to preserve the data about a financial security, FSP requires a data structure that can be used to record, store and retrieve data in its original state.

2.2.3 Auditability

When computation takes place on the blockchain, it can usually be verified by other nodes. Proof of work (PoW) was the first consensus mechanism to materialise this idea - when a node computes

a hash of a block that is smaller than some given number, other nodes can easily verify that the hash is indeed smaller by doing a one way hash operation, rendering all the transaction data within the given block true. More advanced consensus algorithm such as proof of stake (PoS) and delegated proof stake (DPoS) have since been developed and are deemed more robust means of determining consensus and verify the state of a blockchain. Auditability of securities is one of the main requirements of financial reporting; internal processes such as P&L and balance sheet reconciliation, as well as external requirements such as regulations and other legislation, require the underlying security to be fully auditable. FSP leverages the blockchain technology to verify the integrity of FSP-enabled securities and associated transactions, so that the parties in question can comply with given regulations and business workflows already in place.

2.2.4 Determinism

Computer code depicts an objective set of instructions that can effectively be analysed, and an output can be determined upon a set of inputs. Even in highly non-trivial instances of computer programs that involve concurrency, a professional programmer can determine if the output is deterministic or not. Determinism, therefore, refers to the same output given a certain input, no matter how many times or in what circumstances the code is ran. In functional programming, such property is called *referential transparency*. In blockchain, determinism refers to the fact that smart contracts have to be deterministic because each node of the network has to be able to compute the same result given the same input in a contract method. Otherwise, each node that executes the contract method to validate the transaction would end up with different result and no consensus would be possible. Execution of transactions of FSP-enabled assets requires a guarantee that the execution will yield the same result given the same inputs in a variety of conditions, making determinism essential for the implementation of the protocol.

2.2.5 Transparency

By definition, blockchains are completely transparent data structures. For example, by computing various transaction inputs and outputs, one can trivially calculate a Bitcoin balance of any address on Bitcoin blockchain. Transparency of financial data has been a very controversial topic. Investment banks, for example, generate data by trading against their customers flow. Exchanges generate data by means of orders that arrive to their limit order books or get crossed by a matching engine. Regulators, on the other hand, require market participants to submit their trade records to a trade repository (this is especially prevalent in OTC derivatives after GFC), so that the overall risk in a system can be robustly monitored. In today's world a party who generates data has every right to keep it. Financial markets should not be an exception; only subsets of data are transparent to any given party. FSP implements layered and permissioned access to data by leveraging private-public key cryptography, especially multi-signature access in order to solve this problem. For example, if an investment bank is required to commit its OTC derivatives trade data to a trade repository assigned by a regulator, then only the bank and the regulator are the only parties in possession of private keys that give access to that repository.

2.3 Security Tokenisation

Over the last two years, there have been various projects that set out to migrate traditional securities onto the blockchain. This movement has been known as Security Tokenisation. With varying degrees if success, these initiatives have produced first proofs of concept of securitisation via means of blockchain. This section evaluates the extent to which each of the given solutions accomplishes the task of securitisation.

2.3.1 Polymath

Polymath is a security token platform, which allows investors and issuers to interact in a compliant manner. Issuers can launch securities that are backed by ST-20 standard, a Polymath adaptation of ERC-20 token standard with addition of compliance checks to token admin operations. The platform also introduces its own POLY token, which itself is an ERC-20 token and is to be used as a medium of exchange for services that the platform offers.

Polymath has arguably been first to the market of security tokenization and, as of the time of this writing, has achieved the first proof of concept. The main potential weak point of the Polymath network is the fact that its chain code lives on Ethereum blockchain, which limits the

scalability of Polymath. Polymath white paper does, however, state that its contracts heavily optimise gas cost but could be "linked to other platforms".

2.3.2 Harbor

Harbor addresses the issue and life-cycle of private securities. In its white paper Harbor introduces R-Token, an ERC-20 compatible implementation of a compliant security token. R-Token relies on individual implementations of `RegulatorService` interface that define the constraints of transfers of tokens. As such, a Reg D compliant token can check for an array of constraints before a transfer is initiated, e.g. holding period of 12 months is satisfied and a transfer is made to a qualified investor.

Being yet another standard for security digitisation, R-Token has a potential to reach its audience of SMEs looking to raise anywhere from $1 million. By the same virtue as ST-20, R-Token is to be implemented on Ethereum main-net, which may hinder its scalability. Standard fragmentation is another issue that becomes apparent on the large scale, whereby the issuers are left guessing which token standard they should implement.

2.3.3 Securitize

Securitize defines an ecosystem for digital securities (DSs) that consists of DS Services and DS Apps that address all aspects of a security's life-cycle. At the heart of the infrastructure are the modules that are responsible for trust, registry, compliance and communication. DS Token, an ERC-20 adaptation provides an interface that fits within the framework and can be implemented by a security that is issued on the platform.

Subject to implementation, orthogonality of services is a great design decision for any software system, but especially it is vital for a system that is responsible for full life-cycle management of digital securities, where each service is responsible for a subset of all the functions that system needs to handle. DS Token also contributes to the recurring theme that now merits a discussion of its own - standard fragmentation.

2.4 Standard Fragmentation

As new security standards emerge, issuers become increasingly confused about the standard they should implement. The main requirement for a standard needs to be future-proof. No organisation wants to implement a standard that will become redundant in future.

A solution of plumbing interoperability via adaptation layers is always viable and is precisely the approach that OpenFinance network is taking in order to allow trading of security tokens. ERC-20 interface implementation is the only requirement on OpenFinance, however, additional layering will need to be implemented by OpenFinance on a per-standard basis. It is simple to see how this problem may grow out of proportion if new standards keep emerging. Not only will this be technically challenging to manage, it may also have reputational repercussions for the whole space and can drive potential businesses away from considering digitisation of their equity.

Initiatives such as Security Token Standard (Clarke 2018) have been conceived by a consortium of security token platforms as well as regulators and law enforcement agencies to establish a common standard that can be future-proof. ERC 1400 standard is a direct result of this consortium, which draws its design from inputs of dozens of industry participants. At its heart, the design implements ERC-20 standard and layers it with other functionality that members agree upon. Round tables that include as large an audience as possible in discussion of standards are instrumental for convergence to a single standard that everyone can adopt.

3 Financial Securities Protocol

FSP establishes generic securities standard on EOS blockchain. At the crux of its aim is decreasing friction, and increasing determinism and transparency of the marketplace. That being said, FSP does not aspire to be an imposition of any standard - it brings forth a proposition to establish a single, global and generic framework; a framework that can provide sufficient means for the regulatory requirements to be embedded into computer code and the one which will respectively constraint the operations that can be performed with a given security.

3.1 EOS Blockchain

EOS blockchain builds on a decade of blockchain wisdom of space thought leaders such as Daniel Larimer. Scalable decentralised applications invariant from their centralised counterparts is the mantra upon which EOS is built.

3.1.1 Decentralised State Machine

EOS is an open-source platform for decentralised applications. The EOS main-net has been launched in Summer 2018 and dozens of dApps have been deployed on it. Essentially, EOS is a deterministic decentralised state machine whereby block producers ensure validity of state and transactions that occur on the blockchain. EOS has already proven its scalability, consistently being the most active blockchain in Fall 2018. EOS has block time of 500 ms, which is suitable for high-throughput and low-latency applications such as decentralised exchanges to be implemented on top of the platform. Introduction of Demux, a mechanism similar to Ethereum side chains, has unlocked a big potential for deterministic transaction processing off-chain and can increase transaction throughput and frequency beyond the set block time.

3.1.2 Governance and Arbitration

Governance is a process by which people in the community arrive at consensus on matters affecting the community. Under Delegated Proof of Stake (DPoS) consensus mechanism, most of the power of token holders is delegated to 21 community-elected block producers. In turn, block producers are authorised to freeze malicious accounts, prune or update defective applications and propose / vote on changes to the underlying protocol. As such, block producers act as gatekeepers of the constitution and prevent blacklisted accounts from transacting on the blockchain.

3.1.3 Inter-blockchain Communication

Applications such as InterLedger, Cosmos and Polkadot have opened way for network effect to take place on an inter-blockchain level. Inter-blockchain communication (IBC) is especially important if the security token standards continue to diverge (see Section 2.4) and a need for bridging various protocols will become irreplaceable. Systems enumerated above will make it possible, for example, to exchange a security that implements FSP-10 for a security that implements an ERC-1400 in a secure fashion and without a need for a third party.

3.2 FSP Conjecture

Prior to exploration of FSP ecosystem, we need to lay some base intuitions upon which majority of the arguments in this section rest upon. Specifically, we make only one root conjecture in respect to the relationship between digitisation of securities and computation:

Any security whose issuance, governance and life-cycle management logic is unambiguously defined in legal terms can also be defined and executed by a Turing Machine.

This section, therefore, proceeds to outline a set of standards expressed as EOS smart contracts. Further to the above, this paper very much sees digital, also known as "tokenised", securities as a logical continuation of current traditional securities standard. Hence, a reference to a security could mean, depending on the context, a reference to a digital security that implements FSP or its traditional counterpart.

3.3 FSP Ecosystem

At at its core, FSP is a set of EOS smart contract that guide securities through their constrained life-cycle, made such by respective regulations that are embedded into code. The system adopts generic framework in order to make the work-flow of issuance, management and auditing of securities as generic as possible. Contracts responsible for different functions are defined within separate source files, e.g. `fsp.{module}`, promoting modularity in a vastly orthogonal system such as FSP.

3.3.1 `fsp.security`

The security contract defines the most generic of methods required for life-cycle management of securities. Implementation of a vanilla contract that inherits from `fsp.security` is the only requirement for a security to become a part of the FSP Ecosystem. Within the same namespace and inheriting directly from it are the classes `fsp.security.equity`, `fsp.security.bond`, `fsp.security.currency`, which provide vanilla implementations for securities of respective asset classes and act as blueprints for securities compliant to specific regulations. Without complying with any specific external regulation (e.g. Reg series and respective exemptions), vanilla implementations are subject to EOS Constitution, under which, subject to arbitration, blacklisted account holders will not be able to transact and freezing of funds as well as reversal of of invalid transactions is implemented. Where appropriate `fsp.security` contracts call the implemented `fsp.regulator` (see section 3.1.2) methods to check if the action to be executed adheres to regulatory standards under which the security was issued / securitized. `fsp.registry` is contacted any time the contract needs to retrieve data on a holder(s) of the security; for example, when dividend is paid, the security contract iterates over key `fsp.registry` (see Section 3.3.5) data structures, performing respective transfer actions. Any communication traces within FSP are managed by `fsp.communication` contract.

The framework allows developers to define complex logic for individual securities. For example, there could be an instance of `fsp.security.bond.convertible` that defines a complex pay-off schedule and gives a holder an option to convert the asset into `fsp.security.equity` when certain conditions are met. By the same virtue, an organisation could issue `fsp.security.bond.floating` that calls `fsp.security.benchmark` upon coupon date to extract the respective benchmark data in order to calculate the resulting coupon. Further, it is possible to extend the logic to define instances of fsp.security.option and `fsp.security.swap` that query agreed sources to calculate the resulting cash-flows / pay-offs. To generalise, `fsp.security` facilitates for the most complex of financial engineering logic to embedded into a smart contract. The remainder of the ecosystem serves these contracts during their life-cycle.

3.3.2 `fsp.regulator`

As mentioned, the regulator class is a module responsible for constraining various actions, such that FSP can be self-reliant. Methods of `fsp.regulator` implementations get called in various methods of `fsp.security`. The relationship between security and regulator contracts is surjective, meaning that more than one security contract may be assigned to a single regulator contract.

`fsp.regulator` is equipped with the following methods that require implementation:
`fsp.regulator.checkIssue(issuer)`, `fsp.regulator.checkTransfer(sender, receiver)`, `fsp.regulator.checkListing(sender, receiver)`. As regulatory landscape changes the contracts defining the logic will be updated accordingly, which may or may not affect the logic of the security contracts. In its simplest implementation, `fsp.regulator` approves any action, subject to some fundamental constraints e.g. availability of funds, that a caller requests.

One of the main features of the regulator contract is its multidimensionality. `fsp.regulator` can potentially be responsible for management and approval of operations a number of types of securities within a single jurisdiction. In this way, the regulator contract is the gatekeeper of the FSP ecosystem as it places the needed constraints on what and by whom can be done within the system.

3.3.3 `fsp.exchange`

The base exchange contract defines an interface for implementation of various types of value exchange logic. Such logic may be constrained by jurisdictional laws, local financial regulations and other limits that constrain sale and exchange of securities. `fsp.exchange` contract largely leverages polymorphic features of `fsp.security` and, therefore, by definition, the compliance features of `fsp.regulator` contract. Any security exchange rules (e.g. The Securities Exchange Act in U.S.) that apply to respective securities are embedded in fsp.regulator such that these rules are exposed for fsp.exchange to contact.

Various venue implementations could be employed with `fsp.exchange`. The contract can be deployed to operate an order-driven, limit order book via `fsp.exchange.book` or in fact, a quote-driven market aimed at liquidity provision via `fsp.exchange.lp` by one or more LP's. Perhaps the biggest benefit of the exchange instances is their ability to cater to liquidity demands of market agents, while security holders are able to transact autonomously.

`fsp.exchange` contract presents a complete rethink of a fair value exchange. Maker-taker fee schedules are defined specifically on instance creation. The contract also prevents front-running by not allowing multiple transactions to affect single action within the same block, a concept we define as *block-action independence*. EOS blockchain operates at 0.5 second block-time, which renders it a sufficient environment for low latency system such as financial exchange.

3.3.4 `fsp.communication`

The communication component of FSP allows for prompt communication between various modules and the users. Topics of communication can vary according to the action that triggers the communication. Sensitive data is handled via public-private key cryptography, such that only recipient of data can read the contents of communication packets.

3.3.5 `fsp.registry`

Registry contract maintains a list of active holders of instruments and is instrumental for governance operations such as dividend payments and voting. This module goes hand-in-hand with `fsp.registry` since information on proposals needs to be delivered to investors in prompt and verifiable manner. In the same spirit, information from investors needs to be collected and delivered for aggregation.

3.4 FS2P

FS2P stands for Financial Securities Protocol Proposals. It facilitates an open discussion, whereby proposals and their corresponding implementations can be presented and the ones that have merit will be included into the protocol. In its FS2P is an essential part of the protocol because it allows its stakeholders to voice their suggestions for improvements and it provides a discussion mechanism to scrutinise such proposals. Any suggestions shall be submitted to `fsp-core` issues section and should begin their subject with `FS2P-XYZ` where `XYZ` is a sequence of numbers.

3.5 FSP PoC

FSP is the first entity to implement `fsp.security` protocol in order to (a) demonstrate a proof of concept and (b) raise capital for holistic development of the entire FSP ecosystem. Unlike a utility token, there are no services that can possibly be purchased for FSP tokens, instead, the investors will get a share in profits of the entity, as generated from the activities outlined in the section below.

3.6 Revenue Model

Primary mission of FSP is implementation of Digital Economy. The company earns revenue by consulting its clients on digitising their businesses and assets. In this spirit, FSP practices what this white paper outlines and set a standard of how a digital security can be issued, managed and otherwise utilised, leading by its own example. Stakeholders will receive dividends based on the profitability of FSP.

Initially, FSP focuses on securing strategic partnerships with regulators, institutional investors and institutions such as central banks, governments and investment banks. Consulting the partners on implementing the Financial Securities Protocol within their respective organisations will thus be the main revenue driver for FSP.

4 Conclusion

The white paper builds a case for security digitisation on EOS blockchain. Namely, the ecosystem handles issue, sale and exchange, governance and life-cycle management of a security. By taking advantage of inter-blockchain communication protocols, FSP slots into an exisitng ecosystem of security tokens, thus becoming fututure-compatible with other protocols. Performant features of EOS, as well as its constitution, make it a suitable platform for resource-heavy application such as security digitisation network. Last but not least, Financial Securities Protocol will be the first entity to implement the `fsp.security` interface, thus confirming the viability of issue and management of securities via FSP network.

References

Baker, R. P. (2015), *The trade lifecycle: behind the scenes of the trading process*, John Wiley & Sons.

Barclay, M. J., Christie, W. G., Harris, J. H., Kandel, E. & Schultz, P. H. (1999), 'Effects of market reform on the trading costs and depths of nasdaq stocks', *The Journal of Finance* **54**(1), 1–34.

Bodie, Z., Kane, A. & Marcus, A. J. (2012), *Essentials of Investments 9th Edition*, McGraw-Hill.

Clarke, S. (2018), 'Security token standard'.
URL: *https://thesecuritytokenstandard.org/*

CME (2018), 'Cme membership lease and purchase'.

Coffee Jr, J. C., Sale, H. & Henderson, M. T. (2015), 'Securities regulation: Cases and materials'.

Conley, J. P. et al. (2017), Blockchain and the economics of crypto-tokens and initial coin offerings, Technical report, Vanderbilt University Department of Economics.

Fiore, U., Palmieri, F., Castiglione, A. & De Santis, A. (2013), 'Network anomaly detection with the restricted boltzmann machine', *Neurocomputing* **122**, 13–23.

Hasu (2018), 'A storm is brewing over the largest bitcoin exchange'.

Kirelenko, A., Kyle, A., Mehrdad, S. & Tuzun, T. (2011), 'The flash crash: High-frequency trading in an electronic market', *Journal of Finance, Forthcoming* .
URL: *https://papers.ssrn.com/sol3/papers.cfm?abstract*$_i d = 1686004$

Shapiro, G. (2018), 'Tokenizing corporate capital stock'.
URL: *https://gabrielshapiro.wordpress.com/2018/10/28/2/*

Underwood, B. D. (2018), 'Virtual markets integrity initiative report'.