LEVERJ

DECENTRALIZED LEVERAGED EXCHANGE

CONSENSYS

Technical Adviser

LAST UPDATED: 2017-11-22

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

INTRODUCTION

Derivatives trading is the largest market in the world at an estimated 1.2 quadrillion dollars[1], with a current growth rate of 30% per year[2]. The cryptocurrency market is growing at an even faster rate, and is eager for a full derivatives ecosystem that exists within the traditional financial systems. Current growth in centralized cryptocurrency derivatives exchanges, which is at $1 billion daily notional value[3], indicates massive potential for the industry.

PROBLEM

Traditional finance is bogged down by heavy regulation, excessive cost and censorship, among other issues. The cryptocurrency world has inherited some of these failings and added a few of its own, including counterparty risk, account security, identity protection, exchange centralization and exchange instability. Taken together, these points of friction make it inefficient and suboptimal.

OPPORTUNITY

Blockchain based financial systems challenge the status quo by providing censorship resistance, non-repudiation, counterparty risk reduction, and many other desirable properties to financial contracts. **Cryptography and game theory offer an opportunity to build regulatory benefits into blockchain products.**

A trading system has efficiency and risk management requirements that make it usable and practical; however, these requirements are currently only satisfied in centralized systems. Current decentralized exchanges are unsuitable for trading and barely acceptable for hedging risk. Leverj aims to satisfy the requirements for practical trading in a decentralized system by implementing a distributed exchange protocol executing off-chain, yet verifiable on-chain. By supporting derivatives contracts, classical hedging strategies can be combined with financial applications on Ethereum. The degree of centralization may be tunable without compromise of the distributed nature of the protocol. This leaves room to explore decentralized variants of initially centralized algorithms, both of which remain distributed.

CHALLENGES

Efforts to establish markets for leveraged cryptocurrency derivatives have focused on centralized exchanges that traders must trust as the custodians of their funds. In an environment where even the biggest (Bitfinex) and most security conscious (Shapeshift) exchanges experience loss of funds to hacking, a focus on security using blockchain and cryptography becomes imperative.

While decentralized exchanges are nothing new, most of them offer poor user experience, low liquidity, and scant traction. Most of these systems subsequently fail to be adopted at scale.

SOLUTION

Leverj decentralizes the most security critical features of derivatives trading by implementing them in smart contracts. Leverj focuses on derivatives trading and the supporting ecosystem. We plan to build an ecosystem of features that will enable institutions to move into the cryptocurrency world.

---

[1] http://www.bis.org/statistics/d1.pdf

[2] http://www.bis.org/publ/qtrpdf/r_qt0712.pdf

[3] https://coinmarketcap.com/currencies/volume/24-hour/

2. THE LEVERJ PROTOCOL

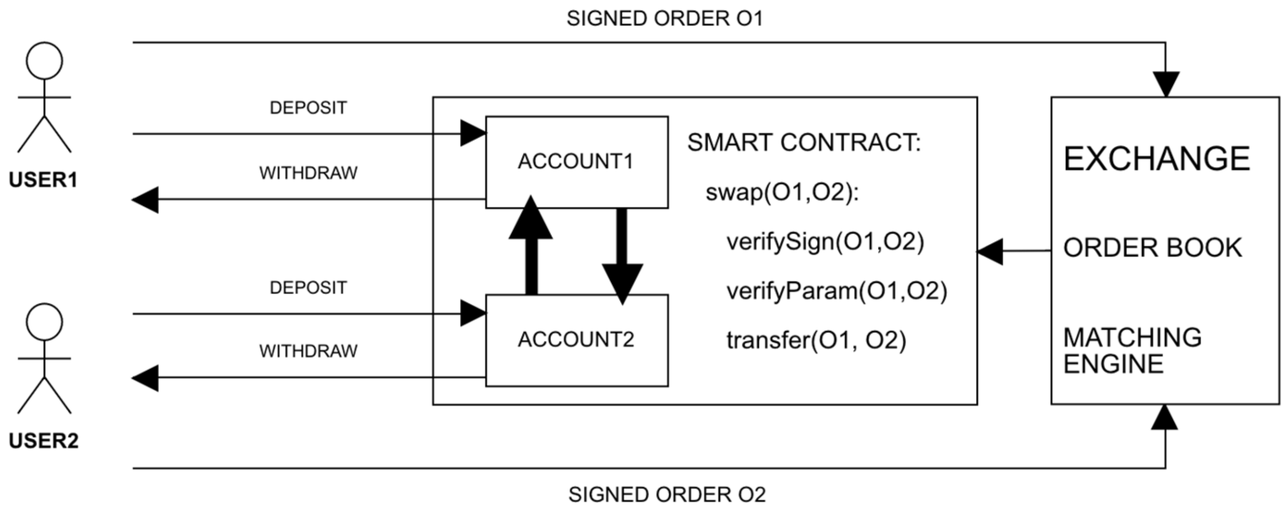


Fig 1. Leverj Protocol

Leverj consists of on-chain Custody and Staking contracts along with an off-chain centralized order book and matching engine. The exchange provides various aspects of the trading experience the user interacts with such as a UI, API, integration with other platform services, etc.

SEGREGATED ACCOUNTS

Custody contract implements the non-custodial model of Leverj. Its purpose is to hold funds and ensure that only the owner can deposit or withdraw from it. When a user deposits into the smart contract (1), Custody allocates any tokens or ether received against the sending address and enables withdrawal only up to the balance an account holds. This ensures that its not possible for any malicious actor to take control of all the funds.

ORDER BOOK AND MATCHING ENGINE

Order book and matching are centralized and are off-chain. The order-cancel-match critical path is optimized for speed and are designed to not depend on the blockchain.

The user signs orders with their private key and sends orders to the exchange(2). This ensures that the key that controls the account is the same key that authorized the order or other operation. The updated order book is streamed to all users off-chain like any other centralized order book. As orders are matched, executions are also streamed to all users. Executions are periodically synced(3) to the blockchain. The Custody smart contract verifies the integrity of the fills and updates user balances(4).

To ensure any pending executions are synced and balances are updated, withdrawals are gated by the Exchange. The user submits a signed request to the exchange, which ensures there are no open orders or unsynced transactions and submits the request to the Custody contract. However after 10,000 blocks of inactivity, the user can withdraw directly(5) from the Custody contract even without exchange involvement.

STAKING

Custody contract accumulates fees and sends it to the Staking contract. The staking contract periodically calculates the allocation for everyone based on the amount and duration of the stake according to the staking formula. Staking generates new tokens as needed. Fees paid in ether are sent to the owner of the staking contract (Leverj) and the appropriate amount of FEE is generated and distributed.

ATTACK VECTORS

There are two main kinds of attack on custodial models. The first is the heist, where a significant portion of the funds is taken at once. The attacker does not expect to be able to repeat the attack and would generally not care if the theft is detected immediately. The second is skimming, where small amounts of funds are taken repeatedly over a longer duration. The attacker generally would like to go undetected since repeating the attack as many times as possible is key to a big payout. Our model aims to provably prevent heists and prevent or detect most types of skimming using fraud-proofs.

PREVENTING HEISTS

For heists to be possible, the possibility for one person to control all coins in custody must be possible. Segregated accounts that only enable the depositor to withdraw only their own balance eliminate this possibility, since the attacker would now need the keys of most users of the platform. Ensuring that the user's keys are never sent across the network is also a fundamental requirement for this to work. Therefore all authentication must be using public/private keys only. Password or other shared secrets should never be used.

TRADING SETTLEMENTS

Movement of assets between users as part of trade settlement requires that both users sign the amounts and price they are ready to exchange. Although the exchange performs the match, the custody contract transfers assets after verifying user signatures and integrity of all changes. Executions need to meet specifications set by both users according to the signatures from their private key for the smart contract to move assets among users.

MALICIOUS USER

Since the only avenue to extract assets is via a user account, a compromised exchange would have to set up a malicious user and collaborate with it to move all assets into that user by supplying data in a way to overcome the checks of the custody contract. Since all executions need signatures from users and executions without assets backing them would be rejected, the exchange would have to rearrange existing legitimate orders to favor the malicious user. These can only occur in small pieces and are skimming attacks.

PROTOCOL

Instead of matching peer-to-peer, users can submit their orders to one or more matching entities (exchanges), which can do the matching and submit fills to the smart contract.

PROTOCOL SPEC

1. User deposits into segregated account on Custodian
   a) User ui deposits asset ti into his segregated account Ai from Ethereum address ei
   b) Custodian updates user balance of ti for Ai
2. Exchange updates balance of Ai after N confirmations enabling trading of new balance
3. User ui submits signed order [illegible]i with signature [illegible]i
4. Exchange validates order [illegible]i against signature [illegible]i
5. Exchange countersigns order [illegible]i with signature [illegible]i and returns to user ui
6. Exchange updates order [illegible]i in order book

7. Exchange matches orders □1 and □2 to creates execution □i
8. Exchange periodically submits execution set □ to custodian
9. Custodian processes execution set □
   a. Custodian verifies user signatures □1 and □2 and execution parameters (price, quantity, expiration, etc.) against orders □1 and □2 for each □i in
   b. Custodian settles asset balance between users u1 and u2 of matched orders
   c. Custodian ensures integrity of all asset balances ensuring all assets add up
10. User ui initiates a withdraw request of n ti from his segregated Account Ai
11. Custodian moves n ti to user's Ethereum Address ei
12. Fees if any are moved from Custodian to a staking contract. There is never any assets flowing to Exchange. All FEE and ether move to the staking contract, which generates and allocates FEE tokens as needed.

PROTOCOL SECURITY

The exchange cannot synthesize or alter orders with the signature of a legitimate user and the protocol constraints prevent catastrophic theft. A compromised exchange however may collude with and favor a malicious user using a variety of skim attacks. To favor a colluding user, the exchange would need signed orders from victim users which would be filled at an adverse price. Since the exchange cannot synthesize or alter orders, it may try to manipulate legitimate orders to use them for victimization. Note that even a coarse expiry time on the orders greatly reduces the impact and detection burden of the attack. Note that this is not a comprehensive list of all possible attacks but a framework to quickly address them by quickly adding fraud-proofs when a new defect is discovered.

REPLAY ATTACK

A simple way to synthesize a victim order is to simply remember a past order and use it when the price is adverse for the victim. The exchange simply duplicates an order and fills it at a price favoring a colluding user. Custodian contract prevents replay attacks by the tracking order ids of all matched orders and rejecting duplicates.

CANCELLED ORDER ATTACK

A variant of the above is when the exchange simply fills an order that was cancelled. Storing cancelled order ids in the smart contract is impractical, since cancels are numerous and cancellation need to be fast. However, proof-of-cancellation (exchange signature on cancel request) can be used as a fraud-proof that can be submitted to the Custodian. The custodian can verify that a cancelled order has been filled and halt the exchange.

PRICE-TIME PRIORITY VIOLATION ATTACK

Even non-cancelled orders can be used for attacks by simply withholding them from the order book and waiting for an adverse price movement and matching with a colluding user. Such violations can be detected by the user using price-time fraud proof: an execution exists for an order with a better price but later timestamp than the victim order.

NON-ACKNOWLEDGEMENT ATTACK

An exchange may refuse to accept legitimate orders from a user due to operational policies such as rate limiting or network issues; these do not produce fraud-proofs. In contrast, a non-acknowledgement attack occurs when the exchange takes a user's signed order and instead of replying with its own signature, saves the submitted order for skimming. It then waits for the price to move and then matches it at an unfavorable price, siphoning profit to a colluding user. If this happens, a user can detect immediately when he sees one of his unacknowledged orders filled. The fraud proof for this is the same as the price-time fraud-proof.

SUPPRESSED EXECUTIONS ATTACK

While executions cannot be synthesized or duplicated, they can certainly be suppressed, enabling a compromised exchange to simply suppress losing trades of a colluding user from being synced to the smart contract and withdrawing funds while the smart contract is still in the stale state. This is a variant of TOCTOU attack[4]. Users who observe withdrawals being processed while the Custodian is in a stale state can submit a fraud proof preventing the attacker from withdrawing.

MITIGATION OF SKIM ATTACKS

The exchange would need to sync executions to the smart contract containing a fraudulent execution before the assets can be withdrawn. The syncing will cause anyone monitoring the executions to detect the anomaly instantly and submit fraud-proofs as described below, preventing the attacker from stealing funds.

A compromised exchange can rearrange orders that flow into and executions that flow out of the matching engine. There are four possible rearrangements: suppress, pass faithfully, duplicate and reorder (i.e., pass after a delay)

There are two possible order operations: Cancel and create. Updates are simply cancel and create.

Faithful passes are not attacks, so we have the following attack matrix:

	Suppress	Duplicate	Reorder
Order Create	Non-Acknowledgment	No effect	Cancel Order Attack
Order Cancel	Non-Acknowledgment	Replay	Price-time Priority
Execution	Execution Suppression	Prevented	No effect

Table 1. Combinatorial attacks on leverj protocol

All these attacks are described above and have fraud-proofs that can be submitted to the Custodian contract to disincentivize skimming attacks.

4 https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use

PRICE-TIME PRIORITY

For a compromised exchange to skim from the user, it would need to violate price-time priority. This can be detected in most cases.

Consider the order book at time t0 and t1. Prices above spread are asks, ones below are bids. Price moves adversely to bid o1. An adverse move would have to put an ask below the victim bid for skimming to be profitable.

t0	t1
302	
301	
300	300
(spread)	299
298(o1)	298(o2)
297	297(o3)
296	(spread)
	295
	294
	293

The exchange holds victim bid order o1 at 298 and waits for an adverse price move. It then sells into the victim's bid with its own ask o2 at 298 and buys from a bystander ask o3 at 297. Since the fraudulent order at 298 cannot be trusted, detection of fraud should depend purely on the victim and the bystander orders.

In general, order time agreed between the exchange and non-compromised user using signatures can be accepted by the smart contract to be sufficient for verification.

In most cases, when o1 is withheld for skimming, the market moving adversely would cause an execution at a better price (<= o1.price) but with worse order time (>o1.time), enabling us to detect the violation.

The time for an execution is effectively the time of the taker order. Therefore, price-time priority has been violated if:

1. There is an execution where the maker order o3's time is worse than the victim's order o1's time
2. o3 price is better than o1 price

Detection for victim bids:

for all executions Ei after o1.time

Let oi = Ei.maker

isViolation = oi.time > o1.time && oi.price <= o1.price

To prevent detection, the exchange would have to prevent any ask hitting the price of the victim order, which would effectively halt normal trading.

LIMITATIONS

In a highly illiquid market, there are many corner cases that the above may not catch. For example, may be no market action for a long time followed by a sudden move (price gap) which can be exploited by a compromised exchange. This is currently not detectable.

MARKET ORDERS AND FRONT RUNNING

Market orders skip ahead of the price-time priority queue and front running market orders cannot be detected using the check above.

Market orders are not currently part of the protocol. We hope to extend market order fraud-proofs or go fully on-chain once plasma or other high speed chain is operational.

SUBMISSION OF FRAUD-PROOFS

A malicious actor would need to withdraw their funds after a fraudulent action. As long as there is a sufficient window of time to detect and submit fraud proofs, the smart contract can prevent the withdrawal or disable further action on the Custodian. Other users can detect the state change and withdraw their assets at their convenience. We propose a waiting period for every user after a withdrawal request, sufficient enough for any fraud proofs to be submitted. The exchange and smart contract would not accept any transactions for a user until their withdrawal is processed. This slight inconvenience is a justifiable tradeoff for the added safety. On the verification of a fraud proof, the exchange would halt. The perpetrator's balance could be awarded to the fraud-proof submitter, making compliance a form of mining.

All attacks can be detected by the victim as soon as they occur and a fraud-proof can be submitted to the smart contract, which can be used to take corrective action such as disabling the exchange and allowing all users to withdraw their funds. A small mandatory delay before withdrawal ensures there is sufficient time to submit fraud-proofs before a malicious user can siphon money from the contract.

COMPARISON TO OTHER DEX

Leverage and Derivatives: Most DEX are not focused on risk management and derivatives offerings. We hope to be the first exchange that offers derivatives with secure custody.

High Speed: Blockchain not involved in the critical create-cancel-execute path, making Leverj highly competitive against other DEX in terms of speed.

Congestion insensitive: Leverj can postpone sync to blockchain during times of blockchain congestion, while enabling trading to proceed, only impacting withdrawals. On-chain matching DEX cannot degrade gracefully during network congestion.

Secure against on-chain attacks: There are a variety of attacks possible against pure peer to peer exchanges. For example, a rouge taker can soak up all bids from makers and not submit trades. Congestion and arbitrage attacks are also possible when market is moving fast.

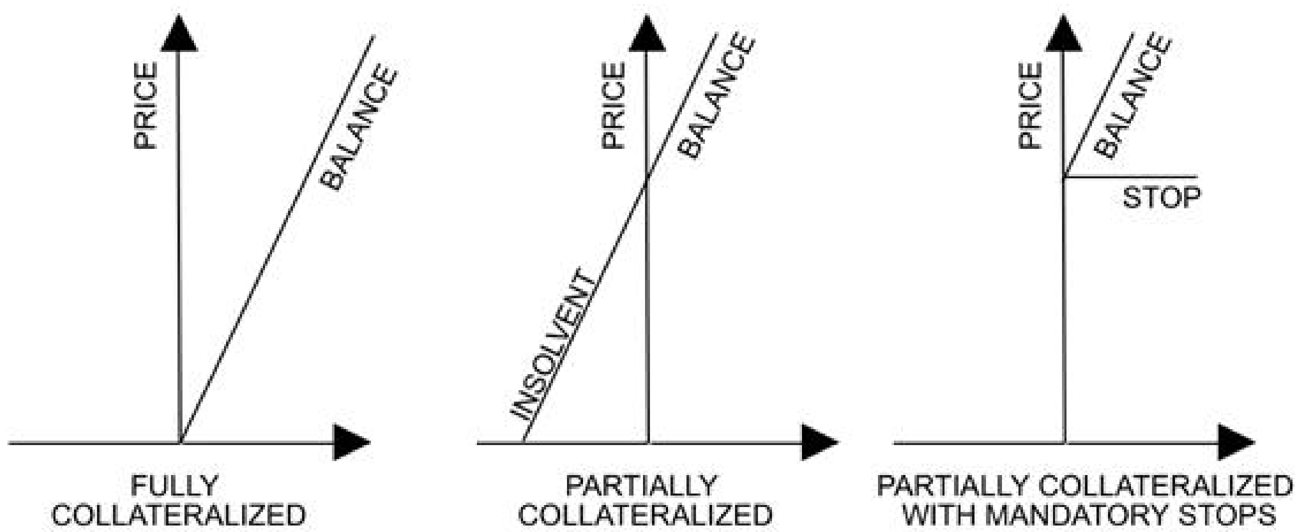
Low cost: 98% of orders are cancelled in developed markets. By not requiring storage costs for cancelled orders, Leverj is nearly 2 orders of magnitude cheaper than nearly every other DEX. Leverj can also hold off syncing to chain when during times of blockchain congestion without impacting trading. Only withdrawals are impacted. This kind of graceful degradation cannot be matched by most DEX.

Other DEX Action	Eth Cost for 100 orders
Stores unfilled orders	0.0196
Stores filled orders	0.0004
Requires gas to cancel	0.0196
Updates on every execution	0.0002
Total	0.0398

Leverj Action	Eth Cost for 100 orders
Does not store unfilled orders	0
Stores filled orders	0.0004
No gas to cancel	0
Updates on every execution	0.0002
Total	0.0006

**Estimated cost at 4Gwei gas price*

3. DERIVATIVES ON LEVERJ



NON-CUSTODIAL DERIVATIVES

The major distinguishing requirement of leveraged exchanges over spot exchanges is risk management. Since users who owe money can simply walk away in a decentralized environment, we need to ensure that no account goes into negative balance.

In the traditional exchanges, risk is managed by continuous monitoring of user balances and closing out positions forcibly when there is a risk of insolvency. This process is expensive and not reliable. Clearing members are bound by legal obligations to make up for any shortfall of their member accounts.

Replacing monitoring and ad-hoc forcible closures with mandatory stop orders enables us to manage risk without a central exchange user. The entire risk system is beyond the scope of this document but relies on the following:

1. Atomic stops: Stop orders that are guaranteed to fill within a max slippage. These enable prevention of accounts going into negative balance.
2. Auto-Deleveraging: Ensures integrity of system and no positions are dangling.

To implement the above in a manner that makes trading enjoyable requires careful crafting of appropriate leverage offered, reference index construction and handling of corner cases.

DERIVATIVES OFFERINGS

Our primary product offering will be ETH/USD inverse contracts based off a median index created from the highest volume spot exchanges. This will enable hedging Ether against fiat using only Ether. We can also offer a variety of products denominated in ether for which a reliable reference index can be constructed.

ERC20 spot and derivatives on highly liquid tokens will also be offered including options and futures including on Token index prices.

4. THE LEVERJ (LEV) TOKEN

LEV is an ERC20 token that represents the participation to trade on Leverj. LEV is not a requirement to trade on Leverj and a trader can choose to simply pay fees in ether. However, regular traders will benefit from holding and staking LEV since its economically attractive to do so.

LEV AND FEE TOKENS

The Leverj DApp is designed with a bi-level token structure a two level tokens. The primary token is of fixed supply, and represents a license to transact on LEV platform proportional to the percentage ownership of the token supply. The secondary token FEE is the accounting mechanism to ensure the rights of LEV can be exercised fully in a decentralized manner.

BI-LEVEL TOKENS VS REVENUE SHARING

Most revenue sharing systems have the following challenges:

1. Building liquidity is difficult.

2. Attracting other service providers to grow a rich ecosystem is extremely challenging without liquidity.

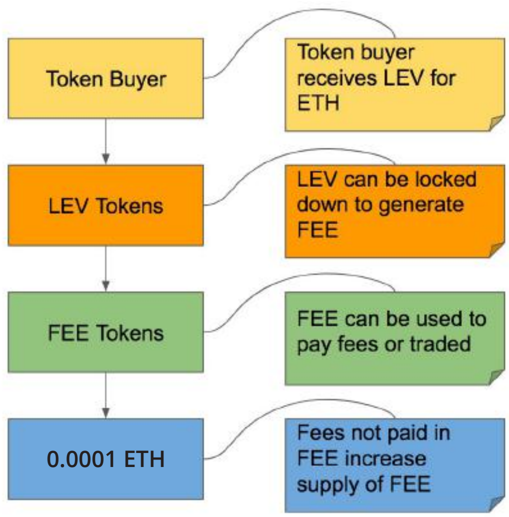
The two level Leverj token system has been carefully crafted using economics and game theory to incentivize liquidity and quickly grow a rich ecosystem.

USER PERSPECTIVE

From the user's point of view, bi-level tokens have the following advantages:

1. The second level token holds fees stable in ETH terms to ameliorate cryptocurrency fluctuations. For example, when the ETH exchange rate is very high in USD terms, it makes sense to sell your full ETH position instead of using part of it to pay fees.

2. The ability to sell excess capacity when trading activity is low. This allows the trader to sell FEE tokens generated when, for example, the trader is on vacation without giving up possession of LEV tokens. This is equivalent to a temporary transfer of the right to use LEV. Indeed, some investors may have a strategy of simply selling generated FEE as a steady source of income.



SYSTEM PERSPECTIVE

From a systemic point of view, two level tokens have enormous positive consequences.

1. The accumulation of FEE tokens over time will increase trading pressure. This is analogous to typically higher volume on no-fee exchanges, simply because more trading strategies are profitable. This increased trading pressure increases volume and liquidity greatly, enabling tight spreads and predictable fills, without slippage and helps facilitate generally healthy markets.

2. A secondary effect of FEE accumulation is that it enables a rich ecosystem with many other participants. The ability to pay for additional services from auto-generated FEE tokens means that traders are more likely to purchase, and providers more likely

to supply services to the system. High liquidity and a rich ecosystem are value multipliers and we believe the overall system would be worth much more than a simple revenue sharing/fee rebate system.

LEV TOKEN

The token sold during the token launch is known as the Leverj LEV token. This token is created only on the ICO issuance and it's supply is permanently fixed.

FEE TOKEN GENERATION

LEV tokens may be used to generate FEE tokens. LEV holders will not automatically generate fee; however, token holders can "lock" their tokens into a smart contract, which applies the user-selected lock duration to a formula designed to regulate the total supply of FEE tokens. Longer lock periods generate larger amount of FEE tokens.

Once users execute the contract, depending on how much trading activity there is on the platform — as well as the FEE market mechanics — they will receive a proportionate amount of FEE.

Once the lock duration expires, the locked LEV ceases to generate FEE and becomes freely transferable by the holder once again. There is no limit (other than duration) to how many times LEV tokens may be used to generate FEE.

GAME THEORY

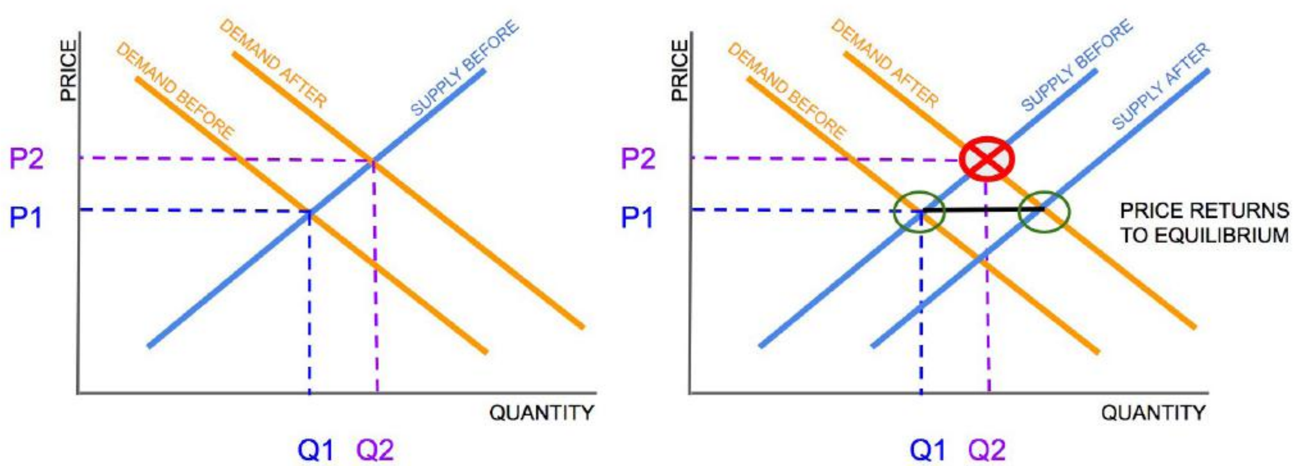
The main goal is to create a functioning market for FEE in ETH (Ethereum) so that LEV holders have access to a liquid market for their disbursements, and Leverj platform users can get a discount on the fees they would otherwise pay in ETH. Connecting these two major users in the Leverj ecosystem will help foster an economy within the community that pairs groups with overlapping interests. FEE will be maintained as a market that maximizes utility for the stakeholders.

FEE TOKEN GENERATION

LEV tokens may be used to generate FEE tokens. LEV holders will not automatically generate fee; however, token holders can "lock" their tokens into a smart contract, which applies the user-selected lock duration to a formula designed to regulate the total supply of FEE tokens. Longer lock periods generate larger amount of FEE tokens.

Once users execute the contract, depending on how much trading activity there is on the platform — as well as the FEE market mechanics — they will receive a proportionate amount of FEE.

Once the lock duration expires, the locked LEV ceases to generate FEE and becomes freely transferable by the holder once again. There is no limit (other



DEMAND PRESSURE & RECOVERY

than duration) to how many times LEV tokens may be used to generate FEE.

ECONOMICS

Market forces are at work in the pricing of any asset, and the FEE token is no exception. An increase in supply, *ceteris paribus*, will increase the quantity provided by the market and lower the price. Therefore, an unexpected supply increase will adjust the price downward, whereas an unexpected demand increase will adjust the price upward.

Using a diverse set of tools to influence the FEE demand and supply mechanisms, both directly and indirectly, the system will target a FEE price that is approximately equal to the coupon value for covering Leverj exchange fees.

DEMAND PRESSURE

When the economic activity on the platform grows, there is likely to be demand pressure on FEE. This pressure will not only affect LEV holders who might wish to generate additional FEE; there may also be significant secondary market demand that drives the price significantly above the targeted coupon rate.

To counteract this effect, more FEE is produced when fees are paid in ETH and distributed to LEV holders, easing the demand pressure and bringing the market back into equilibrium.

SUPPLY PRESSURE

The opposite situation can also occur: an imbalance arises from too much FEE supply, resulting in a price decline. In response to this, the self-regulating system for FEE production will adjust such that the FEE supply is slowed to bring the price back up.

PRICE STABILIZATION MECHANISMS

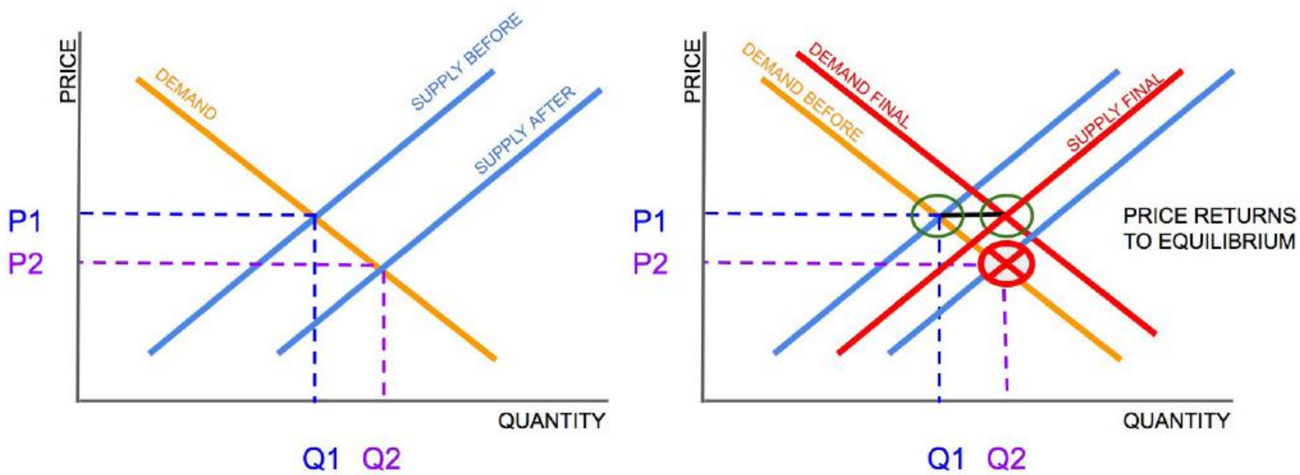
The price of FEE will be managed by a series of Price Stabilization Mechanisms (PSMs).

SYSTEMIC PSMS

The primary systemic PSMs are parameterized by platform activity and supply generated by the same platform activity.

The most important source of demand for FEE tokens will be the users who are purchasing FEE to pay the Leverj trade fees which are denominated in Ether. The platform will accept FEE and it will be tradable in a FEE/ETH order book.

To give a simple example, if an individual is going to make a trade worth 100 ETH and the fee charged is 1% (in practice it will be much less than this), then the user needs to pay 1 ETH or 10,000 FEE (1 FEE = 0.0001 ETH). Assume that the price



SUPPLY SHOCK & RECOVERY

currently trading at 0.00008 in the FEE/ETH order book, meaning it is 20% cheaper to pay your trading fees in FEE than ETH. The trader on Leverj can merely check a box preferring to pay for fees in FEE token instead of ETH, and platform will automatically buy 10,000 FEE from the market at 0.00008 (for 0.8 ETH) and cover the 1 ETH fees, saving 0.2 ETH in the process!

In this model, if the FEE/ETH book is trading above 0.0001 ETH (at say 0.00012 ETH), due to excessive speculative demand, then the platform demand will dry up, and LEV holders who receive FEE will be able to get above-par returns on the FEE they sell into the market for ETH.

On the supply side, when FEE is generated, it is done so based on a formula that attempts to target FEE price to be near 0.0001 ETH. Thus, LEV holders will be able to receive FEE and use it to pay for trading activity on Leverj, save it for future trading activity, or sell for ETH immediately. Our primary concern is that FEE retain proper demand and a reasonable price, should LEV holders choose to sell. The risk of the FEE price being abnormally low outweighs the risk of it being abnormally high.

Thus, if the price becomes low, based on a criteria we make open source, it will trigger a mass-staking by the team's LEV. This will mean less FEE distributes to LEV holders who are selling large amounts in the FEE market. This will help reduce the supply pressure while the demand remains the same, guiding prices closer to the par value.

LEV AND FEE TOKENS

Leverj is designed around a bi-level token structure. The primary token (LEV) is of fixed supply, and represents a license to transact on the Leverj platform proportional to the total token supply. The secondary token, FEE, is the accounting mechanism to ensure the rights of LEV can be exercised fully in a decentralized manner.

The amount of FEE tokens charged can be lower (say 0.1 FEE) or higher (say 1.5 FEE) based on the product traded. Leverj can also adjust the coupon value based on market conditions such as price of ether.

STAKING

Fair distribution of FEE tokens is ensured by staking LEV tokens. Users who stake for longer durations get more FEE tokens. This ensures that users committed to trading on the platform can be assured that they can exercise their license compared to users who are holding LEV simply for speculation.

Leverj uses economic pressure instead of a mathematical model to compute the proper amount of FEE required to be in circulation. This is because a mathematical model will always have elaborate that no model can perfectly account for. An economic pressure relieves us of the need for modeling and we simply use actual demand pressure which can be reduced to simple computation.

In an equilibrium where the volume traded on the exchange does not change, there is sufficient FEE tokens that circulate among market participants, enabling trading without paying fees to the exchange. This is the ideal execution of LEV as license to trade on the platform and FEE as its accounting mechanism.

When the volume falls, excess FEE tokens may be destroyed (or simply stored) and users can continue to trade without paying additional fees.

When the platform is ramping up, increasing volume is likely to result in a situation where there are insufficient FEE tokens to satisfy the trading volume. This may give rise to a premium on FEE tokens and may result in undesirable behavior such as hoarding. To prevent this, fees can be paid in ether and the equivalent FEE tokens are generated and distributed to LEV stakers.

STAKING CADENCE

To simplify the UX and security of the staking contract, there is a fixed staking cadence which computes the number of tokens staked and the duration of the stake. This enables a simple calculation that allocates the FEE tokens to the traders.

EXPIRY

At the end of the staking period, all LEV are returned to stakers and FEE tokens proportional to their stake are distributed to stakers.

STAKING FORMULAS

For single stake:

Let L => Number of lev to be staked (passed by user)
Let T => the expiry block number
Let t = T - current_block => number of blocks to stake
Then Lt => Number of Lev blocks staked
stake[user] += L
evblocks[user] += Lt
total_levblocks += Lt

FEE events (periodic aggregated) could combine with expiry:

Total_Fees += FEE sent for trading fees + ETH sent for trading fees * ETH_FEE_RATE

At Expiry Adjust Supply:
If Total_Fees > FEE_supply:
Generate (Total_Fees - FEE_supply) FEE tokens

At expiry (for all users):

Fee_share[user] = (levblocks[user] / total_levblocks) * Total_Fees
Transfer fee_share[user] FEE to user
Transfer stake[user] to user

5. TOKEN SALE

TOKEN SUPPLY

Token	Description
1000M (1 billion)	Tokens created
400M	**Available for purchase including bonus ***
200M	Founders
300M	Liquidity and Operations
100M	Partners

* *Unsold tokens will be sent to a burning contract where 50% are locked for 12 months and the remaining are locked for 10 years in order to stabilize LEV utility during the early adoption phase.*

* *Founders pledge to donate LEV proportional to the burnt ratio to the liquidity and operations pool*

* *Airdrops and bounties will be paid from the Liquidity and Operations*

TOKEN SALE STRUCTURE

Duration	Price
1ST 150M tokens	4615 LEV per ETH
2ND 250M token	3000 LEV per ETH

TOKEN SALE TIMELINE

Event	Date (12 UTC)
Sale Start	2017-11-07
Sale Ends	2017-12-07

6. POST-SALE CONSIDERATIONS

TOKEN DISTRIBUTION

The following pie chart provides the breakup of the tokens distribution. All tokens, including pre-sale, are distributed via smart contract, audited by ConsenSys, and managed by the independent escrow providers BraveNewCoin.com (BNC).

Purpose	% Share
Partners	10
Liquidity/Ops	30
Token Sale	40
Founders	20

VESTING SCHEDULE

The token vesting schedule, shown below, has been designed to specifically align the long-term interests of the founding team with those of public token sale participants to maintain consistent and healthy growth of the trading ecosystem. The long drawn-out vesting schedule also ensures that the team is continuously motivated and stays vested in the success of the project for a longer duration. Early exit of the core team also impacts the success of the project and thereby the value of the token.

Period	% Locked
Immediately	10
6 months	30
12 months	30
18 months	30

SECONDARY SALES

Leverj holds 30% of tokens for liquidity and operations. Leverj will stake most of these tokens in order to get FEE tokens. Leverj is therefore economically incentivized to hold on to these tokens and has no plans at present to sell large portions of these tokens on secondary market. As part of business development, some tokens may be given to financial institutions as part of partnership agreements, incentivize advisors and new employees. In such cases, we will require lockout periods of sufficient length to ensure there is no major disruption in market value.

In case the Leverj team chooses to sell LEV tokens that it holds on the secondary market in the future, it will sell on or around the 1st of each month an amount of approximately USD 100,000 worth of tokens. For any amounts exceeding this, the public will receive notice at least one week in advance of the time and amount of tokens that may be sold.

Liquidity operations require that a portion (up to 2% of supply) of the tokens will be made available on the order book. Traders can buy from or sell into the book and this means our share of tokens will vary slightly based on market activity.

USE OF PROCEEDS

Developement	30%
Marketing	10%
Biz Developement	10%
Legal	10%
Operations	10%
Liquidity	30%

Disclaimer: Our project is subject to several other considerations that require flexibility in how we spend the raise. For example, if we get an opportunity to partner with a legacy financial powerhouse, we may need to invest significant resources for speedy implementation. We may also have opportunity to work with regulators in untapped crypto markets such as the United States that may require unforeseen expenditures. All-in-all, since we have a centralized component, we have need for operational and strategic flexibility unlike a pure protocol project.

Converting to Fiat: Most of the raise will be kept in ETH and be converted to fiat as necessary. There will be an initial conversion of up to $5M USD to bootstrap the project.

7. PLATFORM FEATURES

BASE PLATFORM

Centralized trading platforms have inherent counterparty and custodial risk. User identity, transaction history, and funds are all ultimately controlled by the exchange operators. The exchange custody of these valuables makes an attractive target for hackers, lawsuits and state actors. The risks and losses inherent in centralization can be substantial1. Leverj provides decentralized identity to avoid identity leaks.

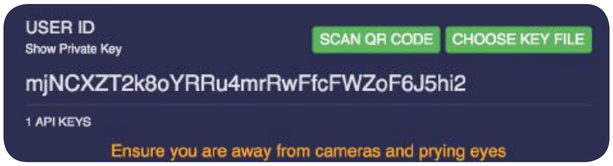
DECENTRALIZED IDENTITY

A third-party issued identity (such as an email address) puts you at the mercy of a centralized exchange's competence, fairness and integrity. Every identity you use can be held hostage to the interests and whims of unpredictable actors such as hackers or governments.

A decentralized identity can be used for authentication, signatures on contracts, attestation of documents, messaging other traders and to share media.

HARDWARE WALLET SUPPORT

Cryptography has made remarkable financial products possible, but at the cost of an ever-present risk of compromise via malware, security breaches, or custodial issues in regards to private keys held on computers and backend servers. Hardware wallet support greatly reduces the chances of malware or other security breaches stealing coins on your trading computer.



DERIVATIVES OFFERINGS

Leverj focuses on derivatives products, which distinguishes it from other DEX offerings. Using non-custodial risk management, we can offer derivatives products without requiring an exchange user to take over losing positions for liquidations. ETH/USD inverse futures will be the primary offering. However, we can offer futures on any market with a stable, well developed market. We can also offer a variety of options or futures on liquid ERC20 tokens.

ON-CHAIN SETTLEMENT

With an on-chain exchange, there are no custody settlement and manual withdrawal processing steps since closing a position results in near-instant settlement. Elimination of exchange custodial responsibility to the exchange has the pleasant side-effect of not requiring the exchange to perform any actions in order for you to access your profits. We eliminate waiting for exchange action to settle trades, process expiries and refill hot-wallets. Every change in your position automatically updates your equity in real-time, making your funds available for withdrawal subject only to blockchain latencies.

8. ENHANCED TRADING PLATFORM

The privacy and security benefits of decentralization and the basics of reliable stops and position management facilitate trading, but fall short of that is available on legacy financial platforms. The Leverj enhanced trading platform brings these features to digital currency, enabling rapid growth of the Leverj platform.

AUTOMATED TRADE MANAGEMENT

The most profitable professional traders use discretionary entry and mechanical trade management. This approach enables them to focus their attention on market opportunities and delegate trade management to software modules. This “fire and forget” approach eliminates an entire class of trade management errors. For example, an order will be placed to enter on the breakout of a signal bar if the bar closes strongly. Once filled, a trailing stop will tighten below every new swing point once a new high is reached. Partial profits are taken on every push and the position is closed on a parabolic move. All of these are orchestrated routinely once the position is open, relieving the stress of trade management and enabling the trader to focus on price action and new entries.

PRICE ACTION ENTRIES

The most common trading regret is taking a position due to "fear of missing out" (FOMO). FOMO entries are caused by hesitation due to a less-than-perfect setup and subsequent late reaction once price moves with unexpected strength. Habitual FOMO trading makes it impossible to build trading discipline. Price Action entries free the trader from absolute price levels and allow focus to remain on unfolding market structure. For example, you may want to enter on the breakout of a signal bar, or want stops to trail below the low of the prior bar instead of a fixed number of ticks. You may want to sell on the close of a bar on the third push, rather than hoping you guessed the exit price correctly. Leverj supports price action entries that enter and exit precisely, reducing unexpected losses and suboptimal exits.

TRADE REPLAY VIDEO

The best way to improve your trading is to observe yourself trading. Trade replay videos allow the trader to view how a trade was planned and executed, from placing the entry order, to stop management, to eventual exit. Video replay can be used to document your trading, share with and teach other traders, or simply archive your greatest trading moments. Even add audio commentary and background music. Your video of making a killing on the big bear move would be fantastic with Carmina Burana as soundtrack.

SUBSCRIBE

Another great way to learn any highly specialized skill is to be mentored by someone who excels in that field. Find the most respected traders, subscribe to their feed, and learn from them a lot faster than you would learn by trading (and possibly losing) your own money. Open up your trade videos and reports and share with the world. If you are a good trader, you can build a following.

MANAGED TRADING

Many people desire the exposure to digital currency, but are too busy in their professional lives to spare their attention for full-time trading. Managed trading presents an attractive alternative to those who have the capital but not the skill to trade. Simply “follow” or replicate trades of highly skilled traders automatically in exchange for a percentage of the winnings. In the beginning this is likely to be a fixed percentage but as the platform evolves, we expect traders to set their own rates.

SIMULATED TRADING

The first few months of a new trader's performance is unlikely to be profitable. In addition, there is substantial risk testing out unproven ideas with real money. Simulated trading enables trying out ideas and fine tuning trading strategy with real-time market data, while avoiding market risk. Once the trading idea or setup is proven, it can confidently be executed on a live account.

HISTORICAL DATA REPLAY AND TRADING

Institutional trading is largely algorithmic and the ability to fine tune and harden a trading system depends on reliable historical data. How would a trading strategy fare during the great bull move and subsequent crash of 2013? Harden trading strategies by replaying extreme market conditions and add safeguards to ensure sustainability in adverse conditions. Leverj brings the advantages enjoyed by institutional traders to crypto trading, enabling re-playing market data to fine tune and perfect your home grown strategies.

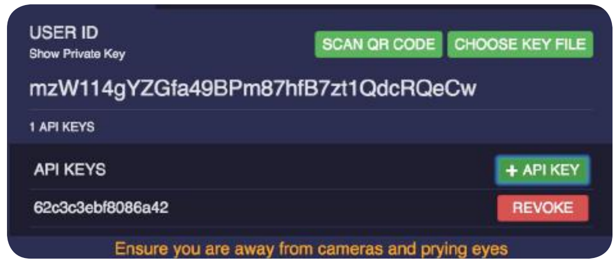
MARKETPLACE

A marketplace for decentralized trading services is essential to a rich ecosystem. Instead of building your own indicators and strategies, buy them from a marketplace. If you have developed a great indicator, list it on the marketplace and get paid in FEE tokens.

PLUGIN FRAMEWORK

A plugin framework enables quick composition of an ideal trading environment, building on the work of others. Plugin your own indicators, trading strategies, reports, or anything else that enrich your trading experience. The plugin framework is a foundational aspect of the marketplace.

ZERO-KNOWLEDGE API KEYS



A trading or reporting service needs to be authorized to perform certain operations on behalf of the user. In the centralized world, this is accomplished through API keys. Leverj provides Zero-Knowledge API keys that enable integration with vendors and partners without relying on transport and storage secrecy. This enables the creation of an ecosystem of decentralized services that can build a new value network on the blockchain.

ISSUES WITH DECENTRALIZED LEVERAGED TRADING

Leveraged trading adds risk management and position management capabilities required for practical trading. Adding margin to a position or re-leasing margin from a winning position to open a new position are practical necessities for trading. Recent attempts at decentralized leveraged trading platforms have resulted in poor user experience due to lack of attention to practical exchange operation issues. Leveraged trading adds another level of complexity to decentralized trading that must be carefully designed. As exchange needs to be performant in addition to secure for trading to be enjoyable in addition to enabling the basic goals of decentralization. The key issues with decentralized trading are latency, finality and liquidity. We address these by using the blockchain sparingly and relying on ancillary technology where possible.

STOPS

Reliable stops are the hardest feature to get perfect, even for centralized exchanges. When a price spike can trigger a stop, but never fill (or fill it at an undesirable price) it becomes imperative to your position. This induces attention fatigue and causes unforced error that reduce your profitability. Professional traders simply cannot afford to trade without reliable stops, since they are vital to precise risk management. Leverj provides atomic stops that are guaranteed to fill within predictable range.

LIQUIDATIONS

When a trader's position moves into a losing area beyond its allocated margin, the position needs to be liquidated. Leverj is able to liquidate positions without the need for a centralized exchange user to take over the position.

POSITION MANAGEMENT

Good position management is often the only difference between a break-even trader and a profitable trader. A platform that facilitates good position management practices is essential to trade effectively.

ADD/REMOVE MARGIN

Current decentralized leveraged systems "lock-in" a margin until the contract expires or is settled. This means profits cannot be taken when available if the market reacts earlier than expected. Positions cannot be saved by adding margin if a pullback is deeper than expected. All in all, this approach to trading is essentially a gamble on direction at a point in time. A sophisticated trader requires the ability to modify the margin backing any position based on price action. Indeed, the freedom to take profit and allocate it to a new opportunity should be smooth and natural to ensure that the trader can take profit when price action enables it. Leverj enables addition and removal of margin with an intuitive stop order inter-face that allows traders to manage position margin.

SPLIT/MERGE

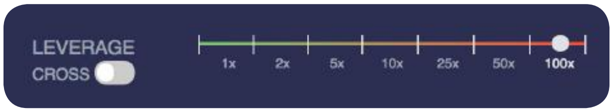
It is a good practice to take partial profit on a windfall move in the trader's favor. The ability to split a large position facilitates this. Once a position is split, it is possible to manage each position differently, for example, a tighter stop on half to protect profits and a looser stop on the remaining for longer holding periods. The converse is the ability to build up a position by many small entries (such as iceberg orders) and manage them as a single position by merging them. Leverj provides splitting/merging of positions, giving the trader flexibility to react appropriately to the market and manage exits, leverage and stops for optimal profit.

CROSS/FIXED

Traders who trade long timeframes and accumulate large positions need to use all available margin (cross margin) to ensure they can accumulate through large dips without being stopped out.

However, often they also wish to trade portions with fixed margin to protect profits on moves on a smaller timeframe. Leverj is the only exchange that offers simultaneous fixed and cross margin while splitting a fixed portion out of the cross margin for partial exit.

NETWORK CONGESTION



Blockchains can suffer congestion for extended durations. A severely congested network may mean that settlement transactions are confirmed with a significant delay, but wont impact actual settlement amounts.

9. TIMELINE

2013

Start

Founders Bharath Rao and Nirmal Gupta meet

Concept for decentralized leveraged derivatives on bitcoin conceived

2014
Q1

Proof of Concept development in motion

2015
Q4

Self-funded full-time development begins

2016
Q1-Q2

Coinpit.io becomes the first exchange to open-source security code

Coinpit.io launches public beta

Industry First Features:

Decentralized Identity

Segregated Accounts

Zero-Knowledge Authentication

Exclusive & Industry First:

Multisig with user controlled private key

On-blockchain Settlement

2016
Q3

Industry first Robust Median Index launched

Coinpit.io launched at TechCrunch Disrupt

2017
Q1-Q2

~600K Seed Angel Investment Raised

Inverse contract launched

Exclusive & Industry First:

Proof-of-Audit embedded in blockchain

Zero-Knowledge API keys

Hardware multisig wallet launched

10. ROADMAP

BASE PLATFORM — RAISE NEEDED

Period	Milestones	Raise Needed
2018 Q1	Decentralized ETH/ERC20 spot trading platform Hardware key authentication instant settlement	$2.5M
2018 Q2	Fully decentralized custody futures trading live	$4M

ENHANCED PLATFORM — RAISE NEEDED

Period	Milestones	Raise Needed
2018 Q3	Price Action Entries Trade Replay Videos	$5M
2018 Q4	Managed Trading Simulated Trading	$6M
2019 Q1	Historical Data Replay and Trading Marketplace Plugin Framework Social Media Trading	$8M
2019 Q2	Automated Strategies Enhanced Reporting Internationalization Encrypted/Anonymous Messaging/Chat/Email	$10M

PRODUCT OFFERINGS		RAISE NEEDED
2018 H1	Major Cryptocurrency Futures Crypto10 Index and Futures	$20M
2018 H2	CFD on OIL/GOLD/Top Commodities	$25M
2019 H1	Single Stock Futures Major World Index Futures	$30M

11. LEADERSHIP

Bharath Rao, Founder/CEO

Entrepreneur. Trader. Techie. Leader. Blogger. Speaker. Inventor
10 Year Wall St. Veteran
Policy and Strategy Advisor to Liberland
MS Computer Engineering from Syracuse University

Nirmal Gupta, CoFounder/CTO

Full Stack Developer.
10 years on Forex Trading Software
BS Aerospace Engineering from IIT Kanpur

Babu SK, Operations

FinTech Veteran, Growth & Tech Strategy
Operational Transformation
MBA, IIM Bangalore

Gerry Howatt, Marketing

20+ year Marketing Executive, Media Strategist, Product Marketer, Partnership Development, Entrepreneur
BA St Lawrence University

Swapman, Advisor Economics & Financial Theory

Financial Market Expert, Crypto Market Expert & Trader, Economist
M.Sc. Economics, University South Denmark

Alexandra Ward, Community Manager

Crypto Personality and Trader.
Administrative Role in Trading Communities.
Moderator of Bitcoin-Related Subreddit.

Benny Sadeh, Software Craftsman

25+ years of Software Engineering

M.S. Computer Science, University of Alabama

Merunas Grincalaitis

Ethereum Smart Contract and Javascript Engineer

Universidad de Granada

12. LEGAL CONSIDERATION

As part of legal due-diligence, the Leverj team has consulted with several law firms around the globe to evaluate the implications of our structure, token launch, and operations. We can make no guarantees regarding the legality of the platform or launch in any given jurisdiction. Regardless, we have modeled the platform to be provably compliant with the spirit of regulations in major jurisdictions and we hope to be a model of regulatory compliance for decentralized applications and token launches. We will be responsive and collaborative with any regulators as necessary going forward.

FORWARD LOOKING STATEMENTS

This document has forward looking statements that are subject to risks and uncertainties, which could cause actual results to differ materially from those anticipated. Such statements are based on our beliefs as well as assumptions made by and information currently available

UNFORESEEABLE TECHNICAL LIMITATIONS

Some of the features described herein are based on our current understanding of blockchain technology and the assumption that blockchain systems continue to work with the same characteristics in the near future. In the event that the nature of the blockchain changes dramatically for example due to high congestion, change in proof of work, network splits, 51% attack or any other unpredictable event, the platform's stability and our ability to deliver features described here may be negatively impacted.

LEGAL IMPLICATIONS OF TOKEN LAUNCHES

LEV/FEE tokens (henceforth "tokens") are functional utility tokens within the Leverj platform. TOKENS ARE NOT SECURITIES. **TOKENS ARE NONREFUNDABLE. TOKENS ARE NOT FOR SPECULATIVE INVESTMENT. NO PROMISES OF FUTURE PERFORMANCE OR VALUE ARE MADE WITH RESPECT TO TOKENS, INCLUDING NO PROMISE OF INHERENT VALUE, NO PROMISE OF CONTINUING PAYMENTS, AND NO GUARANTEE THAT TOKENS WILL HOLD ANY PARTICULAR VALUE.** TOKENS ARE NOT PARTICIPATION IN THE COMPANY AND TOKENS HOLD NO RIGHTS IN SAID COMPANY. TOKENS ARE SOLD AS A FUNCTIONAL GOOD AND ALL PROCEEDS RECEIVED BY COMPANY MAY BE SPENT FREELY BY COMPANY ABSENT ANY CONDITIONS. Tokens are intended for experts in dealing with cryptographic tokens and blockchainbased software systems. TOKEN SALE IS UNAVAILABLE TO CHINESE RESIDENTS, US PERSONS & SEYCHELLES RESIDENTS AND OFAC SANCTIONED COUNTRIES AND PERSONS (SDN).

LEGAL LANDSCAPE FOR DERIVATIVES TRADING

Derivatives trading are an area of interest for many regulators around the globe, including those within the United States. Leverj intends to operate our business in accordance with the laws of relevant jurisdictions. As such, Leverj may not be immediately available in certain jurisdictions. The Leverj team and our advisors are aggressively pursuing strategies to bring the benefits of the platform to the global trading community expeditiously. This includes obtaining securities licenses as required by law.