

EXPREAD: A NETWORK OF CRYPTO EXCHANGES POWERED BY DECENTRALIZED TRANSACTIONAL PROCESSING AND UNIFIED LIQUIDITY POOL

White Paper: Version 2.2

Abstract. EXPREAD offers highly scalable white label solutions on crypto-exchanges to diminish the entry barriers and monopolistic concentration of crypto trading operations. EXPREAD liquidity model enables a seamless aggregation of the market depth to harvest the synergy value from unified liquidity pool. Systematically facilitated order execution allows exchanges to adopt community based, targeted marketing approaches as a more efficient way to leverage their network of acquaintances and accumulated reputation. The internal architecture of EXPREAD ecosystem is based on federated network topology with integrated infrastructure of payment channels protocol (powered by blockchain technology) to optimize decentralization vs scalability tradeoff. The system is a hybrid model effectively designed to combine the advantages of decentralized and centralized crypto exchanges.

Key words: crypto exchanges, business network model, white labels, community orientated marketing, DEX, payment channels, peer-to-peer, distributed governance, blockchain technology

Contents

- 1. Current Systems of the Crypto Exchanges and its Deficiencies2
- 2. Introduction to Design of EXPREAD3
- 3. Economic Rational and Synergy Value Created through EXPREAD Model6
- 4. State Channel Protocol Applied for the Decentralization Internal Clearing.....7
 - 4.1 Details on Operation of the Payment Channel System.....9
- 5. Backward Auditability of the Order Book and Trading Engine.....11
- 6. Procedure of Opening a Venue and Description of the EXPREAD White Label Solution.....13
- 7. Description of the Trading Tools Provided by EXPREAD.....15
- 8. Business Model for the Exchanges Opened in the EXPREAD Ecosystem17
 - 8.1 Lending Scheme in EXPREAD Ecosystem18
 - 8.2 Geographical Breakdown.....20
- 9. Economic Model of the Token and Governance.....22
- Bibliography.....25

1. Current Systems of the Crypto Exchanges and its Deficiencies

Cryptocurrencies are designed to promote the concept of the decentralization of the transactional and data systems. However, the current crypto-economy is trending towards more centralized infrastructures and execution. The crypto-exchanges play major role to provide liquidity to the market, assist token price convergence to fundamental value (for long run) and promote their mainstream adoption. The past 7 years have seen the emergence of several hundreds of centralized and decentralized exchanges, which seems inefficient considering the segregation of the potential liquidity and market debt each new exchange brings into the space. Furthermore, current exchange systems overall are prone to significant risks and failure, which are related to both incidental failures, inefficiency of underlying protocol and design as well as fraudulent activities.

Centralized exchanges have same loopholes as overall systems with centralized architecture: single point of failure, centralized control and governance (lack of transparency, unfair front-running, price manipulation, etc.). These entities are vulnerable to attacks (single point of failure), which may vary from suspension of the service and unresponsive servers (such as DOS attacks) to major security breaches and loss of significant parts of crypto deposits aggregated in an address. The systematic failures of centralized crypto exchanges are illustrated by over 2 billion USD lost over recent years due to scams, bugged security protocols, inefficient management and inept internal controls. All above mentioned failures are driven from two main factors: overreliance on safety of the system (one failure may bring a disaster), lack of adequate checks and balances to identify the misbehaving trusted central party.

Furthermore, there is a systematic lack of interconnectivity and liquidity bridging between these exchanges which leads to emergence of isolated liquidity pools. The segregated market debt leads to inefficient price discovery, arbitrable differences of prices and high cost of execution of big transactions (due to price swing). Though, presently, there are few liquidity aggregators trying to bridge different platforms, only a small fraction of exchanges (some big exchanges) have collaborations through aggregators, which itself further promotes the monopolistic power of big exchanges, creating liquidity barriers of entry for new participants.

Due to above mentioned inefficiencies the full decentralization of crypto currency exchanges may sound a good option in theory, however, it also has deplorable malfunctions if applied in practice. The full elimination of the middle man is prone to several detriments of the utility of exchange function, in terms of higher cost, slower trading engine, basic functionality, etc. The decentralization through ethereum smart contracts was one of the earliest attempts, however the on-chain order book running and matchmaking is unacceptably costly (due to required gas). Later on, other protocols have been created with better configuration, such as 0x and Swap designed to enable off-chain order book and on-chain transaction settlement. Though these protocols are less costly, they have slower trading engine and do not accept “true” market or limit orders, which may be acceptable for one time P2P cryptocurrency exchange, but highly limits the user base interested in more active day-trading, or speculation.

Furthermore, the decentralized systems do not fundamentally solve the liquidity segregation problem. There is no technical standard in the space and proposed decentralized exchange protocols have different configuration process and design which hampers their interconnectivity. Therefore, the exchanges operating on top of them have inherent coordination and chain interoperability problems, which further segregates the liquidity pools in the market.

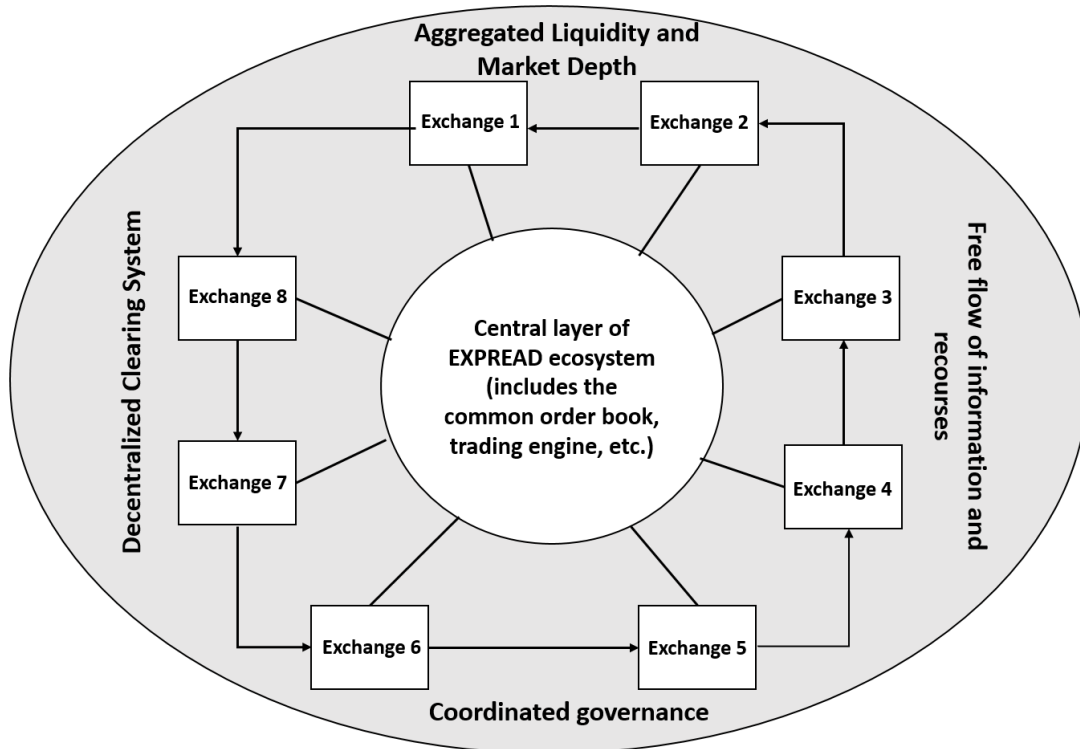
The paper introduces EXPREAD exchange system as a hybrid solution designed to combine the advantages of the centralized system (sophisticated functionality, high performance of trading engine), decentralized systems (higher security, fully transparent and auditable operations, joint governance). The EXPREAD is proposed to completely decentralize and liberalize (very small barriers of entry) the crypto exchange virtually enabling everyone to open his own node of exchange, at the same time bring full aggregation of the liquidity in the whole EXPREAD ecosystem. The system is created as an optimal way to leverage the synergy value of multiparty exchange (proper economic incentives) and unification of the market.

2. Introduction to Design of EXPREAD

EXPREAD is an ecosystem of white label crypto-exchanges, which have shared order book, trading engine and liquidity pool. It is built on proposition of shared economy on exchange service

provision where multiple venues (node, exchange) aggregate their liquidity, technology costs and unique expertise to achieve synergy value from network effect. Furthermore, the whole system is composed in a way to distribute the reserves of the liquidity to avoid single point of failures. The trading system is fully auditable by each node (exchange) providing adequate internal control process.

Figure 2.1: Composition of the EXPREAD ecosystem



Every order initiated in one of the venues (exchanges) attached to the EXPREAD ecosystem is routed to the whole system enabling higher probability of order execution. This is fundamentally different from the current centralized crypto exchanges which mainly are seeded by the internal order flow. Therefore, if the centralized as well as decentralized exchange systems do not achieve critical mass of ongoing liquidity in standalone basis, they will cease operation. The EXPREAD ecosystem through multi-venue design should have much higher velocity of user growth, enabling new exchanges opened in the system to enjoy significant market debt.

The EXPREAD system is composed of three compound layers. At the center of the ecosystem is the EXPREAD foundation which will make sure that unified order book and trading engine are

operating properly. The foundation will be built for the sole purpose to provide technology, security, business advisory and other services to the EXPREAD ecosystem. The foundation will also operate as a central governor driven to create further incentives for the development of the EXPREAD network.

The order book will be broadcasted through all venues (exchanges) opened in the system, which is the next layer. The EXPREAD provides fully customizable interface, functionality, tradable token selection optionality as well as other tools for the internal management of the white label exchanges by the owner. The exchanges (venues) are the gateways for the end users to the EXPREAD system, the accepted orders are registered in the internal book as well directly in the unified book maintained by EXPREAD foundation. The internal order books are not anyhow channeled with the central order book which is used for the backward audit purposes.

The third layer is based on the Payment Channel protocol created to support the design of EXPREAD and is powered by ethereum blockchain. The platform applies a fundamentally novel approach of crypto-fund depository with integrated decentralized reconciliation between different exchanges. Overall, the crypto-funds, deposited in the exchanges (by end users to trade), will be stored in the multi-signature addresses opened for each exchange (venue). The shared control and private keys will be held both by the owner of exchange and by the EXPREAD foundation. So, the system applies a distributed control over all funds stored making sure that none of the exchange owners, as well as the EXPREAD foundation itself, does not have access to the funds in impartial basis (layer of checks and balances). Any conflict raised regarding to the access to the funds between the EXPREAD foundation and any of the exchanges will be resolved by the dispute resolution institute integrated into the system.

The ecosystem supports the movement of the funds through periodic reconciliation (every 2 hours) between exchanges, which is based on state channel protocol with integrated peer confirmation system. The whole reconciliation process (elaborated in section 4) is designed to make sure that all nodes have full, independent information about order flow (originated from their gateway) and any manipulation of the order book and trade engine is swiftly detectable. The information about funds flow and final clearance between the exchanges will be available in the blockchain, and totally auditable at a later point.

So, EXPREAD effectively provides decentralized control over the funds deposited in the system with diminishing concentration coefficient as the number of exchanges (venues) increase. The

maintenance of the centralized order book and trading engine makes sure that the exchanges can run sophisticated trading tools, have fast execution (for high frequency traders) and high scalability. At the same time, the whole trading system is fully backward auditable with off-chain peer validated matchmaking and on-chain execution.

3. Economic Rational and Synergy Value Created through EXPREAD Model

The EXPREAD concept is fundamentally based on the fact that there is a significant synergy value in the liquidity aggregation, which is exploited very poorly in the current model of establishment and running of crypto-exchanges. The absence of the underlying framework of collaboration leads to emergence of hundreds of crypto exchanges, which provide isolated pockets of small liquidity, are completely noncompetitive and unable to serve large volume trades. The value loss because of deficiencies of current model is attributable on one end to failure of exchanges to reach operational efficiency and on the other end unsatisfied customer unable to execute the orders with the best price available in the market.

EXPREAD is an open-ended ecosystem, which will provide white-label solutions and unified trading engine technology powered by permissionless blockchain to build exchanges on the top. The exchanges opened in the network (as part of the alliance) are still heterogeneous entities. Each exchange brings idiosyncratic resources and liquidity into the ecosystem, which further furnishes the competitiveness of the total network. The synergy value is derived from higher volume of offsetting orders, deeper market depth, effective price discovery and lower bid-ask spread for the end users. Furthermore, channeling of the order flow will bring much higher transactional velocity to the EXPREAD exchanges, opening much better business prospects both in terms of short term profitability and long term growth rate.

In addition to solving the liquidity problem, the EXPREAD significantly reduces the barriers of entry in terms of initial capital required (to develop the crypto-exchange protocols) and low-supply expertise specialized in ensuring the security. By handling nearly all technology related functions, EXPREAD assists entrepreneurs to focus on compliance and marketing side of the

business, which are proven to have more importance in the space. The multi-venue structure of the system makes sure that the local community and niche market orientated marketing strategies are viable as the EXPREAD exchanges are not bound to have large number of users in both ends (buy and sell) internally to be operational. In other words, the exchange owners can concentrate and leverage their own network, community and existing client base, where they have accumulated trust, to build their crypto-exchange practice¹.

The targeted marketing is only one of the options, differentiation in terms of transaction fees, interface, selection of tradeable tokens, functionality is accessible to make sure that exchanges are also incentivized to compete internally to attract new customers. Considering the sky-rocking expansion of the crypto market as well as dynamic change of the competitive power of the current exchanges we believe that it will take a great amount of time for the whole EXPREAD ecosystem to achieve an internal Pareto state. Therefore, we project, new venues will bring synergy value (added market depth) to the whole ecosystem which greatly outweighs the cost of cannibalization. At the same time, the internal governance mechanism is embedded in the system to make sure that there is no major clustering of EXPREAD exchanges² (see section 8).

4. State Channel Protocol Applied for the Decentralization Internal Clearing

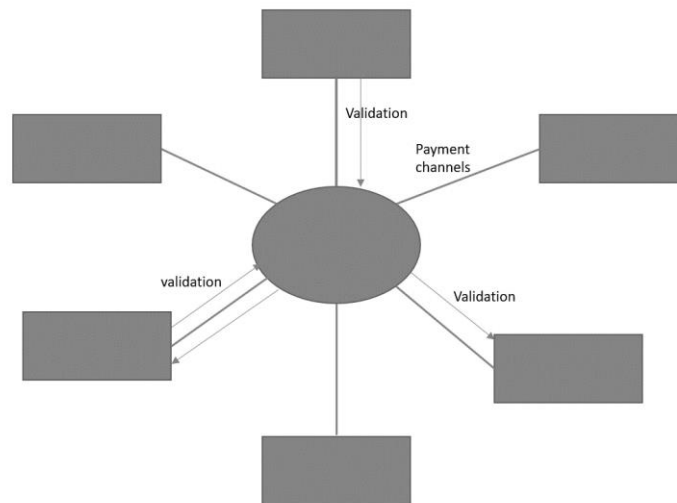
Due to limitations of the blockchain technology for full on-chain order processing and offsetting order flow (high transaction cost, low scalability, etc.)the application of off-chain broadcasting, periodic aggregation of the offsetting transactions and on-chain execution of the reconciling orders is an optimal solution. EXPREAD utilizes a unique application of the payment channel protocol for the distributed settlement of the offsetting orders. Though constructional similarities to the Ethereum based Raiden Network (and Lightning network for Bitcoin) a conceptually new network topology is applied to promote the decentralized interaction between venues. The role of the EXPREAD foundation as a super-node in the system, enabling fast routing and interconnectivity

¹The exchange owners have one out of two private keys of multi-signature addresses (both is needed to access the funds), therefore the credibility of the venue is closely attached to their reputation as well as to the reputation of EXPREAD foundation.

²Further elaborated in section 6.

between the payment channels of all venues, is highly compatible with our underlining business model. Off-chain state transition system is also reasoned potentially back and forth micro offsetting orders between two exchange counterparties, which may bring significant cost and delays if executed on the sole basis.

Figure 4.1: EXPREAD Network Topology



In order to enable off-chain processing of the cross-venue offsetting orders, each of the exchanges in the system has a duplex payment channel with EXPREAD foundation. To support the payment channels, the funds deposited through gateways (venues) are kept in a 2-of-2 multisig addresses (one of them is within channel) with the private keys distributed to the exchange and EXPREAD foundation. Therefore, the EXPREAD foundation serves as an all-time intermediary between all venues in the system, preserving its uninterrupted operation. The functioning of the EXPREAD foundation as a super node has also significant practical implications, as it limits the required number of payment channels to N (number of venues in the system). If network topology had a more distributed structure, it would lead to N^2 open direct payment channels (all venues between each other), which in terms of system management and planning of the minimum deposit requirements, is not feasible. Furthermore, the application sparse graphs (such as Lightning Network) may not be viable as the assumption that there will always be a path (edge between two participants) with enough capacity to execute the reconciliation is a very strong one. If the funds are segregated between different channels there is a high chance that a big order from an unusual partner may deplete the channel interrupting system's operation.

In addition to the role of EXPREAD to path the payment channels between the exchanges, it also acts as a validator in the ecosystem. Overall a three-side validation is applied in case of any reconciliation and offsetting currency movement between the exchanges (validators are the two exchanges and EXPREAD Foundation) and two-sided validation (exchange and the foundation) is applied if the end user is withdrawing money from the venue. So, this mechanism makes sure that even if exchanges are corrupted the EXPREAD has still auditing and validating power to stop the malfunctioning of the system.

4.1 Details on Operation of the Payment Channel System

Overall, the process could be broken down into three main phases, including channel opening, off-chain settlement and on chain execution/dispute handling.

The channel opening phase is repetitive process (followed reopening and closing to withdraw funds). Each of the exchanges has two layers of multisig addresses: one is to deposit(withdraw) user coins and the other is the multisig for the payment channel. These addresses are interrelated, and the funds flow from one address into the other to make sure that before each clearing period there are enough funds in the payment channel to meet the needs of the secure counterparty reconciliation. At the same time foundation has unidirectional payment channel with exchanges (EXC token deposit) to make sure that the exchanges have the comfort to compensate their losses if foundation is corrupted (elaborated on this further below).

The off-chain reconciliation system enables real time transfer of the signed messages to support the cross-venue offsetting transactions, which enables the off-chain and secure execution of the process. This offsetting system itself represents a replicated state machine shared between all the exchanges in the ecosystem. Point to point messaging is applied for the communication between the exchanges and EXPREAD foundation, the messages are bilaterally signed by the white label exchange owner(venues) and the foundation. Therefore, the foundation can act as an intermediary to ensure the safe execution of the on-chain currency movement in the reconciliation period. By design this system does look like a blockchain powered clearing houses, with no leeway for the exchanges to run away from their commitments.

One of the main challenges of protocol with Lightning network is potential operational blackout during off-chain, on-chain round. This is related to the fact that when the system in the phase of on-chain execution, no off-chain transaction can be performed, which is not sustainable in case of EXPREAD platform. To handle this hurdle, we apply incremental deposit system offered by the Spirit channel protocol (A. Miller, I. Bentow, etc.), which allows partly withdrawal and depositing of the money in the payment channel.

The interface of the payment channel system is highly user friendly for the white label owners, and does not require technical background. The EXPREAD foundation is founded to serve and support all the message transfer processes and final settlement, the system offers a confirmation layout for decentralized verification of orders and control over what is validated on-chain. The venues can delegate the verification function of in-chain broadcasted transactions to third party effectively ensuring that they have all checks and balances over the operation of their exchange.

To sum up, the core of the whole system is the creation of right level of internal controls to enable secure implementation of the fund's flow. On the reconciliation and money transfer requests a bounded time requirement will be applied to avoid the breaks of the functioning of the whole ecosystem, if any of the avenues goes off-line for any reason (so it cannot validate from their side).

The uniqueness of the system is that in game theoretic way it is effectively trustless from the side of all participating parties. As all exchanges as well as the foundation has the chance to influence the transaction value if the other party misbehaves.

$$1. (E1(X1 \ggg F) \cup E2(X2 \ggg F) \rightarrow F(X2 \ggg E1, X1 \ggg E2) \rightarrow OK$$

$$2. (E1(X1 \ggg F) \cup E2((X2-1) \ggg F) \rightarrow F(E2(X2) \ggg F) \rightarrow F(X2 \ggg F1, X1 \ggg F2) \rightarrow OK$$

$$3. (E1((X1-1) \ggg F) \cup E2((X2) \ggg F) \rightarrow F(E1(X1) \ggg F) \rightarrow F(X2 \ggg F1, X1 \ggg F2) \rightarrow OK$$

$$4. (E1((X1) \ggg F) \cup E2((X2) \ggg F) \rightarrow F((X2 - 1) \ggg F1, (X1-1) \ggg F2) \rightarrow E1((F(T) \ggg E1) \text{ and } E2((F(T) \ggg E2)$$

$$5. (E1((X1) \ggg F) \cup E2((X2) \ggg F) \rightarrow F((X1),(X2)) \ggg Z) \rightarrow (T, T) \ggg E1, E2$$

Where: \bigcirc podcasting the function inside

F refers to foundation, E refers to Exchanges, Z refers to some third-party address

\ggg refers to the send transactions

\rightarrow moving to the next step

T refers to deposited funds (EXC token) by the Foundation

The system leverages on-chain dispute resolution process inherent to the Lightning Payment Channel. As there is time-flag integrated into the transaction code, the counterparties (in this case the exchanges and foundation) have time to change the transaction outputs if the other party broadcasted wrong outputs (the messaging ensures the parties can do that). At the same time if foundation misbehaves the exchanges can unilaterally broadcast movement of the EXC token to their address. Therefore, the whole system looks like close cycle where none of the players have incentive to misbehave, effectively decentralizing the whole process.

5. Backward Auditability of the Order Book and Trading Engine

Full backward audibility of order book and trading engine by all venues, is a key security measure, to make sure that the foundation has not anyhow manipulated the order book in favor of any of the parties. Considering that each of users have full info on the broadcasted common order book and each of the venues has full access to the order flow from their gates, the process is quite straight forward. Several assertions, such as order accuracy, timing could be easily covered as exchanges have full independent information about the order flow from their end. Each of the orders in the system has a unique id, therefore, the venues could easily search in the system, whether that specific order has been registered in the unified order book with the right amount and time. Other assertions such risk of inflated order book, “dark pools of liquidity” and well-functioning of trading engine will be performed through formal internal audit procedures. Two main audit functions are integrated into the software: to check full completeness (no inflated) of order book and to back test the proper functioning of match making engine.

To check audit assertions and at the same time to keep the confidentiality of the order flow from the gate of specific exchanges, Enigma engine (<https://www.enigma.co/>) or a centralized cloud-computing system (less secure) may be applied. Each of the venues will submit to the Enigma platform (decentralized data computation) info about their orders (for each cryptocurrency) with the timestamp. The system performs computation through simple, systematic algorithms encoded by the

EXPREAD foundation and provided fully open source. The two assertions the formal audit is addressing are the completeness of the order book and the accuracy of the trading engine.

In terms of completeness, the audit procedure makes sure that all the orders submitted through all venues have taken their place in the unified order book. One of the possible ways to checkup the order book is through characterizing its frequency distribution (of the order size to buy and sale independently) in terms of its moments. If the order size series has moment generation function simple computation may be performed. The function may change from period to period, and is one of the statistical information which is provided to the owners of white label exchanges and can be easily verified as they possess the full info about the broadcasted unified order book.

With the existent moment generating function, the number of moments is finite and can be computed as:

$$E[X^n] = \frac{d^n F_x(m)}{dt^n} \Big|_{m=0}$$

where $F_x(m)$ is the moment generation function,

$\frac{d^n F_x(m)}{dt^n} \Big|_{m=0}$ n-th derivative of $F_x(m)$ in terms of m, m evaluated at the point m=0

Though even in case of absence of the moment generation function (such as due to undefined moments), the first 6 moments should cover the major aspects of the distribution. Therefore, if these moments of the unified order book are matching with computed moments of joint distribution (data on separate distributions is imputed by exchanges to the Enigma system), we can reasonably conclude the order book is complete.

As a sample, we can use student F-distribution to characterize the series (a good approximation considering that order size cannot be negative and there is potentially long right tail). The distribution does not have moment generation function, the distributed function can be formulated as:

$$F_x(x) = \frac{1}{B(\frac{n_1}{2}, \frac{n_2}{2})} \int_{-\infty}^{k_1 x / k_2} s^{n_1/2-1} (1+s)^{-\frac{k_1}{2}-\frac{k_2}{2}} ds$$

Where the k_1 and k_2 are the degrees of freedom (of chi-squared dis.).

So, overall the algorithm will be expressed as:

if

$$E[X] = \frac{k_2}{k_2-2} \text{ for } k_2 > 2$$

$$(E[X^2] = Var[X] = \frac{2k_2^2(k_1+k_2)-2}{k_1(k_2-2)^2(k_2-4)} \text{ for } k_2 > 4) ! = \begin{matrix} \text{Moment 1} \\ \text{Moment 2 to} \\ \text{Moment 6} \end{matrix} \rightarrow \begin{matrix} \text{Complete} \\ \text{Order Book} \end{matrix}$$

.....

$$E[X^n] = \left(\frac{k_2}{k_1}\right)^n \frac{\Gamma(\frac{k_1}{2} + n) \Gamma(\frac{k_2-2n}{2})}{\Gamma(k_1/2) \Gamma(k_2/2)}$$

*For the other moments from 3 to 6 apply equation above.

To cover the trade engine accuracy assertion, the system may apply random sampling on the population of filled orders (each order in the system has its unique id) and track whether offsetting order have been the best order (timewise and pricewise) in the system. The sample size is determined as follows:

$$n = \frac{Nz^2 * 0.25}{[d^2 * [N - 1]] + [z^2 * 0.25]}$$

Where n – required sample size

N – population size

d- level of precision

z - z score of confidence level

All the audit procedures are integrated into the software (open source for venues) and will be performed automatically and periodically without much effort.

6. Procedure of Opening a Venue and Description of the EXPREAD White Label Solution

The white label solution provided by the EXPREAD is one of the novelties, effectively positing EXPREAD as the first crypto-exchange white label provider in the market, with unified liquidity pool. EXPREAD provides a scalable technology designed to cater the needs of the owners of exchanges, allowing to apply full branding into our ready-to-use technology. All white labels will be accessible from every device. In addition to using one of our templates the exchange owners can build their own UI on the top of the EXPREAD system. The solution provides easy integrable open APIs to new venues on risk management, messaging system for the off-chain transactional confirmations, customer on boarding, KYC system, audit trails, etc. In the backend, the white labels are attached to the trading engine, which conducts automatic processing and routing of the orders, matchmaking and registry. The venues pay maintenance fee for cloud-hosting of their operations, which is powered with backup process and contingency planning. As all charting solutions as well as functional systems are hosted directly by the EXPREAD foundation, it ensures centralized and fast software updates and maintenance. To make sure there are no operational difficulties within whole EXPREAD network, the EXPREAD foundation provides 24/7 IT service desk.

Furthermore, the system charges the transaction fee on the orders entered and filled as a source of revenue for white label owners (orders inputted from their gateways), based on their specifications. The all packages of the trading features (described in the next section) come already integrated into white labels with periodic upgrades, which can be activated through subscription plans. The composition and distribution of menu bar on the terminal are highly customizable. The functionality depends on the payment plan the owners have chosen; the display of the menu has fixed-layout, where the owners select which features on the menu list to activate. Exchange owner can easily add advertising, educational and other content into the platform to meet the customer needs.

The branding flexibility is one of the main focuses of the system. The UI of white-labels provided in the system is made of different components, which can be independently customized through coloring and distribution in the interface. This allows the owners of exchange dynamically experiment with the design and branding to come up with something that is attractive to their target market.

When it comes to the management of user information, as well as registry of the user identification details, the system is designed to offer a stand-alone operation, with full view and management accesses provided only to the exchange owners. In addition to live accounts, the EXPREAD is also considering to allow functionality of registration of the demo trading accounts for

new users as another section of signup form(JavaScript). It will enable users to get a better understanding how the crypto market behaves in test mode.

The Settlement Notification System, designed as push notification to trigger owner's approval for the off-chain signed messaging to the foundation, is developed to support the off-chain payment channels system. The messaging is performed through file transfer with high level latency and security attached.

To commence the process of establishment of EXPREAD exchange the initiation team should submit an application package to the EXPREAD Foundation. The due diligence is one of the main components of the application process, which involves EXPREAD foundation going through all the documents submitted by the team, such as description of the team background, targeted marketing policy, the license of the legal operation of exchange (if required in a particular jurisdiction), the names of shareholders, etc. Independent third party is involved in the due diligence to verify that the team is credible background, and is independent from the EXPREAD foundation (relationship audit) to effectively mitigate the collusion risk between an exchange and the foundation.

If team successfully passes the due diligence exchange establishment procedure gets initiated. The team pays the initiation fee, which is used to set up the layout, connect to cloud, set up on-chain settlement protocol, train team to use the technical systems, etc. After the application is approved the set-up timelines is specified and technical execution is initiated. The whole process from application to approval should not take more than 2 weeks, and technical set up takes another two weeks. The whole process, therefore, is designed to take less than a month, which is the fastest crypto-exchange foundation process available in the market, from the business initiation to execution.

7. Description of the Trading Tools Provided by EXPREAD

The provision of a vast optionality of the technical analysis and automated strategies toolbox is one of the key value propositions of EXPREAD system. The system is designed to equip traders with exceptional insight into their trading operations across all crypto assets. The exchanges(venues) can activate certain toolkits from their terminal through semiannual subscription fees (application of

more tools leads to higher subscription fees). Though each venue can select to apply whole package of the tools, we anticipate that they will make strategic choice based on the market (institutional, private, etc.) needs they are aiming to cater. Such flexibility of the functional choices enables exchange owners to plan and gradually increase their functional offerings in conjunction with the evolution of the exchange in its lifecycle and the growth of the user base.

The standard package provides (I) Powerful market visualization, (II) Charting, (III) Multi-time frame and multi-instrument analysis and (IV) Over 5 pre-built technical indicators. The full package of toolkits involves following tools and functionalities:

- Live and Customized Quotes: More comprehensive, all-inclusive data on price, market depth, volatility measures with state of art charting layout.
- Technical indicators: Over 20 technical indicators designed to cater the needs of demanding technical traders. The package includes Oscillators (Advance/Decline Ratio Hourly, Advance/Decline 2 Day Momentum, etc.), Trend Indicators (Moving Averages, MACD, etc.) and Breadth Indicators (Up/Down Volume Ratio, Force Index, etc.).
- Personal Accountant: Access (from user account) to the micro accounting system, which provides analytics of ongoing as well as past performance. The matrixes provided include P&L of all the positions took, Average Maximum Favorable Excursion, Average Maximum Adverse Excursion (charting provided), assets (currency) held, performance variance, etc. In the risk level window, traders can drilldown their cumulative exposure by any attributes, such as coin, public chain, country, etc.
- Portfolio Management Tools: Sophisticated portfolio management toolbox with integrated portfolio construction, back-testing and optimization tools. The user can create live as well as mock portfolios in the system and compute the portfolio performance (return, variance, sharp ratio, correlation matrix, etc.) based on the selected time horizon. The optimization tool, automatically calibrates the positions of the selected coins to optimize the portfolio per user specification (highest Sharp Ratio, lowest variance, etc.). The optimization wizard may also be applied to derive portfolio choices for a segment of historical data (with optimization) and use other segment of historical data to strategy efficiency testing.
- Custom Smart Orders: high level functionality to set custom orders (including market, limit, stop market, stop limit orders) with integrated cross-coin and volume-based triggering. In addition to the standard market & limit orders, the users have optionality to set triggers (to buy or

sell) for one coin if the other coin's price touches the predefined level (insight about lag relationship between coins can be leveraged). In his strategy, the user, also may define volume triggers (specific size of order volume triggers the trade). All the functionality is highly user friendly designed for average customer.

- Smart Market Alerts: Set customizable alerts to identify trade triggers. The alerts may be applied also on the net exposures assisting traders to reposition their portfolio to stay in the target coin exposure range.

- Analyst Portal: Unique system that enables the crypto analysts to advertise their services, get subscribers and sell reports. Analyst Portal is designed to make the EXPREAD trading terminals one-stop place to learn and make smart investment decisions.

- Read only Newsfeeds: In terminal, traders can get short feeds from leading crypto news platforms. Furthermore, through the system venues have optionality to hire the news writers as well as other content generators to provide more value-added services to its customers. The open ended, interactive structure (with multifunctional add-ons) of the platform enables the white-label holders to differentiate themselves from the competition.

8. Business Model for the Exchanges Opened in the EXPREAD Ecosystem

As mentioned in past sections, the unique way of marketing cryptocurrency trading platform through community-orientated exchanges is an efficient way to increase the customer base as well as the liquidity of the system. It enables better security and scalability while maintaining decentralized control and governance principles. This model addresses the market segregation problems creating a net of exchanges that will be connected synergistically, providing support and sharing of resources for expansion of EXPREAD ecosystem. The economic incentives and governance mechanisms introduced through EXPREAD intends to create a cooperative, transparent and interconnected community which promotes the collaboration to achieve aggregated success.

In terms of revenue stream, EXPREAD system provides white label owners the functionality to pick a pricing model (from available alternatives) based on market environment, targeted customer

base, location specific characteristics and competition. It is assumed that at different stages of the business lifecycle, the exchanges will apply diverse pricing strategies to stay competitive and enable the business growth. The pricing applied is registered in the EXPREAD system, and the transaction fees charged from an order will be based on the price marketed by the exchange at the point of order origination. The venues will be able to change the transaction fee schedule dynamically (if announced and disclosed timely). Furthermore, the system allows venues belonging to the EXPREAD network adopt varying pricing models to foster healthy competition (from available alternatives). The available pricing models for venues will be ranging from flat fees, dynamic pricing strategies to flexible fee scheduling such as percentage based, volume based, tiered subscription based models. The discretion allowed to change the transaction fees applied in the system is provided to the exchanges within some limits. From game-theoretic perspective the runners of the exchanges should not go into price competition (with EXPREAD) as it will deteriorate their own earnings, and, at the same time, they should compete as an aggregated ecosystem with the external exchanges.

8.1 Lending Scheme in EXPREAD Ecosystem

The network effect among EXPREAD venues will be utilized additionally through an in-house lending scheme that exists between operating venues for strengthening their presence in a market, as well as directed to promote fast growth of new exchanges. The in-house lending module will allow the EXPREAD network participants to borrow and/or lend funds directly to one another through an online EXPREAD platform without the involvement of any outside financial intermediary, under the conditions of clarity, predictability, transparency, higher efficiency, auditability to enable EXPREAD ecosystem to leverage its collective strengths and acquire a higher aggregate market share. It will offer higher risk adjusted returns for the investors, lower interest charged from borrowers, more efficient technology utilization, innovative risk management system, etc. The lending within EXPREAD ecosystem will reduce the costs by eliminating many operational expenses and some of the cost savings will be passed along to borrowers (and investors) through lower interest rates (and higher rate of return).

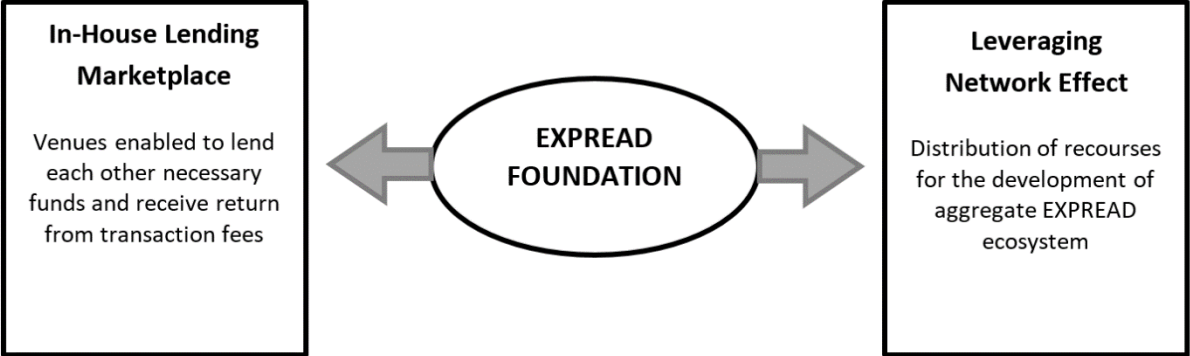
As a return on the provided capital the lenders receive a share of transaction fees earned by the borrower (an exchange). The settlement will be carried out through EXPREAD core to ensure compliance of borrowers. The in-house lending system allows the network participants to raise

necessary funds without credit rating and collaterals, which is the main difference from external fundraising sources. Lenders have access to view the business details of borrowers (team background, execution plan, current performance, etc.); furthermore, they will have the optionality to provide funds in bundles or in cooperation with other lenders. The auction based approach enables borrowers to find the best offer considering the terms of the loan.

- **Fewer Fees:** The EXPREAD lending scheme will require less overhead, lower administrative costs, will enable successful venues to maximize their profits through lending it to existing or new EXPREAD exchanges that need the capital for starting or speeding up their expansion. Lenders receive a certain percentage (from 5% to 100%, agreed by parties for some period) of the future transaction fees charged from customers by the borrower venue.
- **Time:** The lender will distribute the loan to the borrowers within minutes or a day after review and approval of the in-house loan application, enabling fast processing and fund distribution (utilizing the EXPREAD infrastructure).
- **Efficient Processing:** The platform will require less documentation than a traditional bank or credit union making the loan processing considerably easier for the borrower, and will enable a backward auditability as transparency assurance for the lenders.
- **Auditability:** The lenders of the funds will be allowed to request EXPREAD foundation to conduct an external audit on the borrower venue, for examination of efficiency of fund allocation and its correspondence to initial agreement.
- **Transparency of the system:** Transparency of platforms is executed through uniform and clearly disclosed loan terms to ensure long-term maintenance of trust among the counterparties, and elimination of additional unnecessary inefficiencies and hidden terms.
- **Investment terms:** The lending module will allow different arrangements for the lenders to structure their landings, for minimizing their risks (diversification through lending multiple exchanges) and distributing the necessary funds through several funding rounds based on historical and real time financial performance of the borrower venue.
- **Network effect:** Successfully funded and duly executed projects reinforce the network effect of the EXSPREAD, encouraging further cooperation between different venues, liquidity

provision in times of stress and a safety net that can be leveraged for a higher aggregate market share of EXPREAD ecosystem.

Figure 8.1.1 Internal Lending Marketplace

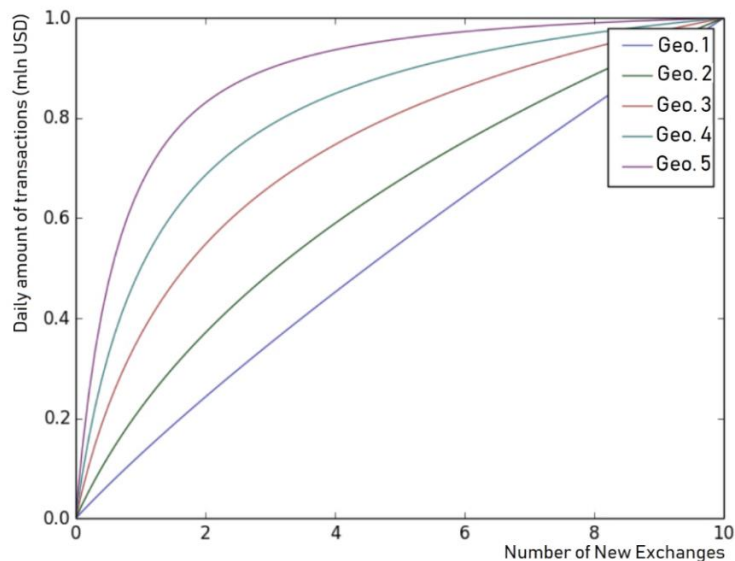


8.2 Geographical Breakdown

In order to protect exchanges/venues in the EXPREAD system as well as to enable demographically balanced development of the whole ecosystem, continuous benefit-monitoring function will be applied in the system. In the scope of this function, the whole crypto exchange market will be divided into 25 geographical segments (the list will be available on the website along with details of exchanges in the continuous basis). At each point for each of the geographical segment the total user info, number of order and transaction volume will be recorded.

For every new exchange/venue opened in a particular geographical segment the number of new users as well as old users (who switched venue) will be recorded for better assessment of market condition. If the system detects a high amount of cannibalization between two EXPREAD exchanges it may lead temporarily (or permanent) suspension of registration of new exchanges in the particular geographical area. Overall, per geographical area the demand function may have following marginally diminishing functional form:

Figure 8.2.1 Elasticity of the demand in geographical area to the number of exchanges



The elasticity of the daily transaction size to the increase of the number of exchanges in different geographical locations will be different (see Figure 8.2.1, for the five exchange locations). In order to monitor the potential cannibalization between exchanges, the geographical segregation is performed based on the intensity of existing competition in the same country's territory and relatively low competition in proxy locations (such as in a third country where the exchanges are not located).

The calculation matrix will be calibrated in a way to enable the solution of the optimization problem of the cannibalization cost (CC) and the expansion benefits (EB) of the local EXPREAD ecosystem. The cost of the cannibalization is defined by the transaction volume of old users, which get acquired by the new exchanges (in the same location) if KYC is performed in the country, or in terms of loss of transaction volume in a particular exchange (after the entry of new competitor exchange in the same location). The benefits are defined by the growth of the transaction volume in total local ecosystem after entry of the exchange. To optimize the process, the calculation formula assumes that if the marginal cost of cannibalization of the last exchange in the segment (MCC) is more or equal to the marginal expansion benefit (MEB), the registration of new teams targeting that particular geographical segment (e.g., country, region) will be suspended or permanently stopped.

$$MCC = \frac{dCC}{dN} \geq \frac{dEB}{dN} = MEB$$

Where, N – is the number of the exchanges in the geographic segment.

The central monitoring is needed to ensure that exchanges, which join the network targeting specific demographic and customer base, do not lead to the cannibalization of other exchanges, but rather are focusing on engagement of the original clientele.

9. Economic Model of the Token and Governance

The system through its economic model of the token is designed to promote the development of EXPREAD creating a significant pull mechanism for the venues as well as to assist decentralized and user influenced governance of the ecosystem. In general, the functionality of the token is divided into three main elements: user specific utility, internal currency in the ecosystem and governance apparatus.

From the side of the end user, the token (EXC) provides a significant discount on the exchange transaction fees, which yields significant utility to the customer in case of both high frequency as well as large volume trades. The discount model applies simple machine learning process to optimize the trade-off between fast payback/high profitability for the white label holders and considerable discount benefit on the transaction cost for token holders. The discount is determined by the size of the token holding and may reach 100% if a specific number of tokens is possessed by the holder. As supply of the token will be highly limited (21 million), the demand and utility of the token will increase with the liquidity of the ecosystem and depth of aggregated order book. Therefore, the early movers will get significant value in terms of discount earned.

The second benefit for external token holders is that token provides an access to render services to the different venues (exchanges) as well as EXPREAD ecosystem in general. The services can range from selective news feed generation for the exchanges to writing crypto-related reports and investment advisory papers. The services also may be related to meet more venue-specific needs such as design modifications, advertising, promotional programs, etc. On the website of the EXPREAD

foundation there will be specific section for the outsource job postings (by different venues) to assist the token holders to get involved in the community.

In addition to the discount benefits, the token also represents the internal currency of the EXPREAD ecosystem. The payment of the maintenance fees, subscription payments to unlock further functionality in the terminals, internal flow of resources between exchanges (through venue to venue lending) will be executed using the token of the platform. Furthermore, the compensation to the external users for the rendered services will also be executed using EXC token.

As mentioned above the EXPREAD ecosystem is aiming to adopt a user-influenced governance in its hybrid system. The EXPREAD foundation has strategic functions in terms of governance, such as coordination of the operation of exchanges and ensuring the development of the total ecosystem. In terms of more functional, protocol specific decisions the owners of exchanges as well as token holders have significant influence. The governance process operates through nomination of the upgrade proposals and voting performed by the token holders and venues. Only owners of exchanges, EXPREAD foundation and limited number of token holders (with significant token holding and vested interest) have the functionality to nominate proposals for public discussion and vote. All token holders can participate in the voting process to determine the best proposals for the ecosystem.

Another uniqueness of EXC token is the distribution mechanism in the post-ICO stage (there are tokens allocated on the distribution for the promotional purposes). The mechanism embedded for the token distribution is called “proof-of-trade”. In terms of distribution of the tokens, it is similar to bitcoin protocol (12.5 EXCs distributed every 10 minutes) with diminishing allocation(pegged to the bitcoin distribution schedule).

From the perspective of individual customers, the distribution of the token is dependent on the trading volume (of a user), total trading volume of the whole ecosystem and the index of venues used for posting the order.

$$\text{Distribution to an end user} = \frac{\text{ex.Index} * \text{user trading volume}}{\text{sum}(\text{trading volume of the exchange} * \text{ex Index})}$$

Where:

- User trading volume and trading volume of the exchange are determined based on all crypto trading conducted (nominated in EXC token).
- Ex Index is the characteristics of the particular gateway used.

Periodic indexation of exchanges will be conducted to differentiate them in terms of their length of the involvement in the EXPREAD ecosystem. The newly established exchanges enjoy some preferential treatment when it comes to the distribution, providing higher distribution to their users. This approach is adopted to promote the development of new venues.

Bibliography

- [1] Sprites and state channels: Payment networks that go faster than lightning, Andrew Miller, IddoBentov, RanjitKumarsen, etc., 2015.
- [2] The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, Joseph Poon, Thaddeus Dryja, 2016.
- [3] How to use bitcoin to design fair protocols, IddoBentov, RanjitKumaresa, 2014.
- [4] An open protocol for decentralized exchange on the Ethereum blockchain, Will Warren, Amir Bandeali, 2017.
- [5] A fast and scalable payment network with bitcoin duplex micropayment channels, Christian Decker, Roger Wattenhofer, 2015.
- [6] Electronic Communication Networks and Liquidity on the Nasdaq, James Wetson 2002.
- [7] Trade classification algorithms for electronic communications network trade, BidishaChakrabatry, Bingguang Li, VanthuanBguye, Robert Ven Ness, 2007.
- [8] A fast and scalable payment network with bitcoin duplex micropayment channels, Christian Decker, Roger Wattenhofer, 2015.