Eximchain: Supply Chain Finance solutions on a secured public, permissioned blockchain hybrid

Juan Huertas , Hope Liu and Sarah Robinson

Date of Whitepaper: March 13th 2018 V6

ABSTRACT

Eximchain brings visibility to global supply chain finance (SCF) through smart contracts. We build a public, permissioned chain for small-and-medium enterprise (SME) buyers and suppliers to create supply chain optimization tools and gain access to affordable capital sources to grow their businesses. Our smart contract-based ecosystem allows SMEs to quickly implement customized SCF solutions or issue digital tokens on a permissioned fork of Ethereum supporting data privacy. We adopt a consensus protocol and quadratic voting based governance model to provide practical, finite time security guarantees on our public, permissioned blockchain hybrid. From financing to procure-to-pay, our products utilize smart contracts to optimize the global supply chain for buyers, suppliers, and financiers. Eximchain is an official candidate of the Blockchain Regulatory Sandbox Program in Guiyang, China and a member of EEA (Enterprise Ethereum Alliance).

1. ABOUT EXIMCHAIN

Eximchain project was kicked off in 2015 at MIT (Massachusetts Institute of Technology) by a team with decades of academic and industry experience in computer science, banking and global supply chain across the world. Our vision is to use blockchain technology to bring the global supply chain into the digital era and lower financing barriers for SMEs. The project has received valuable mentorship and guidance from the MIT Media Lab Digital Currency Initiative, MIT Center for Transportation and Logistics, and Plug And Play Fintech Accelerator. The project was chosen as the Grand Champion of the 2016 Boston Seagull Entrepreneurship Contest, the Engine of Innovation Prize of the 2016 Rice Business Plan Competition, and a Finalist of the 2017 MIT $100K Business Plan Competition Accelerate.

2. SUPPLY CHAIN FINANCE OVERVIEW

Traditionally, supply chain management has focused on the material flow of physical goods from manufacturers to end consumers. However, the recent global economic downturn demonstrated that managing financial flows within the supply chain can be as important as managing physical flows of goods and services[1]. Supply chain finance (SCF), one of the most exciting and promising new products emerging in the banking industry, is a set of technology-based business and financing processes that allow financiers to fund an organization's operations through its supply chain relationships. SCF enables buyers to optimize working capital and suppliers to generate additional operating cash flow while simultaneously minimizing risk across the entire supply chain. More specifically, SCF enables buyers and sellers to shrink their inventories, collect money from customers faster and delay payments to their suppliers. Citi recently completed a working capital study that showed companies managing working capital through SCF were able to reduce these assets by 30%, resulting in EPS (earning per share) increases in the range of 1% to 4%. Furthermore, the top 10% of companies that reduced their CCC (cash conversion cycle) were rewarded with a 30% stock price appreciation[2].

3. THE PROBLEM

According to the International Finance Corporation (IFC), small to medium-sized enterprises (SMEs) in developing countries face a financing gap totaling over $2 trillion[3]. In China alone, the vast majority of the 40 million SMEs remain unserved by existing financial resources[4]. This financing gap is particularly concerning because, as cited by the World Bank, SMEs contribute up to 60% of total employment and up to 40% of GDP in developing markets[5]. Innovative SCF solutions offer a powerful tool for SME buyers, suppliers and financiers to overcome this funding gap[6]. Innovations in this space have traditionally been driven by large corporations and banks in the field; however, cutting edge financial technologies offer new opportunities to extend the benefits of SCF to businesses of all sizes. According to a 2015 McKinsey Report, of the $20 billion potential revenue pool that exists for implemented SCF programs, only $2 billion is being captured today[7]. One primary issue inhibiting the widespread adoption of SCF programs among SMEs is that they currently lack a trusted tool that provides transparency to eliminate information asymmetry problems. Beyond this, there are quite a number of difficulties for adoption of SCF programs on a global scale:

First of all, any supply chain strategy cannot be determined in isolation. The market for SCF programs is inherently dynamic: exogenous factors, such as interest rates, and endogenous factors, such as inventory decisions and capital constraints, influence the evolution of the system.

Furthermore, the complexity of implementing SCF across the global supply chain limits its adoption. It takes tremendous effort to onboard suppliers and integrate the process with the existing operational flow by involving finance, procurement, and IT departments inside the organization.

Last but not least, it is difficult to align incentives among different participants. Suppliers, buyers and financiers are independent decision makers attempting to maximize profits in the face of asymmetric cost structures and uncertainties. Such independent profit maximizations often lead to poor performance of the entire supply chain.

The Eximchain platform solves these challenges by offering seamless integration into the existing workflow of SMEs and enabling developers to create customized tools for specific businesses and industry use cases.

4. OUR SOLUTION

Eximchain offers a platform to implement smart contract based SCF solutions on a permissioned fork of Ethereum supporting data privacy. Our ecosystem will enable SMEs to gain access to affordable capital sources by giving financiers visibility into the supply chain cash flow. The first game theory-based application we plan to build, **Multi-Party Dynamic Contracting***, (details to be described under Appendix- Use Case Example) will be designed in such a way that no partner can improve his profit by deciding to deviate from the optimal set of decisions. That is, there is no incentive for the buyer, the supplier, nor the financier to deviate from the set of actions that will achieve the globally optimal solution. The implementation is executed by the consensus of the network in a standard, automated, private, and auditable fashion. From the user's perspective, after making the initial input and setting up the negotiation rule, they can receive the negotiation result from a "black box" where the system automatically executes an optimization engine through multi-stage coordination until Nash Equilibrium is reached and each participant's incentive is aligned.

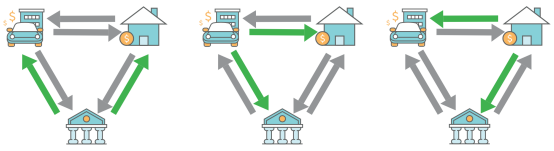
Buyers and suppliers can automate contracting processes with the Eximchain network. Suppliers and buyers normally have different and conflicting objectives. For instance, suppliers want buyers to commit themselves to purchasing large quantities of products in stable volumes with flexible delivery dates. Conversely, buyers need to be flexible to their customers' needs and changing demands. The difficulty with global optimization is that it requires firms to surrender decision-making power to an unbiased decision maker. Additionally, establishing trust between the supplier and the buyer is difficult to achieve. For example ,in January 2013, the Walt Disney Company sued Blockbuster, accusing them of cheating its video unit of approximately $120 million on under a four-year revenue-sharing agreement[8]. Through the Eximchain platform, buyers and suppliers can carefully design supply contracts to maximize profit on the supply chain with more visibility into demand, inventory and upstream/downstream operations through a trusted and secured network. Additionally, interactions and agreements are saved automatically with a traceable record.

Financiers will be onboarded to the network with aligned incentives. In the real marketplace, suppliers and buyers frequently finance their working capital from a variety of credit sources, such as banks, and incur significant financing costs. Studies have shown that under the assumption of positive inventory financing costs, traditional supply contracts fail to achieve joint profit maximization[9]. Based on the limited information displayed in contracts, it is hard for banks to understand the market expectation and real dynamic between buyers and suppliers to mitigate risk. In 2014, a Chinese trading company, Dezheng Resources, and its subsidiaries were alleged to have used duplicate receipts to pledge metal as collateral for loans. The result was a flurry of lawsuits, including the UK High Court case between Mercuria and Citi, over exposure to a $270 million financing deal[10]. The Eximchain platform provides access to smart contract history between two parties, which grants banks more visibility into the supply chain operations and enables them to better estimate the risk of a transaction. Furthermore, access to this smart contract information will provide other financiers, beyond traditional banks and lenders, with an opportunity to fund and generate value off of these transactions.

Eximchain allows developers to create variations on supply contracts secured by the network and build solutions that are customized to their global supply chain. Currently, supply chain partners use a variety of solutions to align incentives and mitigate inventory risk, including: buybacks, quantity discounts, revenue-sharing and two-part tariffs contracts. On the Eximchain platform, developers can build customized solutions based on specific industry needs, user dynamics and market competition. Banks and anchor buyers can easily scale the solution on the global supply chain by involving upstream and downstream players. Although these solutions will be varied, the contracting process will be highly standardized and can be seamlessly integrated into the bidding process and other supply chain management tools.

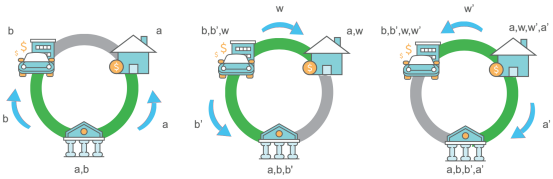
Customized negotiation rules:

Each graph represents one state transaction. The negotiation will end after all parties reach Nash Equilibrium based on the negotiation rules set by each party. Grey arrows represent locked status while green arrows represent unlocked status.



Private channel coordination:

Each communication channel is private where only the involved parties can see the information provided during each negotiation. The system runs automatically based on pre-set inputs and only updates state of each negotiation cycle for involved parties.



5. VALUE FOR OUR STAKEHOLDERS

Financiers:

Risk Mitigation

We enable dynamic, real-time monitoring of supply chain financing processes to provide visibility into the whole supply chain's operations. Lenders can now better understand the actions taken by end purchasers and upstream suppliers of each deal to better assess risk. With the combination of a "Purchase Money Security Agreement" (PMSA)[11], also known as purchase money security interest, on the loan, which makes the lender the first claimant of the collateral related to the loan in the case of default, the financiers gains a much better estimation on the risk and return of the investment despite all external uncertainties.

Operational Efficiency

With more information about the trade, the financier could more accurately set the rating and risk factor. Increased transparency over trade transactions tends to lower the risk factor and thus risk equivalent, which improves efficiency in operation and management of the loan. By digitalizing and standardizing the contracting process, financiers save the overhead effort of processing paperwork, understanding different terms, and going through multiple levels of manual review to make a final decision about the credit they are issuing.

Investment Opportunity

In the traditional corporate financing scheme, the financiers would be banks, focused on assessing the borrower's historical credit, capital position, collaterals and guarantees of the companies in the supply chain that they are providing credit to. However, in the SCF view, financiers could be any investor or anchor buyer who is capable of assessing and taking the credit risk of the SCF product. Our solution will lower the barrier to entry for financiers in the global supply chain, and will allow institutional investors and accredited individual investors who are looking for short-duration, low risk and highly collateralized credit products to offer alternative funding sources to SMEs in the future.

Buyers and Suppliers:

Working Capital Management

By adopting our solutions, suppliers facing difficulties obtaining affordable credit will now be able to access capital through banks or alternative sources. Capital-constrained buyers who rely on direct financing from a financial institution can obtain trade-credit in addition to standard contracts to subsidize their costs of inventory financing and improve their working capital.

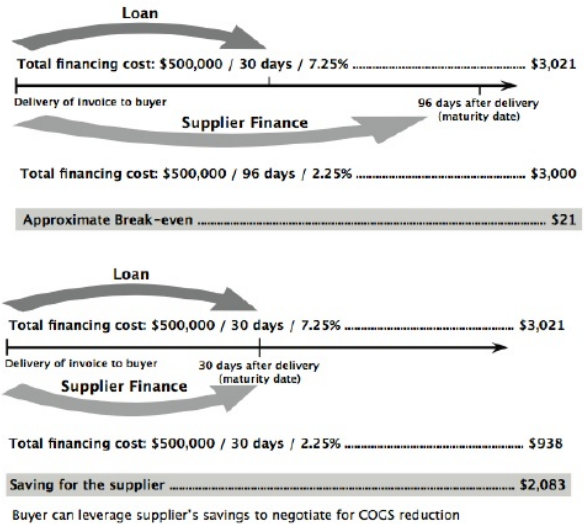
Given the lack of transparency of the supply chain, we see that most SMEs rely on margin money deposits for bank guarantees[12] or factoring houses to get loans. For example, in China, banks normally require 5-20% of the loan amount as a margin deposit depending on the credit risk of a SME. Fees charged by factoring houses can run as high as 15% of the loan amount every year[13]. With the combination of a PMSA and improved clarity on each deal, potentially up to 15% of annual working capital loan for SMEs can be unlocked either by paying less to cover margin deposits or by eliminating the fee of the third-party guarantee company.

On the buyer side, a company with $10 million in revenue and a 60% cost of goods sold (COGS) ratio can experience a cash flow increase of $16.7k per day of extended payables ($10m * 60%/360 days=$16.7k). Parlaying that into a 60-day term extension on trade-credit would result in a potential annual working capital/cash flow benefit of $1 million for the buyer ($16.7k * 60=$1m).

Credit Rate Arbitration

The Eximchain platform enables anchor buyers to take advantage of their comparatively better credit ratings to offer SCF programs to fund their suppliers in return for extended terms, lower prices, and improved long-term relationships. In this "buyer-driven" model, the anchor buyer becomes the financier in the ecosystem.

For example, if a supplier's access to capital is 5 percentage points higher than the buyer's 2.25% financing rate, a simple calculation will show the buyer that a 30-day invoice for $500k can be extended to 96 days without adding costs to the supplier. On the other hand, if the buyer were to maintain the 30-day payment terms, the supplier could achieve a reduced carrying cost of approximately $2,083(representing 0.4% of the $500k contract). Armed with this knowledge, the buyer could negotiate a price reduction based on all, or some portion, of these savings. For a company with $10 billion in revenues and $600 million in COGS, even a 0.4% drop would equate to $2.4 million in savings[14].



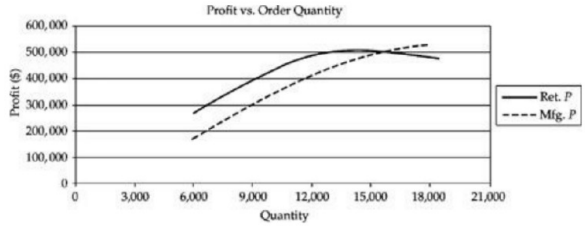
Supply Chain Optimization

The Eximchain platform also helps participants achieve global optimization, without the need for an unbiased decision maker, by allowing them to share the supply chain's risk and the potential benefit. Below is an example to quantify the value created for the supply chain based on a dynamic contract between a supplier and buyer:

Assume the price of a product for the end customer is

$125 per unit, the wholesale price paid by the retailer to the manufacturer is $80 per unit, the fixed production cost for manufacturer is $100k, the variable production cost per unit is $35, and any item unsold in the end has a salvage value of $20. This implies that the retailer's marginal profit for selling a unit: $45, is smaller than the marginal loss: $60*. The optimal order quantity depends on marginal profit and marginal loss. So the retailer's optimal policy is to order 12k units for an average profit of $470k as shown on below graph Profit vs. Order Quantity. If the retailer places this order, the manufacturer's profit is $400k ((12k*($80-$35))-$100k=$440k). Note that in this case, the retailer assumes all of the risk of having more inventory than sales.

By using a Buy-Back Contract where the manufacturer offers to buy unsold items from the retailer for $55, the retailer's marginal profit: $45, is now greater than its marginal loss: $35, thus motivating the retailer to order more than average demand. In this case, the retailer has an incentive to increase its order quantity to 14k units, for a profit of $513.8k, while the manufacturer's average profit increases to $471.9k. Thus, the total average profit for the two parties increases from $910.7k, (=$470,7k+$440k) in the sequential supply chain to $985.7k (=$513.8k + $471.9k) when a Buy-Back Contract is used. The Eximchain platform allows the retailer and manufacturer (i.e. the buyer and supplier) to share the additional $75k in profit generated from this contract based on their consensus[8].



*– Marginal profit/loss is the profit/loss of a firm or individual when one additional unit is produced and sold. Marginal profit and loss determine the optimal ordering quantity- the ordering quantity that gives the maximized profit for a firm or individual.

Supply Chain Provenance

Using smart contracts and a token system, Eximchain can expand the supplier-buyer-financier model and help buyers to gain visibility over the whole supply chain by interacting with upstream suppliers.

Process Automation

Eximchain helps to automate the negotiation and contracting process through private communication channels. Both buyers and suppliers can stop wasting time on tracking the supply chain process flow manually and will, instead, be able to maintain an audit of the final agreed upon contract in real-time through Eximchain's trustless network and secured protocol.

6. ECOSYSTEM

Introduction

Eximchain streamlines complex multi-party transactions in SCF by using blockchain to solve information asymmetry problems. We recognize that partnerships and a **minimum viable ecosystem (MVE)**, rather than a minimum viable product, are crucial to successfully bringing a new blockchain solution to market.

MVE: The smallest configuration of elements that can be brought together and still create unique commercial value

MVE

Combining a Blockchain, SDK, and Platform layer is necessary to bring enough players to bear for a healthy minimum viable network. Eventually, others will be able to develop solutions on our platform and make them immediately available to parties on the chain. In order for a blockchain to work, the computers on the system must validate and agree that a transaction was completed. This is accomplished by agreeing on a sequence of 'blocks' which each contain a set of transactions. BTC, for example, incentivizes participation in consensus by rewarding the first user to propose and validate a new block at each canonical height. Importantly, our design draws a distinction between nodes capable of proposing and validating blocks.

Blockchain

Technical challenges with blockchain technology have kept corporate players at bay. At the time of this writing, further research and development for the full potential of this technology to be realized are required on the Bitcoin and Ethereum main nets. These are:

Scalability- All smart contract code must be executed by all participants on the network.

Privacy- All information on a public blockchain is visible to all participants to read.

Faced with the choice of waiting for Ethereum to end the Ice Age[15] and release Casper in the coming years, or building on recently produced viable solutions in this area, we have chosen to leapfrog the Ethereum Roadmap by leveraging Quorum, an enterprise focused version of Ethereum released by JP Morgan. Quorum allows us to leverage Constellation[16] and a minimal Ethereum client fork to offer:

Confidentiality- private transactions secured by the network

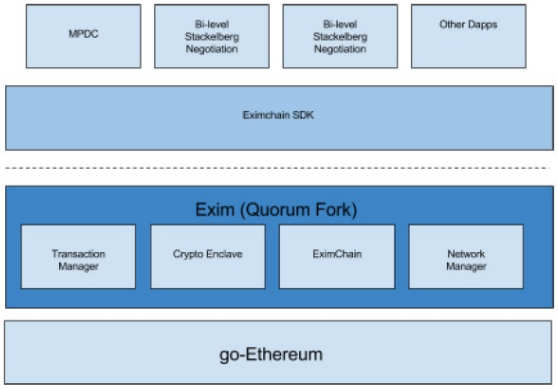
Performance- performance increases to handle the load that complex private transactions place on the network.

Consensus- permissioned consensus and governance rules to drive new economic incentives at the protocol level.

Quorum, and therefore Eximchain, is designed to develop and evolve alongside Ethereum. Because it only minimally modifies Ethereum's core, we are able to incorporate the majority of Ethereum updates quickly and seamlessly[17]
.

At the lowest level, we are modifying how the ethereum client protocol enables consensus and permissions the blockchain. Our blockchain distinguishes between participants that can validate blocks and participants that can propose blocks. The latter allows us to both secure priva-

te transactions on the network and incentivize developers to participate in the evolution of our environment.



Consensus

Rather than proof-of-work (mining), Eximchain uses a vote-based consensus algorithm that forks QuorumChain to add a few governance rules. The governance mechanism is included in the appendix for completeness; implementation details can be found here.

Settlement Finality

The recent development on Istanbul BFT (Byzantine Fault Tolerance), which will be incorporated into Quorum, ensures settlement finality and speeds up settlement time to under 1 second from the current tens of seconds to tens of minutes.

7. GOVERNANCE

The reason why Eximchain chose to use Quorum is because the current proof of work-based blockchains like Bitcoin and Ethereum are not ready for enterprise-grade solutions (details to be described under Appendix- Motivation). We believe the incentives of developer pools, clients, and corporates contributing value to the ecosystem must be aligned at the protocol level. This governance model can be applied to other public, permissioned blockchains that are looking to address similar issues.

Our proposed quadratic voting-based governance model allows for a series of checks and balances between nodes. We analyze how a voting system-based consensus model draws a clear line between safety and liveness: the percent vote required for consensus trades safety for speed. We analyze the counter balance of power between actors in the system, proposing a model that discourages collusion and analyzes the robustness of the protocol to keep block proposers and validators in check under: **independent choice, coordinated choice, and a bribing adversary.** We conclude by analyzing several failure modes of the system and subsequent recovery.

Voting Smart Contract[17]

Quorum Consensus Process Flow [17]

Quorum Consensus Block Creation [17]

Quorum Consensus Block Voting [17]

Maker Nodes

Maker Nodes are responsible for proposing blocks and their addresses are registered in the BlockVoting contract. The initial set of Maker Nodes is pre-configured in the genesis block and will be comprised of our initial token holders who we expect will add strategic value to the project, however once the network is established, this will begin to change as described below.

Maker Nodes will have the responsibility of voting in a new Maker Node every governance cycle. Nodes can opt to become Maker Nodes if they are KYC approved and voted in by an agreed threshold of existing Maker Nodes according to the Quadratic Voting Governance Mechanism.

Validator Nodes

Validator Nodes help to secure the network and they are also registered in the BlockVoting contract. They are responsible for voting to determine which block will be the canonical hash at a particular height. Like Maker Nodes, the initial set of Validator Nodes is pre-configured in the genesis block.[18]

Registered Voter Nodes

Registered Voter Nodes tie real world identities of nodes. All nodes (including Maker Nodes, Validator Nodes, and other network participants) are required to register to vote in order to participate in network governance mechanism. Registered Voter Nodes will have the responsibility of voting out a Maker Node every governance cycle and may be voted in as Maker Nodes once the network is established.

Governance Analysis

It is important to consider the evolution of the system and stakeholders in the face of dishonest nodes (traitors) and incentive driven collusion.

Recent developments in permissioned distributed ledger technology (DLT) have enabled us to design novel consensus rules that allow for a fundamental change in the underlying incentive mechanism and actors that underlie the consensus protocol of permissioned, public chains.

The desired outcome is to keep a cohort of dishonest nodes from gaining control of the block proposal mechanism or forking the chain, while bootstrapping a cohort of honest nodes with vested interest to protect the network and punish potential traitors. In the face of an undefeatable adversary leading to mechanism failure we analyze the time, collusion, and resources required for such an attack.

While not strictly necessary for the purposes of this analysis, it is important to keep in mind the real world identities behind these nodes will largely represent corporate incentives in the global supply chain and development communities. Ultimately, we believe the incentives of these stakeholders must be aligned at the protocol level. It follows that developers have a vested interest and duty to secure the infrastructure their applications, clients and corporates rely on. Similarly, clients and end-users have a vested interest

in ensuring honest development that improves the ecosystem, as well as a vested interest in punishing freeloaders on the network. The latter reflects our view that Maker Nodes should represent developer pools, motivating clients and end-users to become Registered Voter Nodes to participate in governance.

In all cases, while attacks on the network yield several failure cases, the confidentiality of private data stored on the blockchain is preserved. That is to say, protocol or governance failure does not necessarily entail breach of security to private data as long as private keys remain secure.

Adversary under independent choice

The consensus algorithm and governance is not fully open to any client issuing commands. Under independent choice, stakeholders have no incentive to deviate from the protocol as their attack would be defeated by the network. Nodes cannot single-handedly confirm the proposed block at each canonical height. Maker Nodes who deviate from the protocol would reveal their intentions to the network, placing themselves at risk of being voted off the Maker Node pool in the next governance cycle. Both Maker Nodes and Validator Nodes have a history of who voted them into the system, by a majority Maker Node vote and by invitation respectively; in this way the reputation of known traitors is linked to other nodes on the system (and real world entities) visible to anyone in the voting smart contract.

Adversary under coordinated choice

Assume an undefeatable, coordinating, racket of dishonest nodes who by a series of governance cycles gain control of a majority of block maker nodes that would allow them to control block proposal to deviate from the protocol. The consensus algorithm is not fully open to any client issuing commands; taking control of block maker governance requires traitors to be voted into the block maker pool.

Assume all nodes in the initial block maker pool of **size k**, under irrational choice, consecutively vote into the pool: an undefeatable coordinating racket of dishonest block maker nodes of size, m, over a sequence of n governance cycles. We analyze the cost, coordination and time required to launch an optimal attack and fool the network.

Let b[1], b[2], . . . , b[n] denote the nodes added to the block maker pool and s[1], s[2], . . . , s[n] the nodes removed from the block maker pool over n governance cycles length T. A **k-strategy** is a sequence that allows the coordinated adversaries to control block proposal after a sequence of n governance cycles by voting in m nodes without replacement.

$(b1, s1) \rightarrow (b2, s2) \rightarrow ..... (bm, sm)$; $m \leq n$,

where worst case, m=n and $m > \frac{1}{3}$ k, assuming a traitor is added each cycle and an honest node is removed. If the adversaries can assure the above, it is left up to the reader to see coordination of the attack requires collusion of $\frac{1}{3}$ k nodes over a minimum attack duration, $P = \frac{1}{3}$ kT before our strong assumption of k honest initial nodes fails.

For a concrete example, k= 2048, T = 2 weeks , a perfectly coordinated attack to control block proposal would take **26 years** and coordination of **683 parties**. Each must be capable of convincing honest nodes representing the developer pools, clients, and corporates that they are contributing value to the system throughout the duration of the attack to keep any of them from being voted out at each governance cycle and extending the minimum attack period.

Undefeatable Bribing Adversary

Assume an undefeatable bribing adversary who by a set of highly unlikely events, knows exactly which nodes will propose the next sequence of n blocks and the price required to bribe each one to propose a tampered block. Assume all nodes will commit treason for a price, the undefeatable bribing adversary has resources k at his disposal, and is driven by profit incentive. We analyze the cost of such an attack, m, over a sequence of n blocks.

Let b[1], b[2], . . . , b[n] be nonnegative integers that denote the price required to bribe each block-proposer to confirm the proposed block at each canonical height, over n blocks. A k-strategy is a sequence that allows the adversary to control block proposal over a sequence of n blocks for a price m.

$1 \leq b1 < s1 < b2 < s2 < .... < bm < sm \leq n$,

where m is a positive integer less than or equal to k. The profit corresponding to the strategy is the total reward obtained if you bribe the network for b1, and profit s1 from controlling a fixed number of transactions for one block, bribing the network for 2 blocks at b2, profiting s2 from controlling a fixed number of transactions for two blocks, and so forth. If the adversary can calculate the profit from controlling each proposed block p[1], . . . , p[n] it is trivial to design an algorithm for the adversary to compute a k-strategy with maximum profit.

Governance Level Attack

A similar k strategy could be designed to control governance over n vote cycles at cost m to an undefeatable bribing adversary.

Our governance model is unique in that nodes have the responsibility of periodically voting out Block Maker nodes counterbalanced by block maker nodes being able to appoint a replacement. We make an analogy to Block Makers as generals and other nodes registered to vote as soldiers to reason in laymen terms. You can say that governance level attacks are part of the protocol and built into the system to discourage majority collusion. Under similar assumptions as above, we expect generals (Block Makers) to appeal to soldiers (registered voters) to defend their status. A coalition that controls over $\frac{1}{2}$ of tokens could vote out any general they chose, we expect this to incentivize generals to spin up soldiers in their control to defend their status the only way the protocol allows: by voting out another general not in their coalition, simultaneously improving network security.

Governance Hardening

Assuming an initial token supply of X tokens, we analyze the case where an adversary owns X-1 tokens and is attempting to gain control of the governance mechanism. We analyze the minimum cost of controlling a sequence of n governance cycles with length T of an undefeatable attack

strategy. We analyze the cost and time required from an undefeatable adversary to maintain control of the network. Our governance model implements **quadratic voting** making the cost of each v votes for a governance decision cost v^2 tokens, all tokens paid are then redistributed equally among the voting pool. To assure control of the first governance cycle, the adversary must place 2 votes at a cost $v[1]^2 = 4$ tokens, controlling X- 5 of the token supply in the second cycle, to assure control of the next cycle, the adversary must place 6 votes at cost $v[2]^2 = 36$ to beat the possible 5 votes against his governance decision; this can continue to scale this way until $v[k]$ where the marginal cost of k nodes voting against the adversary increases:

(votes1, cost1) → (votes2, cost2) ... → (votesn, costn)

Optimal Defense : (1, 1) → (4 , 4) → (25, 25) → (676, 676) → (k-1 , k-1)

Optimal Attack: (2, 4) → (5 , 25) → (26, 676) → (677, 458329) → (k, k^2)

Sequence of optimal voting decisions for an attacker would cost:

$1 + 4 + 25 + 676 + 458329 + 210066388900 + ... + v[k]^2 < X - 1/2$

By correctly parameterizing the system it is possible to prove an adversary can control a bounded number of governance cycles that can be defeated by k honest nodes.

Counter Measures

The premise of attack from a bribing adversary is a valid concern if we are to expect the value of the network to scale as the square of connected users [Metcalf's Law]. Perhaps unsurprisingly, distributed concentrations of wealth and a smaller block size discourage bribing people to deviate from the protocol for profit incentive. In practice, the non deterministic choice of block proposers using random timeouts limits the calculation of such a k-strategy by an undefeatable bribing adversary. The cost of the k-strategy to launch a governance or protocol level attack scales inversely to the percentage of validators required for block confirmation and number of nodes on the network. Our proposed governance model allows for a series of checks and balances between nodes. We are experimenting on mechanism design trade offs on our testnet and will make our results public in the coming year.

Bootstrap Mechanisms

QVEC- Quadratic Voting on Ethereum Chain

Peacekeepers

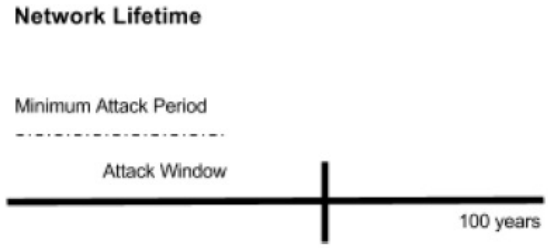
These are k = safety_factor * initial_token_holders_participant nodes originally launched as block makers to defend the network and are registered in the voting contract as part of the bootstrap mechanism; these nodes participate in consensus but are forced to abstain at each governance cycle. They will be first to be voted off the block proposer pool to make room for new Maker nodes, allowing the ecosystem to become fully decentralized over time while ensuring the minimum attack period of an undefeatable adversary cannot be realized in the infancy of the network.

Quadratic Voting

Nodes can make v votes for a governance decision by paying v^2 tokens, from there it's just a majority vote. All funds raised are returned by giving back to each individual in the voting pool,1/(voting_pool-1) of the funds paid by the voter. The theory is that if someone gains x from a decision being made, and each vote has a probability p of being pivotal, then they have the incentive to keep buying votes for as long as the price of the next vote is less than px. Because the total price of v votes is v^2, and we know from calculus that the derivative of v^2 is 2v, users will have the incentive to keep spending tokens until 2v > px; hence, they will spend v = px/2 tokens. You can see from this math that the number of tokens that a voter buys should be proportional to x, ie. the amount that they gain from the decision being made. Hence, the number of votes that a voter makes should actually reflect the strength of their preference, and not just which option they prefer.[19]

Finite Attack Window

It would be irresponsible of us to claim undefeatable adversaries are unlikely in practice* or claim that the protocol will defend the network indefinitely, rather we choose to err toward practical guarantees that ensure network safety by attempting to bound the minimum attack period and cost of an undefeatable adversary. It follows shortly that given an unbounded amount of time a determined enough undefeatable adversary would eventually be able to launch a successful attack. The only way to hedge against this is to ensure a finite possible attack period in a similar time scale to the minimum attack period of an undefeatable adversary. In 100 years, the voting contract will suicide halting all further change of state in the network, triggering open-source licences on any remaining proprietary portions of our software.



*For example a single blockchain enabling Export/Import (or any other value exchange for that matter) could become a military or terrorist target.

8. APPLICATION

At a higher level, we are creating a smart contract SDK. The smart contract SDK layer will allow developers to build applications from basic components, accelerating development of future SCF solutions.

We want to enable the engineering of monetary systems and make implementation of monetary theory, economics and law accessible to developers. The first step is enabling the implementation of systems that can be reduced to modeling the strategic interaction between two or mo-

re players,specifically in situations containing a set of rules, outcomes, and desired objectives. Participants can build supply chain applications on top of the Eximchain smart contract SDK:

Our aim is to show developers how our SDK easily supports complex multi party transactions, enabling them to build applications and other supply chain finance products on top of our ecosystem.

Smart Contract SDK

Financing: Through instant and transparent proof of order verification on blockchain, suppliers seize early payment discounts to improve working capital and buyers seize credit arbitrage opportunity.

Procure-to-Pay: Participatants can maintain an audit of the final agreed upon contract in each step of the procure-to-pay process in real-time through a trustless network and secured protocol.

Sourcing: Sourcing platforms or rating agents can use the Proof of Existence (PoE) functionality- document time stamping, verifying document integrity, demonstrating data ownership without revealing data, to provide independently verifiable reputation data.

Inventory Management: By sharing real-time demand information cross the supply chain, participants can make better inventory plans and automate the reconciliation process across different ledgers and systems to save time and reduce cost.

Supply Chain Optimization: Using Multi-Party Dynamic Contracts - a combination of private channels and a configurable state machine to coordinate a confidential bi-level stackelberg SCF negotiation (as described in Appendix).

Supplier Management: Using smart contracts and a token system, Eximchain can help buyers to gain visibility over the whole supply chain by interacting with upstream suppliers but still maintain privacy on each transaction level.

Risk Mitigation: Eximchain enables dynamic, real-time monitoring of supply chain processes to provide visibility into the whole supply chain's operations. Participants can manage risks in one place.

Private channels

Series of confidential two way channels coordinated by the FSM (Finite State Machine).

FSM

Coordinates rules and implements mechanisms modeling the strategic interaction between two or more players. Takes the shape of coordinating information exchange between a number of two way private channels through a semaphore notion and embedded mechanism design.

Strategy Computation Machine

We consider the design of Computational Game-Theoretic Frameworks - machine games, where we replace strategies by Turing machines (smart contracts)[20]. For example, given the state of a game, a strategy computation machine may return a distribution over possible actions, the complexity of the computation depends on implementation of the machine but the interface can be clearly defined.

Platform development status and plan

Q3-Q4 2017

Signed letter of intents from 9 companies including SMEs, a listed company in China and a cross-border e-commerce platform.

A Strategic Cooperation Agreement with Guiyang High-tech Industrial Development Zone Management Commission and Guiyang Big Data Development and Management Commission, China.

Current Stage (Q4 2017- Q1 2018)

Governance hardening

First POC in Supply Chain Sourcing

Large scale network testing

Token Generation Event

In the next few months, Eximchain will launch several testnets and onboard SMEs to execute smart contract based solutions through the network.

Release 2.0 (Q2 to Q3 2018)

Native Token Swap

Mainnet Launch

First Governance Cycle

Second POC in Supply Chain Financing or Inventory/Logistics Management

First SDK Release

Release 3.0 (Q4 2018 to Q1 2019)

Second SDK release

Second Governance Cycle

Third POC in Supply Chain Financing or Inventory/Logistics Management

Over the next 15-18 months, our platform will enable participants in the global supply chain to launch their own supply chain management tools using our smart contract SDK.

9. TEAM AND ADVISORS

Team

Hope Liu, CEO of Eximchain, B.A. from Peking University and MBA from MIT, handled cross-boarder transactions at UBS Beijing, Hong Kong and Singapore for 6.5 years. She is the Lab Lead of the North America Blockchain Association and has been working on Eximchain project from MIT Media Lab since 2015. She led the team to win the grand champion of Boston Seagull Entrepreneurship Competition and has been featured by mainstream blockchain medias in U.S.

Juan Huertas, CTO of Eximchain, B.S.in Computer Science from MIT. He started coding at age 13 and has been a Technology Consultant for startups since he was 18 years old. He built a cryptocurrency enabled game to play and distribute cryptocurrency anonymously during his junior year in college at MIT.

James Xu, Architect of Eximchain. He worked in IBM for 14 years holding various positions across the globe as enterprise packaged software offering manager, Delivery Project Executive of a team 100+ across 14 time zones, and Associate Partner managing key account in China. He has extensive exposure in supply chain management, retail, CPG and global trade domains. He also co-founded a startup, building a EV car sharing platform.

Jia Zhang, Business Analyst of Eximchain. Jia has been in supply chain field since 1994. She spent 7 years in ICBC managing global trade finance and international settlement. After that, she acted as the Chief Representative of MS Textiles in China for almost 10 years, managing local supplier relationships, goods inspection, and logistics arrangement. She speaks Chinese, English and French.

Louis Lamia, Director of Engineering and Infrastructure at Eximchain, B.S.in Computer Science from MIT. He was a Software Development Engineer at Amazon Web Services on the Elastic File System team for over 2 years involved in various projects, most notably encryption-at-rest.

Douglas Sanchez, Director of Product at Eximchain, B.S.in Computer Science from MIT. Before joining Eximchain, he was leading industrial, product and brand design for Tulip, a manufacturing app platform startup in Boston.

Advisors

Ramble Lan is the president of NABA (North America Blockchain Association), Chief Architect of the Regulatory Sandbox in Guiyang, China, and the Chairman of Supply Chain Blockchain Association in Fujian, China. He is also the CEO of SwftCoin (www.swftcoin.com).

Tiger Zhong is the CEO of Trademanger (www.Trademanager.com)- a platform that provides big data services for small and medium sized business in global trade with over 50k active users. He has experience providing services to small and medium size business in China for over 16 years.

Catherine Dai is the Founder and Owner of BoaoTech and HongKong Boao, Co-Founder and Shareholder of GiboStar Int'l. She plays Angel/VC role for 16 companies ranging from TMT, Biopharmaceutical, Heavy industry, to Garment, Catering, and Entertainment Industry in China.

Daniel Wang is a China based, U.S. trained executive with extensive transactional background. He is currently the director of investment of a Fortune 500 company, and used to be an attorney practicing in Silicon Valley, Hong Kong and Mainland China.

Can Kisagun is a co-founder at Enigma- a data-driven crypto investment platform that raised $45m during Token Generation Event in 2017. Previously Can worked at McKinsey & Company for 3 years focusing primarily on finance and banking engagements. Can holds an MBA from MIT Sloan and BS in Industrial Engineering from Northwestern University. Prior to Enigma, Can was a co-founder of Eximchain.

Peter Missine established himself as an independent strategy consultant after a few years at McKinsey & Co. Prior to his MBA at MIT Sloan, Peter spent five years as an international commodity trader on three continents for Louis Dreyfus Commodities (LDC). At LDC he also worked with international trade flows, supply chains, transfer pricing and anti-dumping.

Manmeet Singh is currently the managing partner of Blockseed Venture, Expert-in-Residence at Chinaaccelerator and the Investment Advisor for Nanjing Municipal Government. He previously run an Asia focused financial advisory firm and was the China Representative of ICIC Bank.

William Peckham is the Managing Partner of Proteus Growth, a cross border strategy consulting firm based out of Beijing, as well as China Operating Partner of Higher-Order VC, a crypto currency fund. He has served as an advisor to numerous foreign tech startups in China including Robomed, Enigma, Rogue Initiative, INS Ecosystem, and Quintype.

10. TOKEN AND PARTICIPATION

Eximchain Platform Native Tokens (Eximcoins) will be used to pay network fees, validate state changes, and execute governance. Eximcoins will also be used to access applications built on the Eximchain network developed with the Eximchain SDK.

Token Structure

Because Eximcoins will be native to the permissioned fork of the Quorum blockchain which will be integrated into the Eximchain platform and will only be available when the platform is deployed for commercial use (Mainnet Launch) (which is expected to occur in Q2 2018), Eximchain plans to sell a digital token native to the Etherium blockchain that will be a precursor to Eximcoins (EXC Tokens) (the sale of EXC Tokens, "Token Sale"). EXC Tokens will be ERC-20 compatible tokens distributed on the Ethereum blockchain pursuant to a related ERC-20 smart contract. Shortly before Mainnet Launch, EXC Tokens will be permanently frozen and not capable of being used for any purpose, in preparation for being converted into Eximcoins. Each EXC Token will be automatically converted to one Eximcoin at Mainnet Launch.
Total supply of EXC Tokens: 75,000,000
Fundraising target: US$20m equivalent

Token Distribution

Token distribution:
Sold during Token Sale: 60,000,000
Bonus Account (including airdrop): 15,000,000

Sold during Token Sale: No more than 60,000,000 EXC are to be sold to buyers. Each token will be sold for the ether

equivalent of approximately US$0.33. There will be no bonus or discount available to contributors during the Token Sale.

Bonus Account: 15,000,000 EXC Tokens from the total EXC Token supply will be allocated to a bonus account. Approximately 10% of the EXC Tokens in the bonus account will be allocated for an Airdrop, as described below. The remaining EXC Tokens in the bonus account will be reserved for distribution by Eximchain in its discretion to marketing and community partners during the EXC Token generation event and participants in the Eximchain Bounty Program.

Airdrop: In conjunction with the private sale, Eximchain plans to conduct an airdrop of EXC Tokens to persons who were placed on a whitelist of persons who expressed an interest in purchasing EXC Tokens but who did not participate in the private sale. Eximchain will deliver a small quantity of EXC Tokens (valued at about US$200) to each such person for free.

Conversion of EXC Tokens to Eximcoins

Shortly before Mainnet Launch, the EXC Tokens will be permanently frozen and not capable of being used or transferred for any purpose, in preparation for being converted into Eximcoins. At Mainnet Launch, all EXC Tokens will be automatically converted to Eximcoins on a one-for-one basis. An additional 75,000,000 Eximcoins will also be created and distributed at Mainnet Launch, as follows:

o 30,000,000 Eximcoins will be allocated to a promotional account that Eximchain will manage to promote the use of the platform by SMEs and early adopters to be selected by Eximchain in its discretion over a 10-year period. It is important that Eximchain token holders plan to use our supply chain solutions and participate in the early stages of the Eximchain governance mechanism. Eximchain will distribute Eximcoins from the promotional account as an incentive for early stage participants who will use the Eximchain platform to conduct contract negotiations, build supply chain products and participate in network governance. SMEs interested in applying for tokens to cover development and prototype phases will need to sign a Commitment Letter or Letter of Intent to qualify.

o 30,000,000 Eximcoins will be distributed to the Eximchain founding team and advisers.

o 15,000,000 will be allocated to a reserve account that Eximchain will manage in its discretion to assure there are sufficient Eximcoins in circulation for use on the platform.

The Eximcoins allocated to the promotional account will be locked (incapable of transfer or use) and will be unlocked during the 10-year period beginning at Mainnet Launch in equal monthly allotments.

The Eximcoins distributed to Eximchain's team and advisers will be locked and will be unlocked during the 4-year period beginning at Mainnet Launch in equal monthly allotments.

The Eximcoins distributed to the reserve account will be locked and will be unlocked at the end of the 2-year period beginning at Mainnet Launch.

Token Sale Timeline

Token Sale: Q1 2018
Mainnet Launch and start token listing process: Q1-Q2 2018
List tokens on multiple exchanges: Q2-Q3 2018

Use of Funds

Eximchain intends to use the funds from the sale of EXC Tokens at the Token Sale for the following primary purposes:

Platform Development: This includes maintaining competitive salaries for top talent in China and the U.S. paying for software hosting, accelerated development of legacy system integrations and acquisition of hardware. The hardware and hosting will be offered to anchor buyers and that will need stand- alone computers to manage their respective supply chains on a global scale.

Build the Supply Chain Ecosystem: This includes effort to onboard SMEs through incentivizing early stage users and on-going business development to onboard suppliers, buyers and financiers. Eximchain will reserve a proportion of tokens for this purpose in a secured wallet to ensure fair distribution.

Operational Expenses: This includes basic operational costs such as office space, legal costs to pursuing and obtaining required licenses, and security measures.

However, Eximchain may in its discretion use those proceeds for any purpose, whether or not consistent with the foregoing. Eximchain makes no undertaking, representation or warranty in respect of its use of such proceeds.

Participation

Eximcoins will only be minted in the genesis block, associating them with the wallet addresses of the holders of EXC Tokens. EXC Tokens will only be minted while the contract is active.

The private sale registration was closed on Jan 11th 2018. In conjunction with the private sale, a total US$500k worth of EXC Tokens are available for airdrop. Only participants on the whitelist can join the airdrop process. The Token Sale KYC process is scheduled to continue through to March 2018. All participants in the Token Sale, including airdrop participants, must complete our KYC-AML process.
The whitelist registration was closed on Jan 16th 2018.

We invite engagement and dialog on our business model and our ecosystem design. The opportunity that these technologies will unlock for businesses of all sizes is remarkable and we need public involvement to fulfill that mission.

To become a part of our community, give us feedback on the whitepaper or just to find out more about Eximchain:

Visit our website at www.eximchain.com .

Join our Telegram channels.

Follow us on Twitter.

Or email us at hello@eximchain.com.

11. LEGAL CLARIFICATION

Eximcoins are utility tokens whose entire value derives from the services provided by the Eximchain platform in exchange for holding or consuming the tokens, as detailed above. They are not intended for speculation and hold no claim to intellectual or other property or cash flows. They grant no right to participation in the company, and no claim in decision making over company assets or strategy. There is no promise of value or claim on revenue associated with EXC other than that derived from platform usage. In short, EXC are not securities. Also, the estimations under Value for our Stakeholders are based on assumptions and there can be no guarantee that they will be achieved. Actual results may vary substantially from the figures shown.

DISCLAIMER OF LIABILITY

To the maximum extent permitted by the applicable laws, regulations and rules, Eximchain shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you.

NO REPRESENTATIONS AND WARRANTIES

Eximchain does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper.

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), you represent and warrant to Eximchain as follows: (a) you agree and acknowledge that the EXC tokens do not constitute securities in any form in any jurisdiction; (b) you agree and acknowledge that this Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities in any jurisdiction or a solicitation for investment in securities and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper; (c) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this Whitepaper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with; (d) you agree and acknowledge that this Whitepaper, the undertaking and/or the completion of the Eximchain Initial Token Sale, or future trading of the EXC tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of the Eximchain , the EXC tokens, the Eximchain Initial Token Sale and the Eximchain Wallet (each as referred to in this Whitepaper); (e) the distribution or dissemination of this Whitepaper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to Eximchain ; (f) you agree and acknowledge that in the case where you wish to purchase any EXC tokens, the EXC tokens are not to be construed, interpreted, classified or treated as (i) any kind of currency other than cryptocurrency; (ii) debentures, stocks or shares issued by any person or entity (whether Eximchain) (i) rights, options or derivatives in respect of such debentures, stocks or shares; (ii) rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss; (iii) units in a collective investment scheme; (iv) units in a business trust; (v) derivatives of units in a business trust; or (vi) any other security or class of securities. (g) you are fully aware of and understand that you are not eligible to purchase any EXC tokens if you are a citizen of China, or a citizen, resident (tax or otherwise) or green card holder of the United States of America; (h) you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology; (i) you are fully aware and understand that in the case where you wish to purchase any EXC tokens, there are risks associated with Eximchain and the Distributor and their respective business and operations, the EXC tokens, the Eximchain Initial Token Sale and the Eximchain Wallet (each as referred to in the Whitepaper); (j) you agree and acknowledge that neither Eximchain nor the Distributor is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you; and (k) all of the above representations and warranties are true, complete, accurate and not misleading from the time of your access to and/or acceptance of possession this Whitepaper or such part thereof (as the case may be).

CAUTIONARY NOTE ON FORWARD LOOKING STATEMENTS

All statements contained in this Whitepaper, statements made in press releases or in any place accessible by the public and oral statements that may be made by Eximchain or their respective directors, executive officers or employees acting on behalf of Eximchain or the Distributor (as the case may be), that are not statements of historical fact, constitute ”forward-looking statements”. Some of these statements can be identified by forward looking terms such as äim”, ”target”, änticipate”, ”believe”, ”could”, ëstimate”, ëx-

pect", ïf", ïntend", "may", "plan", "possible", "probable", "project", ßhould", "would", "willör other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding Eximchain's financial position, business strategies, plans and prospects and the future prospects of the industry which Eximchain is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to Eximchain's revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this Whitepaper regarding Eximchain are matters that are not historic facts, but only predictions. These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of Eximchain to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others: (a) changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which Eximchain conducts its respective businesses and operations; (b) the risk that Eximchain may be unable or execute or implement their respective business strategies and future plans; (c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies; (d) changes in the anticipated growth strategies and expected internal growth of Eximchain ; (e) changes in the availability and fees payable to Eximchain in connection with their respective businesses and operations; (f) changes in the availability and salaries of employees who are required by Eximchain to operate their respective businesses and operations; (g) changes in preferences of customers of Eximchain ; (h) changes in competitive conditions under which Eximchain operate, and the ability of Eximchain to compete under such conditions; (i) changes in the future capital needs of Eximchain and the availability of financing and capital to fund such needs; (j) war or acts of international or domestic terrorism; (k) occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of Eximchain ; (l) other factors beyond the control of Eximchain ; and (m) any risk and uncertainties associated with Eximchain and their businesses and operations, the EXC tokens, the Eximchain token sale and the Eximchain business(each as referred to in the Whitepaper). All forward-looking statements made by or attributable to Eximchain or persons acting on behalf of Eximchain are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of Eximchain to be materially different from that expected, expressed or implied by the forward-looking statements in this Whitepaper, undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of this Whitepaper. Neither Eximchain nor any other person represents, warrants and/or undertakes that the actual future results, performance or achievements of Eximchain will be as discussed in those forward-looking statements. The actual results, performance or achievements of Eximchain may differ materially from those anticipated in these forward-looking statements. Nothing contained in this Whitepaper is or may be relied upon as a promise, representation or undertaking as to the future performance or policies of Eximchain. Further, Eximchain disclaim any responsibility to update any of those forward-looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future.

NO ADVICE

No information in this Whitepaper should be considered to be business, legal, financial or tax advice regarding Eximchain, the EXC tokens, the Eximchain token sale and the Eximchain business (each as referred to in the Whitepaper). You should consult your own legal, financial, tax or other professional adviser regarding Eximchain and their respective businesses and operations, the EXC tokens, the Eximchain token sale and the Eximchain business (each as referred to in the Whitepaper). You should be aware that you may be required to bear the financial risk of any purchase of EXC tokens for an indefinite period of time.

NO FURTHER INFORMATION OR UPDATE

No person has been or is authorized to give any information or representation not contained in this Whitepaper in connection with Eximchain and its respective businesses and operations, the EXC tokens, the Eximchain token sale and the Eximchain business (each as referred to in the Whitepaper) and, if given, such information or representation must not be relied upon as having been authorized by or on behalf of Eximchain token sale and the Eximchain business (as referred to in the Whitepaper) shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of Eximchain or in any statement of fact or information contained in this Whitepaper since the date hereof.

NO OFFER OF SECURITIES OR REGISTRATION

This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper. Any agreement in relation to any sale and purchase of EXC tokens (as referred to in this Whitepaper) is to be governed by only the terms and conditions (T&Cs) of such agreement and no other document. In the event of any inconsistencies between the T&Cs and this Whitepaper, the former shall prevail.

You are not eligible to purchase any EXC tokens in the Eximcoin Initial Token Sale (as referred to in this Whitepaper) if you are a citizen of China, or a citizen, resident (tax or otherwise) or green card holder of the United States of America. No regulatory authority has examined or approved of any of the information set out in this Whitepaper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

RISKS AND UNCERTAINTIES

Prospective purchasers of EXC tokens (as referred to in this Whitepaper) should carefully consider and evaluate all risks and uncertainties associated with Eximchain, the EXC tokens, the Eximchain token sale and the Eximchain (each as referred to in the Whitepaper), all information set out in this Whitepaper and the T&Cs prior to any purchase of EXC tokens. If any of such risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of Eximchain could be materially and adversely affected. In such cases, you may lose all or part of the value of the EXC tokens.

12. ACKNOWLEDGMENT

We would like to express our gratitude to the many people who supported us as we wrote this paper: Nina Yan, Zach Chen, Jessie Liu, Malak Alyousef, Louis Lamia, Steven Rivera, John O'sullivan and Sawan Jindal. Thank you.

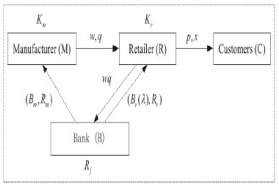
13. APPENDIX

Use Case Example

*Multi-Party Dynamic Contracting

Inspired by the system proposed in "Optimal bi-level Stackelberg strategies for supply chain financing with both capital-constrained buyers and sellers"[21] and "A partial credit guarantee contract in a capital-constrained supply chain: Financing equilibrium and coordinating strategy,"[22] below we provide an example of a Dynamic SCF system that can be created through the Eximchain platform.

In the supply chain financing system shown, we formulate the interactions between the capital-constrained buyer (Retailer), the capital-constrained supplier (Manufacturer) and the financier (Bank) as privately executed smart contracts that coordinate a bi-level Stackelberg game. The Bank acts as the leader in setting the financing rate for the Manufacturer and Retailer. The Manufacturer acts as the subleader to make the best response according to Bank's decision and to set the wholesale price for the Retailer at the same time. The Retailer acts as the follower to respond to both the Bank and Manufacturer.



Firstly, the leader (Bank) will evaluate the Retailer's and the Manufacturer's financing conditions (e.g., initial capital, bankruptcy risks and procurement/production quantities) and make optimal decisions to announce the interest rate Rr and Rm, respectively. Then, in response to the Bank, the subleader (Manufacturer) will simultaneously update his decision and decide how much to charge the buyer for the wholesale price w. Acting as the follower, the Retailer decides how much to order according to Bank's interest rate, Rr, and Manufacture's wholesale price. To pursue the result of the Stackelberg equilibrium, Retailer and Manufacturer select a best-reply policy, denoted by (4) and (5).

The model can be expressed as below:

$$
\begin{cases}
(Leader)\ \max\limits_{R_r,R_m} \pi_b(R_r,R_m;q,w)=\pi_b^r(R_r;q,\lambda)+\pi_b^m(R_m;w) & (1)\\
s.t.\ \pi_b^r(R_r;q,\lambda)=\min\left(B_r(\lambda)(1+R_r),E\left[p\min(q,x)+v(q-x)^+\right]\right)-B_r(\lambda)(1+R_f) & (2)\\
\pi_b^m(R_m;w)=\min\left(B_m(1+R_m),(w-c)q\right)-B_m(1+R_f) & (3)\\
q^*(R_r,w)=\arg\max\limits_{q}\pi_r(q;R_r,w,\lambda) & (4)\\
w^*(R_m,q)=\arg\max\limits_{w}\pi_m(w;R_m,q) & (5)\\
(Sub-leader)\ \max\limits_{w}\pi_m(w;R_m,q)=wq-(cq-K_m)(1+R_m) & (6)\\
s.t.\ K_m\le cq & (7)\\
(Follower)\ \max\limits_{q}\pi_r(q;R_r,w,\lambda)=E[p\min(q,x)+v(q-x)^+-B_r(\lambda)(1+R_r) & \\
\qquad +(K_r+B_r(\lambda)-wq)(1+R_f)]^+ & (8)\\
s.t.\ K_r\le wq & (9)
\end{cases}
$$

The Eximchain ecosystem involves a single shared blockchain and a smart contract SDK. Besides the model mentioned above, our software architecture is tailored to implement many SCF products from basic components on our ecosystem. Ultimately, developers can use our software to create variations on Stackelberg Strategies or their own multi party SCF products.

MOTIVATION

As of writing, large mining pools control and secure proof of work based blockchains like Bitcoin and Ethereum, as the systems shift toward transaction based economies, and proof of stake respectively, the financial incentive provided to devote a large amount of hash power or coin holdings to secure the network will drive decentralized networks into the palms of a handful of mining pools. We believe it is important to distinguish the value these pools contribute to the chain by devoting resources to add security to the network, from the value developers contribute by adding novel functionality to the ecosystem.

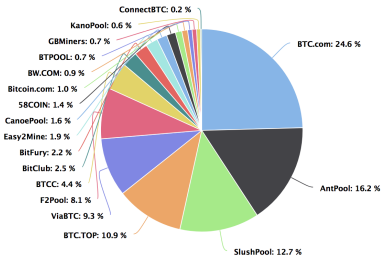
Recent developments in permissioned-DLT have enabled us to design novel consensus rules that allow for a fundamental change in the underlying incentive mechanism and actors that underlie the consensus protocol of permissioned, public chains.

We propose a system that grants developers, and members of our Token Generation Event a privileged position in the consensus protocol of the underlying blockchain, incentivizing and funding developer pools to add functionality to the system by allowing them to exclusively collect network rewards at the protocol level from state changes driven by Dapps on the network.

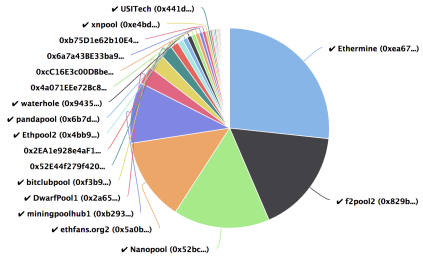
Today*, Ethereum and Bitcoin stakeholders (as a whole) keep mining-rigs humming to the tune of $5M and $6M per day respectively. Bitcoin, touted as the prime example of successful dPoW is majority controlled by a handful of mining pools, with no roadmap to alleviate the centralization of hash power. While the case is similar for Ethereum at present, we will have to wait and see how their transition to security deposit based dPoS will affect the distribution of block proposers and whether token holders begin to bond their ETH (which brings up peripheral concerns about illegitimate initial token holders who will have a huge incentive

to raise as much ETH as possible).

Hashrate Distribution - BTC March 2018



Hashrate Distribution - ETH March 2018



Considering a 66% attack is possible in both networks under collusion of less than 10 parties, it becomes clearer that the security of these ecosystems are largely hinged on the bounties available to these miners each day, none of whom contribute to the codebase of the underlying system that enables the creation of this value. The result is that mining pools have complete control over how the system evolves; in these networks, developers are second class citizens, constantly at risk of forks in a network that their applications, clients, and corporates rely on, forks that are ultimately decided by the mining groups profiting from their innovation and market speculation. Perhaps due to the latter, these networks look more like security rackets every day, where each additional dollar of network incentive gives you less security than the last dollar*. A new protocol is necessary to align network incentives with those of developers, clients, and corporates.

*consider that only 5 months ago Ethereum miners were getting paid $500k/day to secure the network compared to today's $5M/day

Consensus + Token FAQ

The token functions to keep the network incentivized to participate in consensus and governance. Our native token's primary use is to pay gas, a mechanism used to incentivize Block makers to process your transactions. Further all nodes registered to vote can make 'passive income' (don't particularly love the term) by participating in governance system via quadratic voting. 1000 EXC min required to participate in consensus mechanism, as a masternode, but note that this is not exactly PoS: nodes can be voted off the consensus mechanism irrespective of their wealth via quadratic voting governance. Masternodes are required to have 1000 EXC collateral, a dedicated IP address, and be able to run 24 hours a day without a more than a 1 hr connection loss, they claim 100% of the transaction fees in blocks they make.

14. REFERENCES

[1] Lotta Lind, Miia Pirttilä, Sari Viskari, Florian Schupp, and Timo Kärri. Working capital management in the automotive industry: Financial value chain analysis. *Journal of purchasing and supply management*, 18(2):92–100, 2012.

[2] Benefits Beyond Treasury: How Supply Chain Finance Impact the Bottom Line. Citi Transaction Services. `http://www.citibank.com/transactionservices/home/about_us/articles/docs/citi_insights_scf_updated.pdf/`, 2012.

[3] Peer Stein, Oya Pinar Ardic, and Martin Hommes. Closing the credit gap for formal and informal micro, small, and medium enterprises. 2013.

[4] Blockchain Platform for Supply Chain Finance Launches in China, CFO Innovation Asia, 2017.

[5] Small and Medium Enterprises (SMEs) Finance. The World Bank. `http://www.worldbank.org/en/topic/financialsector/brief/smes-finance/`, 2015.

[6] How Supply Chain Finance Can Close the Funding Gab for SMEs., 2016.

[7] Mckinsey on Payments, Supply-chain finance: The emergence of a new competitive landscape, 2015.

[8] David Simchi-Levi, Edith Simchi-Levi, and Philip Kaminsky. *Designing and managing the supply chain: Concepts, strategies, and cases*. McGraw-Hill New York, 1999.

[9] Chang Hwan Lee and Byong-Duk Rhee. Coordination contracts in the presence of positive inventory financing costs. *International Journal of Production Economics*, 124(2):331–339, 2010.

[10] Henry Sanderson and Neil Hume (2014), Qingdao fraud case taints commodity financing. Financial Times. `https://www.ft.com/content/b3cc4dc4-86ba-11e4-9c2d-00144feabdc0?mhq5j=e3/`, 2014.

[11] `https://www.investopedia.com/terms/p/purchase-money-security-interest-pmsi.asp//`.

[12] `http://www.investopedia.com/terms/b/bankguarantee.asp//`.

[13] Based on the prevailing rates on margin money deposit for bank guarantee and guarantee fee offered in China .

[14] Bob Dyckman. Integrating supply chain finance into the payables process. *Journal of Payments Strategy & Systems*, 3(4):311–319, 2009.

[15] Ethereum to end the Ice Age. `https://github.com/ethereum/go-ethereum/commit/71d32f54f70917c53fd3a691cface3bc73ffa1b7/`.

[16] Quorum allows leverage Constellation. `https://github.com/jpmorganchase/constellation/`.

[17] `https://www.jpmorgan.com/country/US/EN/Quorum/`.

[18] `https://github.com/jpmorganchase/quorum/wiki/QuorumChain-Consensus/`.

[19] `https://www.reddit.com/r/ethereum/comments/453sid/empirical_cryptoeconomics//`.

[20] Joseph Y Halpern and Rafael Pass. Game theory with costly computation. *arXiv preprint arXiv:0809.0024*, 2008.

[21] Nina Yan, Hongyan Dai, and Baowen Sun. Optimal bi-level stackelberg strategies for supply chain

financing with both capital-constrained buyers and sellers. *Applied Stochastic Models in Business and Industry*, 30(6):783–796, 2014.

[22] Nina Yan, Baowen Sun, Hui Zhang, and Chongqing Liu. A partial credit guarantee contract in a capital-constrained supply chain: Financing equilibrium and coordinating strategy. *International Journal of Production Economics*, 173:122–133, 2016.