Whitepaper

http://zoreum.com

Abstract

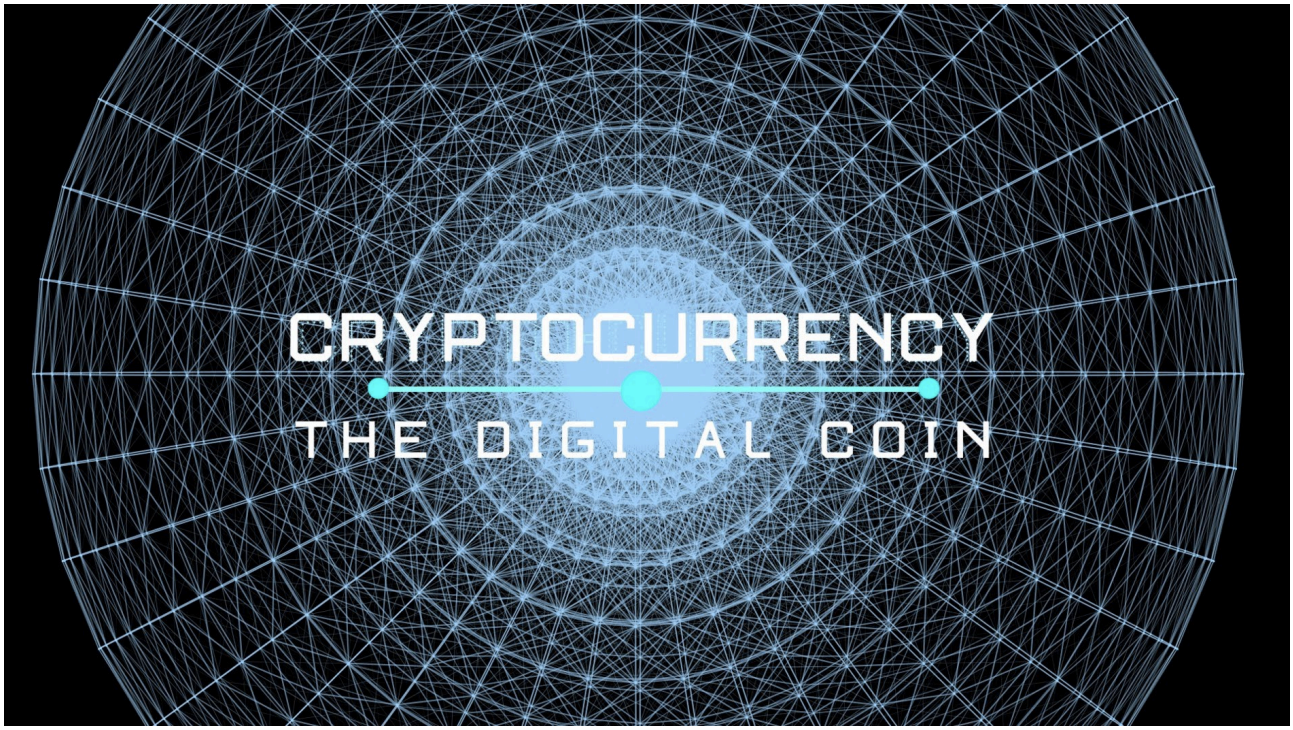
Today, cryptocurrencies are primarily traded on centralized exchanges where user funds are at risk to hackers and platform managers. Decentralized exchanges (DEXs) allow users to retain control of their funds as trades are mediated by smart contracts on a blockchain, but on-chain computation is generally too slow to keep up with high volume order books. This paper describes Zoreum Labs ZRS shares. Primary service is to develop a Semi Decentralized exchange and Decentralized applications (dApps). ZRS Semi Decentralized Exchange is the next generation commercial grade public and private blockchain systems for trusted value transfer. We believe that transparency, safety, and anonymity, combined with our creative solutions, are the priority values that should drive the new crypto exchange industry forward. ZRS has been created to satisfy these goals as we strive to incorporate the best features of decentralized exchanges and development of dApps.

Zoreum Labs plan to develop a fully Decentralised Exchange in the 2nd quarter 2019 with unique user interface tools.

Zoreum Labs is a Block chain assets market platform. It wants to provide the safest, fastest and most secure Semi Decentralized Exchange with easy to use interface like Centralized exchange.

1 Introduction

Cryptocurrencies aka digital assets are real and here to stay. Digital asset is one of the safest and trusted kinds of digital currency that people prefer nowadays. We all need to trade in the safest possible ways. Digital asset gives us that assurance which makes them an important source of investment right now and in the future as well. Another reason why digital asset have become extremely in demand is because of their policies. One does not really need to deal with a third party when it comes to digital asset. This gives reassurance and a feeling of safety. The fact that these are digital currencies alleviates the need for a third party. One can transact or trade independent of the location.



It all started with bitcoin, which was first released on January 9, 2009, and various versions launched in the following years. It was the first application of Blockchain.

Everything is being tokenized on the Blockchain. From financial and physical assets to events, work, activities, business networks and even time. In the beginning, web based centralized exchanges like Mt Gox, BitStamp, Kraken, Bitfinex, Coinbase etc were set-up to provide a means of exchanging blockchain coins and eventually tokens.

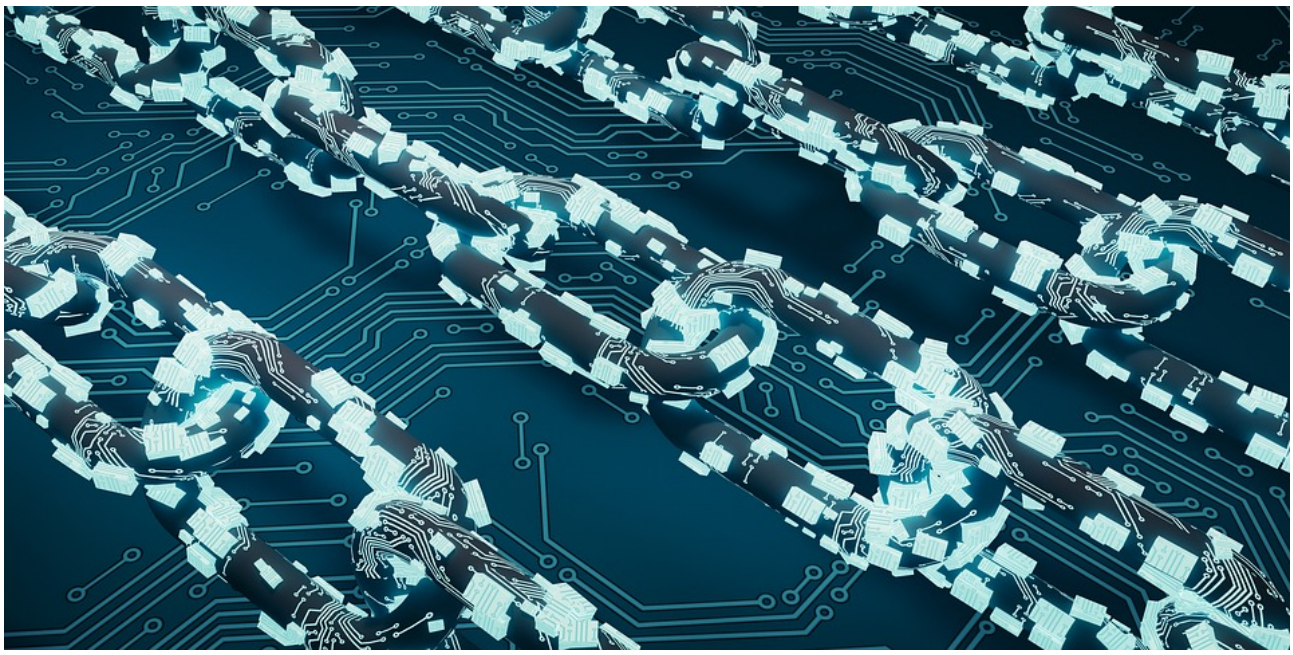
The drawbacks of web based centralized exchanges has led to the emergence of decentralized exchanges that use smart contracts to protect users from internal fraud, exchange hacks and provide other great functionalities.

In this paper, we propose to build a robust decentralized exchange with easy to use interface like centralised exchange, many decentralised exchanges lack this feature. **Zoreum Exchange** is a new decentralized exchange that embodies these ideas, built on the Ethereum blockchain and smart contracts are implemented using ERC-20 technical standard. This white paper presents our vision for the **Zoreum Block Chain Assets Market Platform**, the performance benefits of our technical approach, and how ZRS fits into the broader Decentralized ecosystem. We also discuss our roadmap over the coming months and plans for a public token sale.

2 Background

2.1 Blockchain and Smart Contracts

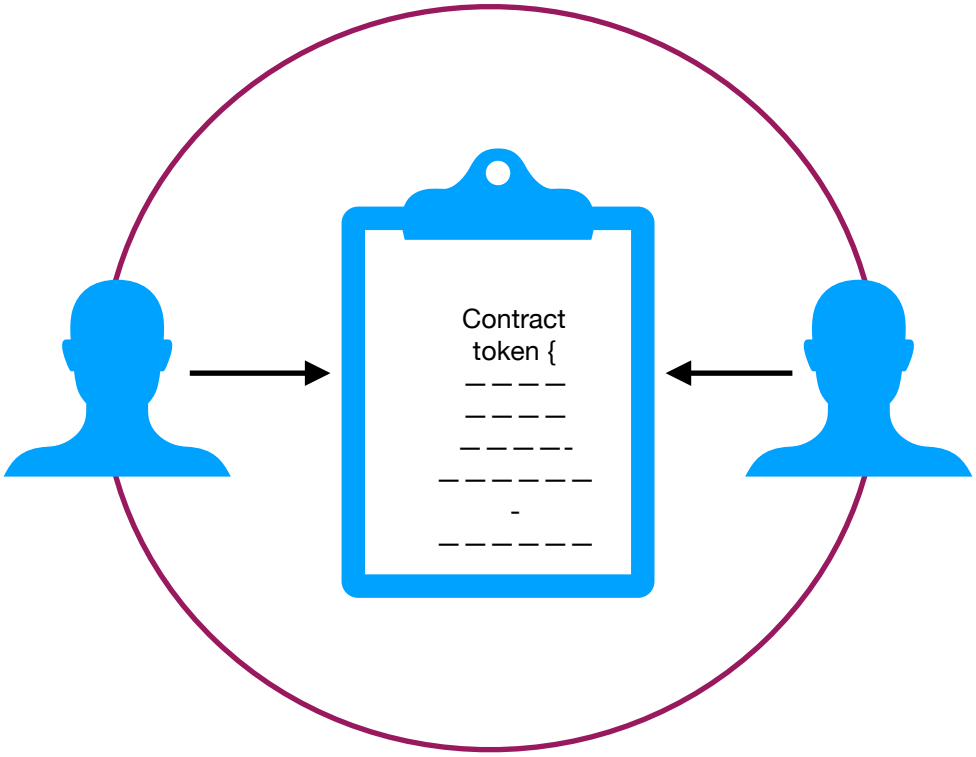
A **blockchain** is a decentralized ledger that can record transactions between two parties in a verifiable and permanent way without the need for a central authority. In 2009, Bitcoin emerged as the first public blockchain with large-scale adoption as a digital currency. Other chains have since attempted to improve on this technology. Most notably, Ethereum launched in 2015 as the first blockchain with programmable, Turing complete smart contracts.



Decentralization in simple term means that the application or service continues to be available and usable even if a server or a group of servers on a network crashes or are not available. The service or application is deployed on a network in a way that no server has absolute control over

data and execution rather each server has current copy of data and execution logic with them.

Smart contracts allow developers to publish programs on a blockchain that anyone can inspect, and that will deterministically execute to accomplish complex goals in a way verifiable to all involved third parties. For example, a smart contract might accept incoming funds from a user, then release them at a certain date, or collect funds from a series of users and split them evenly. These smart contracts are what make possible more sophisticated distributed on-chain applications such as decentralized exchanges.

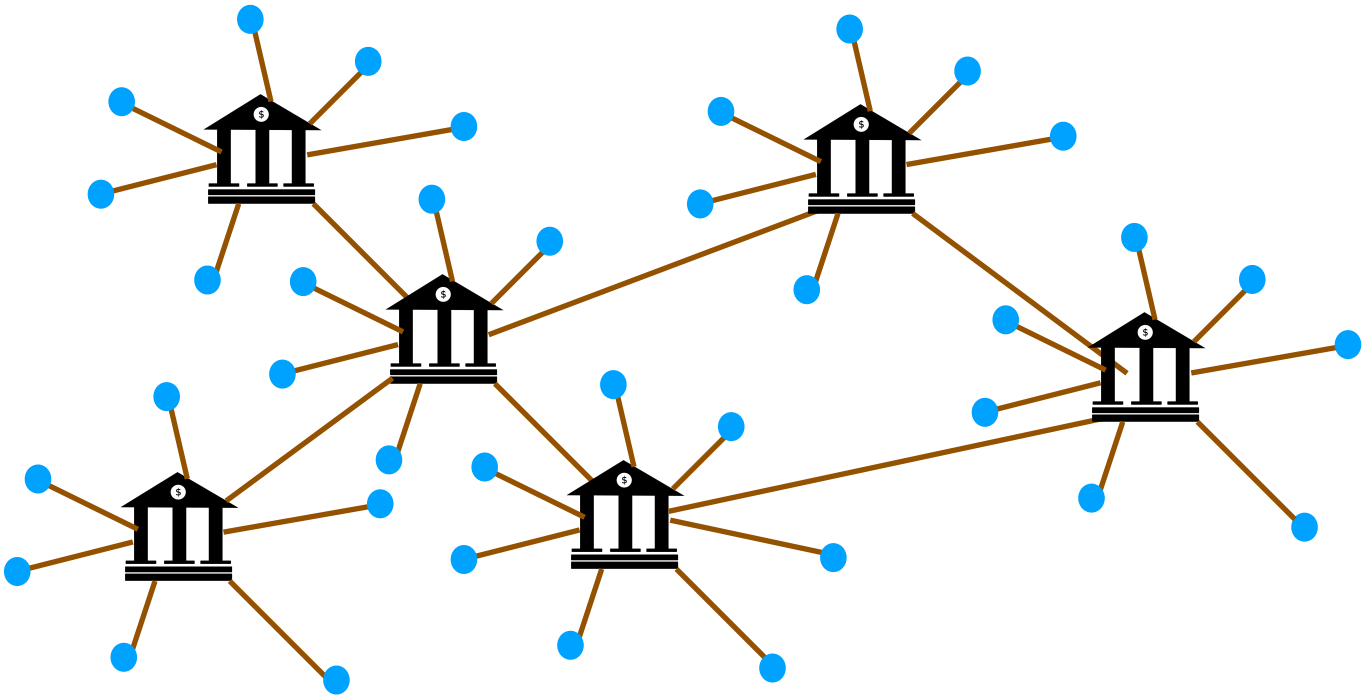


ERC20 is a protocol standard that defines certain rules and standards for issuing tokens on Ethereum's network. ERC stands for Ethereum Request For Comments and 20 stands for a unique ID number to distinguish this standard from others.

If token's Smart Contract includes certain function as per the ERC20 standards then the token is ERC20 compliant.

2.2 Decentralized Exchanges

A decentralized digital asset exchange platform, users transact directly with their peers without the need for a central server. There is no centralized platform service that is in possession of order books and custody. Funds are therefore controlled by the users and participants in the platform.



Decentralized Exchange

The decentralized exchanges decentralise the 4 core functions:

1. **Deposit of the Capital -** The funds / capitals remain in the wallets of the traders and not with the middle man anytime.

2. **Broadcasting the Order -** It happens directly from trader to trader over an inter-blockchain DHT network overlay. Traders' apps compiles an order book themselves instead of relying on a central order book service.

3. **Matching the Order -** When one accepts another's order, their apps communicate to set up the coin exchange process, and this is broadcast over the inter-chain network.

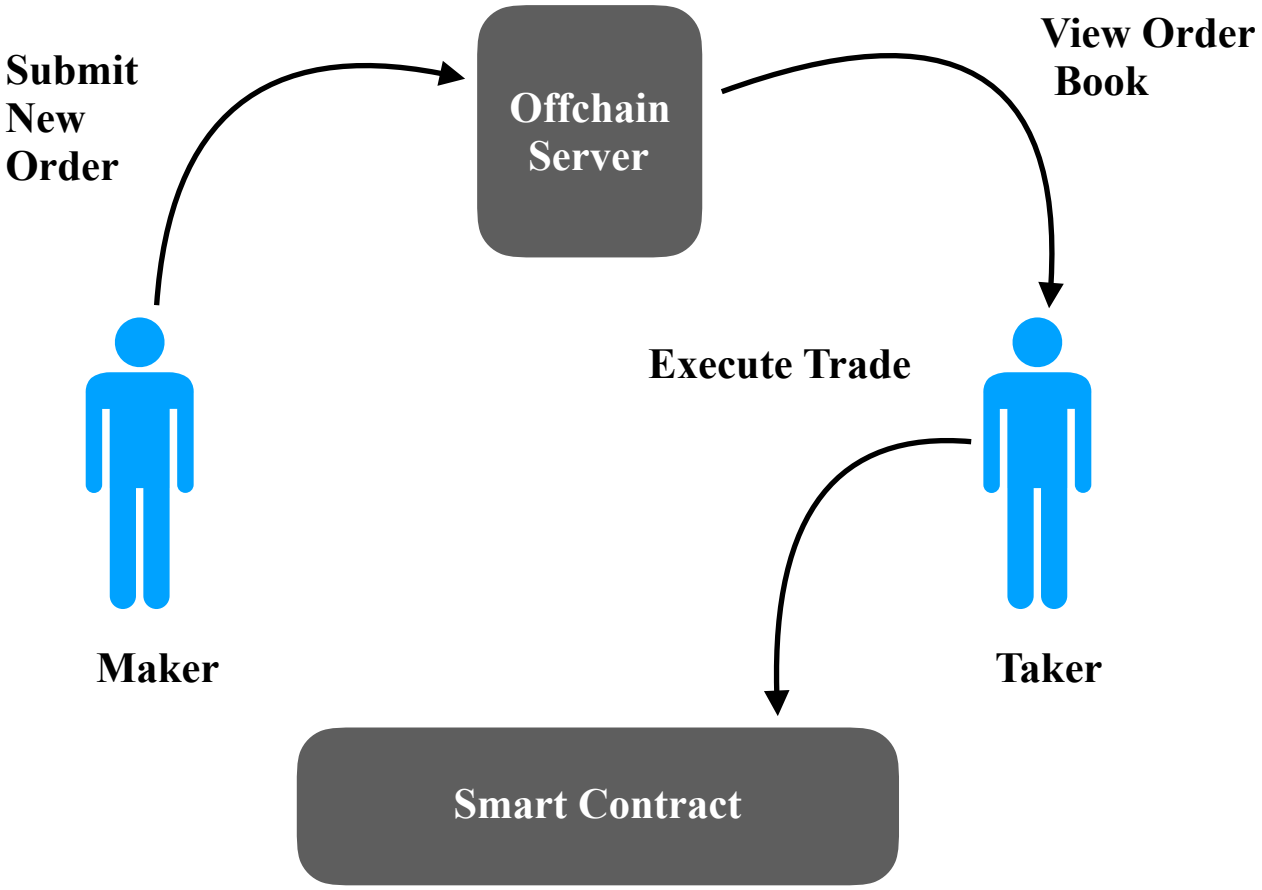
4. Lastly, **the token exchange -** It is achieved without the involvement of an intermediary, in a manner that does not require counter-parties to trust one another beforehand. An atomic swap protocol must be utilised (meaning that either the exchange of both currencies takes place, or nothing takes place), which employs a system called OP_CHECKLOCKTIMEVERIFY to nullify transaction malleability-based attacks.

The emergence of decentralized exchanges make sure that transacted parties are in control of their funds and they can do effective trades. The decentralized exchanges implement smart contacts on Blockchain which runs all the required checks, functions, etc thus removing the need for a centralized third-party to control trading parties transactions and accounts.

Trading Logic

The new market orders can be stored “on-chain” or “off-chain”. On chain means they are stored in the smart contract, off-chain means a third party like a central server. In practice, no orders are stored on-chain for EtherDelta due to the cost and speed implications. Instead the following mechanism is used.

A person can submit open buy or sell orders for a given ERC20 token—in exchange terminology this person is the Maker. Another trader can browse these orders and choose to execute on them—this is called the Taker.



Zoreum provides a Decentralised exchange with vastly improved performance and usability.

3 The Zoreum Lab's decentralized Exchange

ZRS is an open protocol for decentralized exchange on the Ethereum blockchain. It is intended to serve as a basic building block and provide a platform to build and drive increasingly sophisticated dApps. **ZRS** uses a publicly accessible system of smart contracts that can act as shared infrastructure for a variety of dApps. In the long run, open technical standards tend to win over closed ones, and as more assets are being tokenized on the blockchain each month, we will see more dApps that require the use of these different tokens.

Our mission is to create a platform that functions as an intuitive portal between the current financial system and the new digital blockchain-based economy. We will achieve this by developing an end-to-end trading platform that enables everyone to be part of this global value network.

This section provides the description and visualisation of decentralized exchange platform. The solution is explained as detailed as possible, however, developments in the crypto space are progressing so rapidly that it is desirable and wise to leave certain lower-level specifications as open as possible in order to ensure technological agility in the future.

3.1 User-Interface Design

The User Interface of the decentralized exchange has been designed to provide the best User experience without discounting anything on the security of the transactions. The UI is very smart and simple. These designs will be released through our communication channels.

All **ZRS** members will interact with the exchange through the user-friendly UI. The UI has been designed in such a way that it addresses different user profiles. These user profiles range between beginner crypto

investors and semi-advanced crypto traders. In general, the user experience will look and feel: simple, smooth, smart and intuitive. The UIs fundamental functions include: portfolio balance, market data, trade portal and account settings. The portfolio balance shows members' current portfolio balance and is based on real-time market data. Buy and sell trades from fiat to crypto, crypto to crypto, and crypto to fiat, can be done through the trade portal. Additionally, the trade portal will assist members in making a correct buy or sell trade. This means that members will be advised on the amount and price of their crypto investment to ensure transparency and healthy investment decisions.

3.2 Internal Exchange

All trade requests will run through the Governance Manager. This ensures that members' accounts and orders are valid and compliant with internal and external rules and constraints. The Compliance Manager will ensure that regulatory Know Your Customer (KYC) and Anti-Money-Laundering (AML) requirements will be updated and correctly installed in the Governance Manager and Account Settings. Besides rules and constraints, the Governance Manager will validate trade requests and lock available funds when necessary. When a trade request is correctly validated, the Governance Manager will order the Wallet Operator to lock members' funds. This will allow the Internal Trade Engine to match internal trades safe and secure. To protect members from front running, the matching of orders is shielded from the outside world by using a private order book and only made public when they are completed. When a trade request cannot be matched internally, the Internal Trade Engine will send the trade order to the External Trade Engine for external order matching. When a trade request can be partially filled internally, the residual order will be send out to the External Trade Engine. Orders that are filled by the External Trade Engine will be received and combined by the Internal Trade Engine to validate the total matched order. Finally, when the complete order is

correctly validated, the funds will be settled in the Wallet Operator and broadcasted to the chain.

3.3 Wallet Operator

Members' funds will be settled and stored in the designated blockchain wallets. The individual wallets will be tracked in the Multi-Wallet and managed by the Wallet Operator. The **ZRS** Wallet Operator will run a node for every blockchain that is supported in the exchange. This enables the effective reading and writing of transactions to the blockchain network. Every member will be able to create a personalised contract address via the Wallet Operator for every supported digital asset or token. The crypto wallets that are used in the **ZRS** Exchange are basically a trust-less and decentralized digital wallet that will hold their funds in a non-custodial manor. The **ZRS** Wallet Operator is a manager that links members' wallets on multiple blockchains through the Multi-Wallet. It has custom features in order to perform exchange activities such as funds checking, locking and settling. In the process of setting up an order that is signed and validated by the Governance Manager, the Wallet Operator will lock members' funds in order to ensure an atomic swap of ownership. If the order fails in the process of internal or external matching, the system will automatically revert the funds back to members' wallets. When the order is successfully matched internally or externally, the completed order will be settled and members' funds will be unlocked.

3.4 External Exchange

The External Trade Engine will receive unfilled orders from the Internal Trade Engine and decides how to distribute these orders in terms of size and time. Additionally, it will execute these external trades as efficient as possible on the External Exchanges. The External Trade Engine will optimize its decisions based on the available liquidity and additional

transaction costs. The External Trade Engine receives the required trade information from the Analytics Manager. Additionally, the Analytics Manager also determines the corresponding volatility risk of every trade, which will be communicated to the Exchange Accountant. The Exchange Manager's job is to translate the received trade requests to actionable API orders. The Exchange Manager will facilitate the communication with External Exchanges through APIs. Additionally, it communicates order state changes upstream with the **ZRS** Accountant, Analytics Manager and the External Trade Engine. The Analytics Manager monitors the External Exchanges for available liquidity by scanning their order books in real-time. Moreover, it calculates the expected transaction costs of every supported trade pair by volume and direction. It shares this information with the External Trade Engine, Accountant and the UI.

3.5 Accountant

The **ZRS** Accountant is there to perform trade and trust intermediation. It tracks members' funds throughout the entire trade and settlement process. This functionality is important so that the exchange can partially fill members' orders without having to settle multiple trades. This ensures members' order privacy, reduces transaction costs and allows members to experience an atomic swap of funds. In order to intermediate effectively, the Accountant will need to track and monitor all active orders in the settlement process to cover the complete finality of a transaction cycle. This cycle will be volatile due to possible network delays. Therefore the Accountant will measure and govern the overall risk of settlements. It is responsible for balancing the crypto and fiat assets that are necessary to perform the realtime trades. The Analytics Manager will provide the Accountant with an ideal distribution of assets to effectively balance exposure and trade flows. Additionally, the Accountant will communicate with the Wallet Operator and the Exchange Manager to ensure a live feed of cash positions throughout the entire Exchange. Besides managing asset

flows, the Accountant will also manage the cold storage of inactive funds to minimize exposure. The amount of funds that will be cold stored is relatively low in the beginning, due to low liquidity. However, when the number of active members increase, volume and liquidity will increase which will allow us to increase the cold storage ratio.

3.6 Security Measures

It is essential to ensure secure communication between the functional entities described above to assure a robust system. We value our members' trust in us and our ability to offer a high quality service. Therefore, we take the following measures to secure our services:

- We encrypt all communication over the internet allowing only HTTPS, using settings like HSTS, properly chosen CORS settings, CSRF protection and carefully chosen SSL settings.

- We secure the API's we build using tokens, with expiry. - We secure our cookies, using flags like 'Secure', 'HttpOnly', 'SameSite' and proper expiration.

- In terms of secure communication between public and private nodes, we only allow carefully chosen SSL ciphers and key exchange algorithms, while keeping tabs on developments and vulnerabilities around information security. We also use client certificates internally to enable secure communication, even in our private network. This means that data is not sent over an unencrypted network connection, even in our private infrastructure.

- We carefully choose our firewall settings and network topology, to separate and compartmentalize risks where possible without

compromising usability and testability. This enables us to allow traffic we trust, while blocking untrusted traffic.

- Additionally, we pay attention to OWASP updates, including mailing lists and other resources that enable us to stay on top of new vulnerabilities and/or patches (think BEAST, CRIME, KRACK etc).

- We do regular audits including penetration tests, load tests and code reviews with independent parties to ensure consistent security of our platform.

- We have DoS protection in place to protect us against common DoS attack strategies, and monitor our systems continuously. We also have a schedule that allows our team to be on call 24/7, if anything happens.

- We use a KMS for key rotation and organization of sensitive data. We value consciousness of risks inside our organization, as this is the best structural way to reduce risks in a consistent manner.

Please note that these measures are only a part of all security standards we implement in practice. We handle a more elaborate protocol internally, but the above provides a general overview.

4 The Zoreum Shares

Zoreum labs are pioneer in offering 'Blockchain as a Solution/Strategy' BaaS protocol, specialised in supply chain management of varied vertices. Zoreum Labs launches the Zoreum shares (**ZRS)**. Primary service is to develop a Decentralized exchange and Decentralized applications. Through the Decentralized exchange the Zoreum Labs will get regular income of trading fee that would sustain the cost to run the company. Through dApps development, the Zoreum Labs will address the issues that business and social communities are facing. Already three dApps Projects are in Proof of Concept phase. The underline assets for ZRS shares are success of dApps projects and regular income from Decentralized exchange.

The Decentralized exchange being developed by Zoreum Labs is the next generation digital asset exchange that aims at taking advantage of the opportunities presented in the digital asset exchange space, addressing the areas of deficiencies identified in current exchanges and providing a solution to the specific needs of traders and investors. It will not only win the trust of investors, but will also offer a completely new dimension to exchanging.

Zoreum shares (**ZRS)** will be utility tokens which can be used as tokens for trading fee payment for discounts. Even in new dAap's development life cycle Zoreum shares (**ZRS)** has utility value.

Zoreum shares (**ZRS)** has high potential to appreciate as the underlying assets are exchange and dAaps.

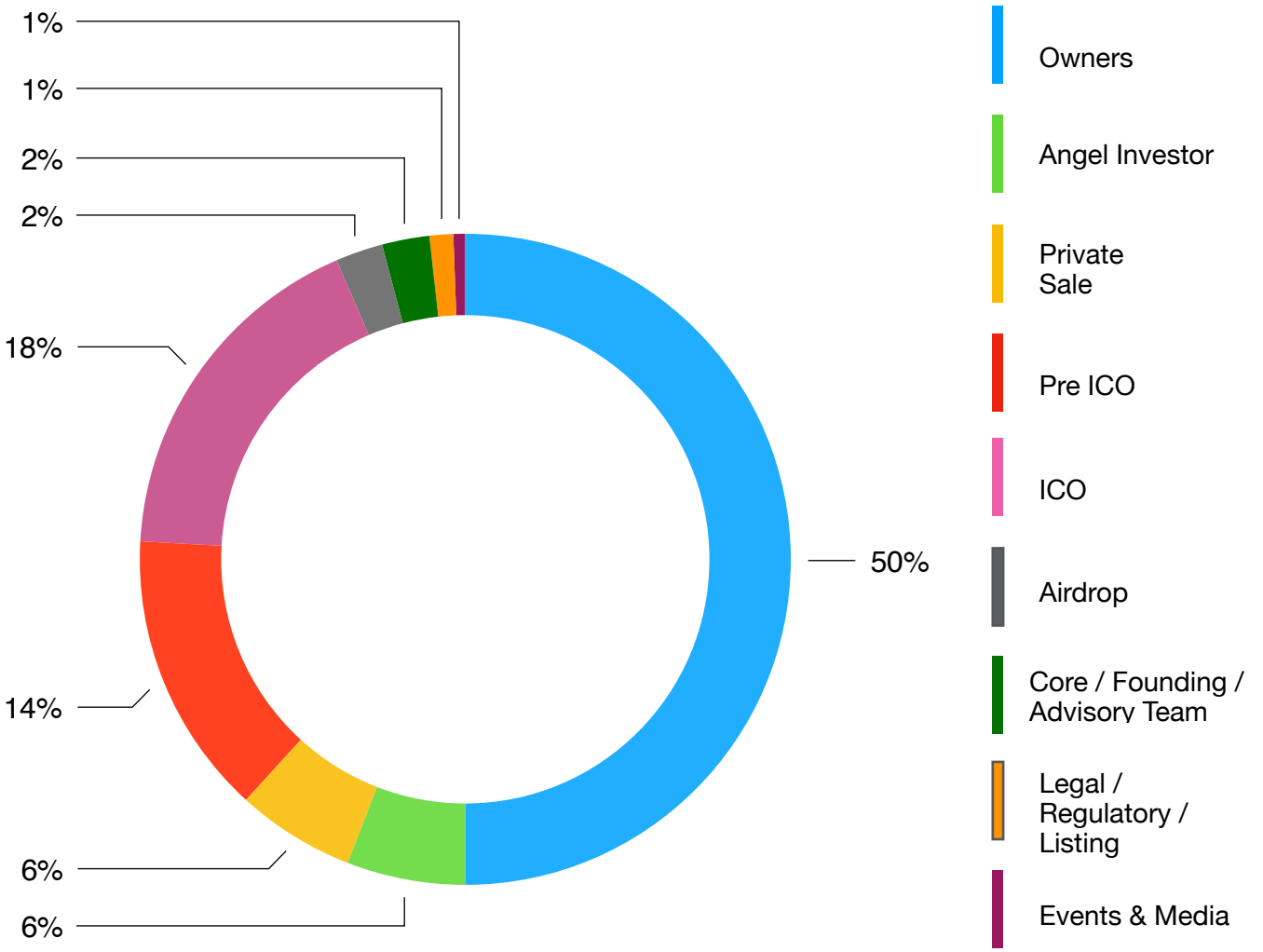
4.1 ZRS

The Zoreum shares (ZRS) is the dedicated digital asset of Zoreum Labs. A decentralized ethereum based token with a maximum quantity of 850 million units. As an ERC-20 smart Token, the ZRS shall be easily transferable between users on the Ethereum Blockchain.

4.2 Tokenomics

This section describes the total distribution of shares / tokens.

Total supply	850 million shares/tokens
Owners share	425 million shares/tokens (3 years lock)
Angel Investors share	50 million shares/tokens
Private Sale	50 million shares/tokens
Pre ICO Sale	120 million
ICO Sale	150 million
Airdrop / Bounty/ Marketing	20 million shares/tokens
Core / Founding / Advisory Team	20 million shares/tokens
Legal / Regulatory / Listing	10 million shares/tokens
Events & Media	5 million shares/tokens



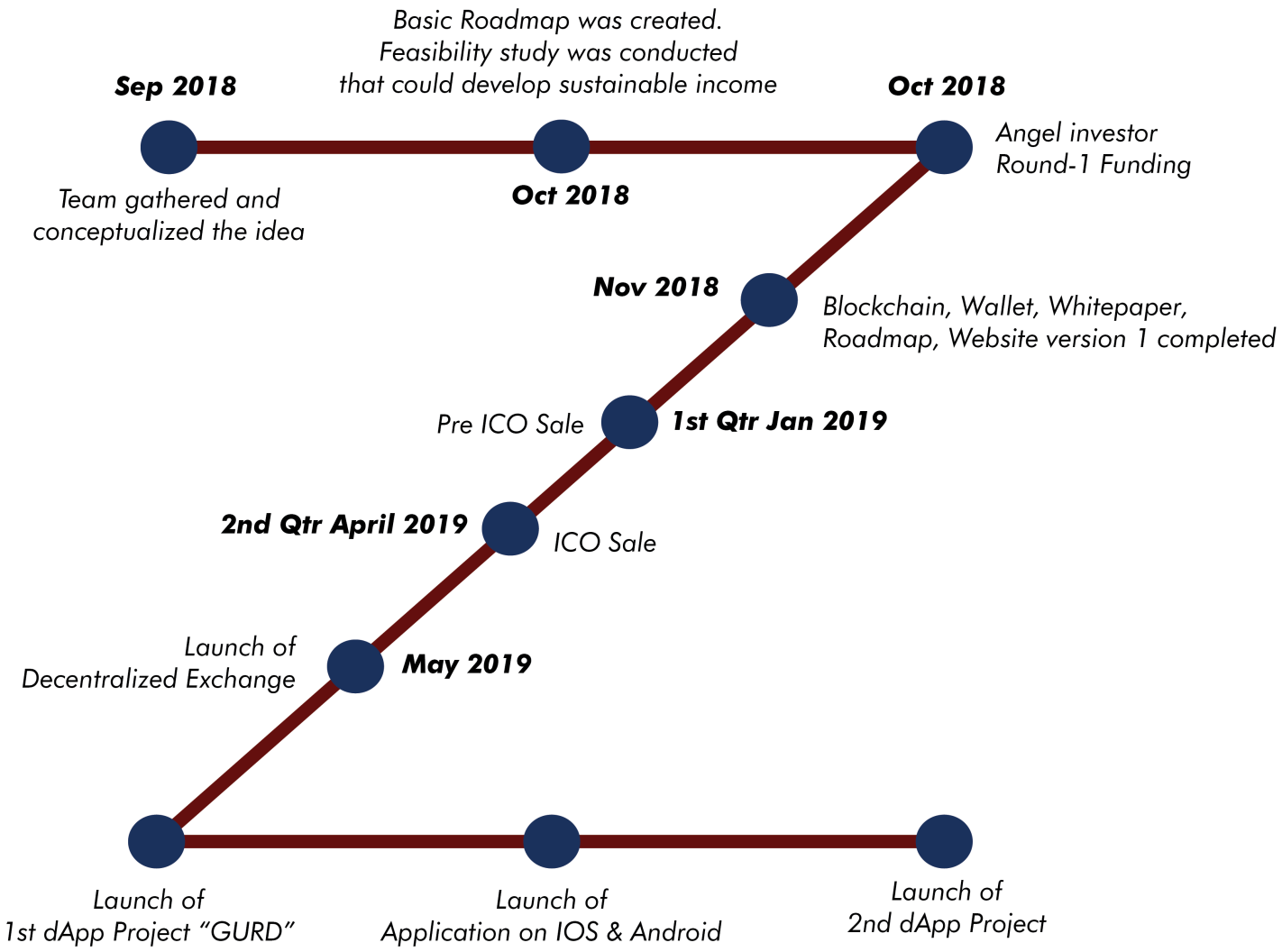
4.3 Mission

To be in Top Tier 10 companies in the world by the year 2022 in offering Blockchain end to end 360 degree solutions.

4.4 Vision

Zoreum Labs will be the best company to work for to invest in and to innovate.

5 Roadmap


Basic Roadmap was created.
Feasibility study was conducted
that could develop sustainable income
Sep 2018
Oct 2018
Angel investor
Round-1 Funding
Team gathered and
conceptualized the idea
Oct 2018
Nov 2018
Blockchain, Wallet, Whitepaper,
Roadmap, Website version 1 completed
Pre ICO Sale
1st Qtr Jan 2019
2nd Qtr April 2019
ICO Sale
Launch of
Decentralized Exchange
May 2019
Launch of
1st dApp Project "GURD"
Launch of
Application on IOS & Android
Launch of
2nd dApp Project

6 Decentralized Application

Decentralized application aka DApp is an open-source software platform implemented on decentralized blockchains and are fuelled using tokens which are generated using a protocol/algorithm.

Being an open-source application makes it truly decentralized as anyone can see and contribute to the code. It also fastens the process for scalability of product development in terms of both quality and quantity. There are noticeable common features of DApps:

- **Open Source** - Ideally, it should be governed by autonomy and all changes must be decided by the consensus, or a majority, of its users. Its code base should be available for scrutiny.

- **Decentralized** - All records of the application's operation must be stored on a public and decentralized blockchain to avoid pitfalls of centralization.

- **Incentivised** - Validators of the blockchain should be incentivised by rewarding them accordingly with cryptographic tokens.

- **Protocol** - The application community must agree on a cryptographic algorithm to show proof of value. For example, Bitcoin uses Proof of Work (PoW) and Ethereum is currently using PoW with plans for a hybrid PoW /Proof of Stake in the future.

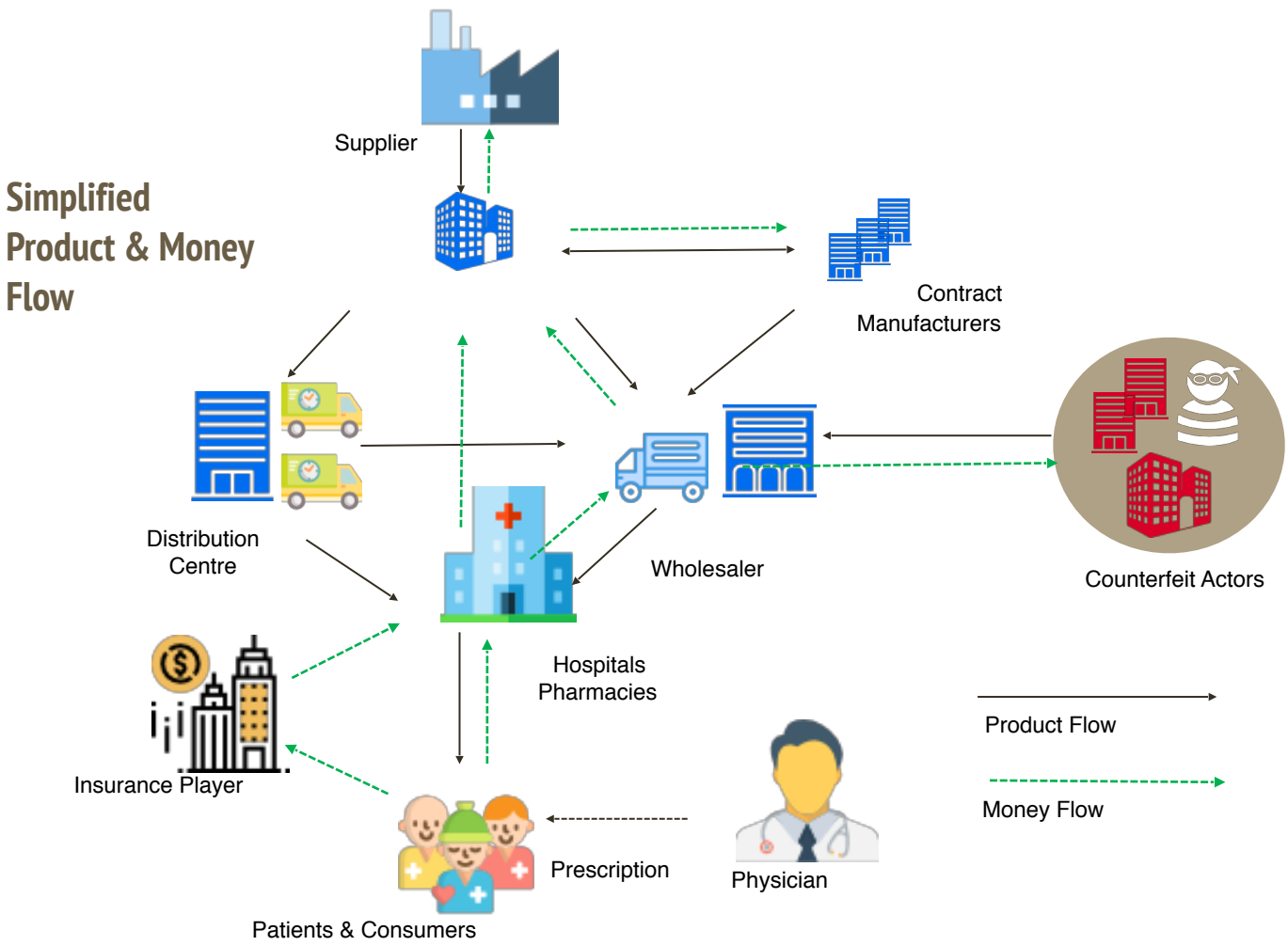
7 The First Baas dApp to be launched by Zoreum Labs

The Pharma Products are transferred along the chain from suppliers to manufacturers to distributors to re-packagers to retailers and finally consumers, changing hands many times in the process. The number of stakeholders involved makes it difficult to track any single product's authenticity and integrity from the beginning of the chain to the end and thus leading to large and growing market for counterfeit drugs.

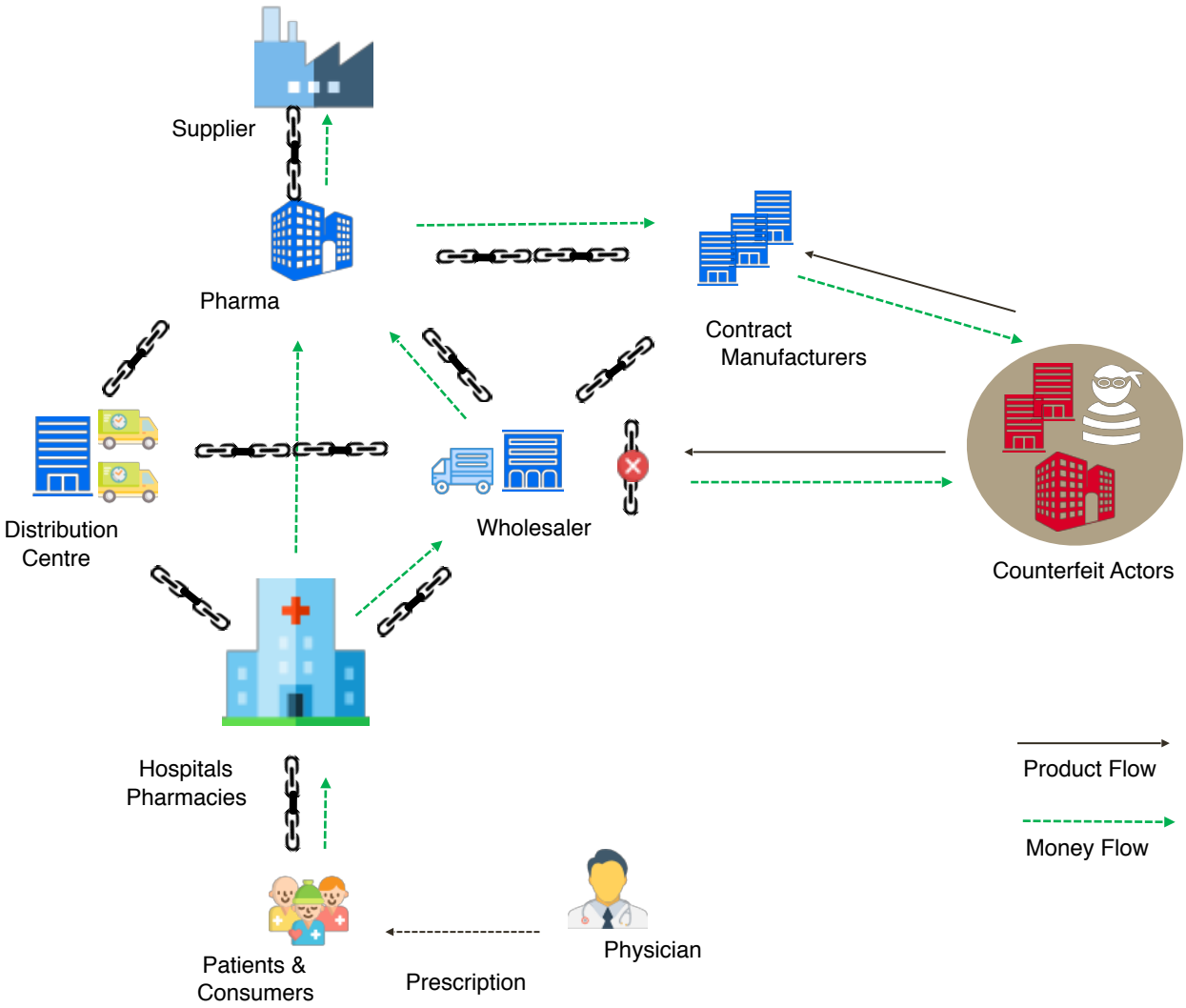
AsliMedicine.com is a blockchain enabled solution that tracks the provenance of your medicine from supplier to consumer and ensures regulatory compliance, product integrity and builds on consumer trust. With this solution from AsliMedicine.com, the consumer can now scan the unique QR/BC code using their mobiles and track all activity in real-time transparently. The activist consumer can also report the fake/counterfeit drug through the App and get rewarded from us.

A combination of AI and Blockchain technology creates an immutable record and stored securely in distributed ledgers. Only trusted, verified parties would be granted permission to add information to the blockchain's record.

7.1 Existing System



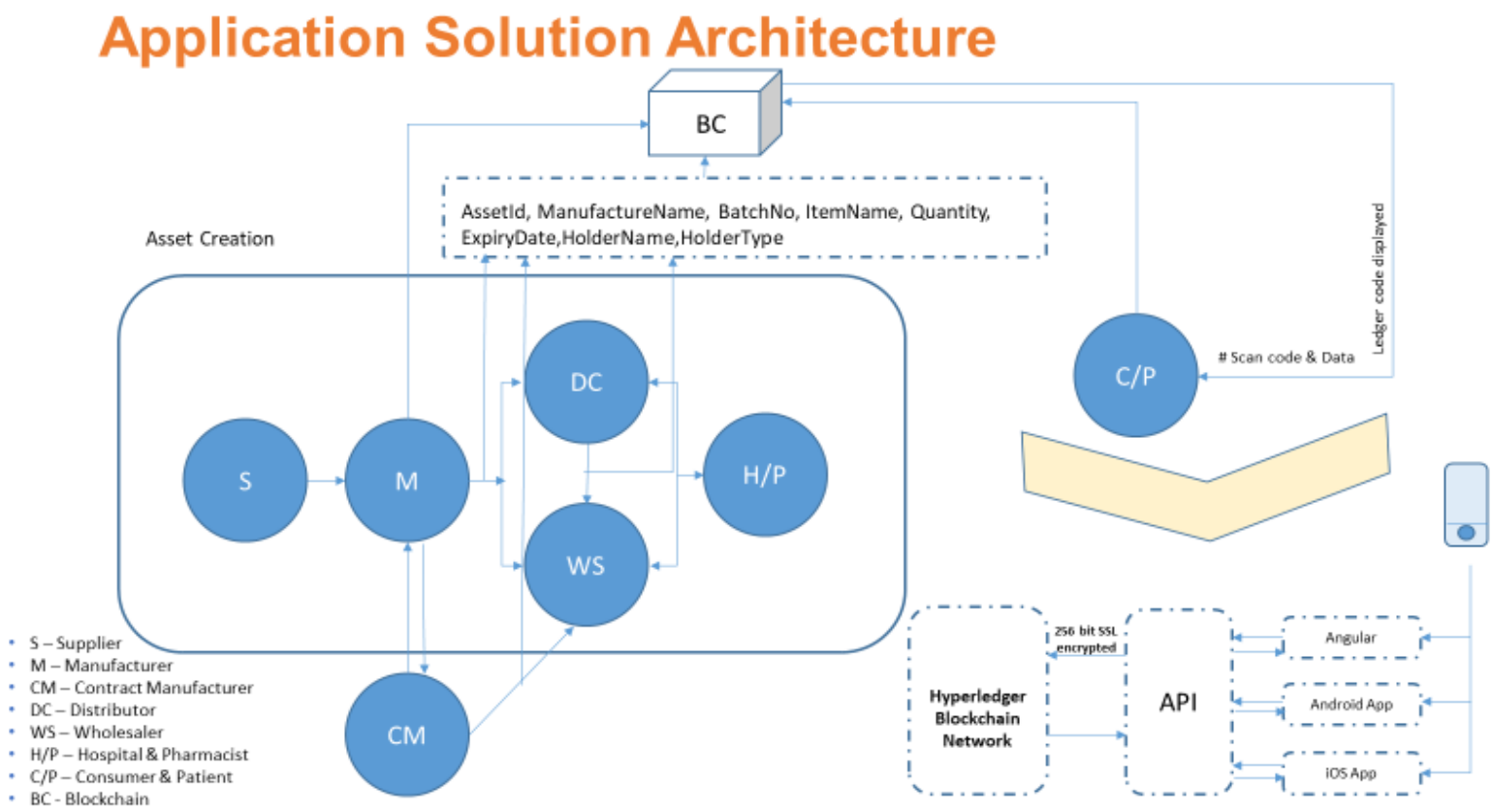
7.2 Proposed System



7.3 Platform Specifications

- Component Specs:
  - Hyperledger Fabric v1.1
  - Go Lang v1.10
  - Angular JS
  - iOS SDK
  - Android SDK
  - Apache Webserver
  - Linux OS

7.4 Architecture



7.5 Post Course Roadmap

Immediate term (1 – 3 months)

- Supply chain process for Pharma industry identified
- Identified Polio drug as a focus area
- Industry visit and validate the pain-points
- AsliMedicine.com website created and build proto-type
- Launch website and build v1 of DApp of the solution
- Polio vaccination and industry/process directions from Drug Control authority
- Market Nationally and Roadshows in Major cities

Medium term (3 – 12 months)

- Integrate with text based National services like Pharma-Secure, Central Govt Drug Technical Adv board initiatives
- v2 of the App – production readiness
- Execute on 2 – 3 with National Pharma players
- Participate in International seminars in Vienna, Europe BC Investment conference
- Participate in African BC conference and Indian Pharma Tech Expo (Aug 19)
- Add technical features
- Partnerships with other private and public entities

Long term (1 – 3 years)

- Roadshows in other parts of the world
- Deliver v3 of the product that takes care of International standards

8 Zoreum Team

Our Team has the perfect mixture of experience, knowledge and positive attitude.

RamKrishna

COO: *BS in Computer Science from Osmania University, Advance Diploma in Digital Marketing from Delhi School of Internet Marketing, MBA from IIM Calcutta.*

Mr. Ram Krishna has an all-encompassing experience in the field of marketing and the financial sector. He is a philanthropist by heart and humorist by nature. With all this, he is a techno-entrepreneur & blockchain-technologist and is popularly known as RK in the Fintech circle.

Mr. Krishna has founded Pranco, Blockchain Technologies Pvt. Ltd specialized in blockchain technologies and P2P decentralized modules. He holds a strong network in Asian & emerging financial markets as well as a network of angel investors and venture capitalists. Moreover, he has also crowdfunded many start-ups through ICO.

He is certified BlockChain Architect in world's prestigious educational institute International Institute for Informational Technology - IIIT Hyderabad which is one of the 20 Blockchain educational Institutions across the globe sponsored by Ripple.

He is experienced Blockchain Architect worked for dakuce a HongKong based crypto exchange in capacity as CEO and well know in blockchain industry across the globe for 2 things:

1. For refunding all the money collected to retail investors around 2.23 million USD collected during ICO period.
2. Launching the exchange as per road map and achieving break even in less than a year.

He is a global speaker on Blockchain and emerging technologies.

He is a leading professional business coach and mentor who have focused on blockchain technologies, starting with Allianz and going forward with generating $1.5 billion revenue with key accounts portfolio together with 600 other teammates.

He is dedicated to enable the achievement of innate entrepreneurial potential, particularly in high-growth economies. He is also a blockchain and IOT product enthusiastic who creates, manages and scales service-based companies in emerging markets. He has a specialization in doing real-time data analysis and financial modelling in building large complex transactions and is an Alumni of IIM Calcutta, which is a leading and premier business school in the world.

Smita Varakhedkar
CCO

Smita has expertise in multiple Organisations pertaining to IT and Non IT businesses. With a sound understanding of all departments of a corporation

She is expert in Blockchain and Digital asset, maintaining robust client relationship, management services and driving Technical groups to supply extraordinary support to the Clients. With a proven track record of creating a seamless communication structure among various departments within an organization, she encourages and empowers individuals to perform at their highest potential.

Worked with companies like Dakuce, Pranko Technologies as a core team member. To the flip side she contributes to the social responsibility having Co-Founded “Sahi Disha Foundation” an NGO.

Smita has the urge to learn and try out new technologies. She believes that technology can make living better. She’s been associated with Blockchain and Digital asset related projects for quite sometime now. Having belief in the potential of Blockchain deliverables she is been handling projects such as ICO Catalyst, The Cryptostar and Zoreum.com.

Abit Ghimire

Exchange Strategic Partner

Abit is an avid crypto expert. His journey in crypto space started in early 2014 as an active digital asset and blockchain enthusiast and trader. His passion for cryptocurrencies led him to open the first and foremost crypto exchange in Nepal, Bitsewa. As a Founder and Managing Director, Mr. Ghimire drew investments and efficiently managed all operational activities including, banking, administration, marketing, and strategy. During his stint at Bitsewa, he partnered with UK digital asset miners.

Charles Markette

Advisor

Charles work for an end to end development / consulting company (alliedblock.com) and also a law firm (aigbelaw.com). Both companies are blockchain agnostic. He is also a U.S. securities lawyer. His practice includes public and private offerings, broker-dealer and investment banking matters, secondary market transactions, venture and private equity capital investments and mergers and acquisitions, initial coin offerings (ICOs).

Ravindra Chebiyam

Head - Technology & Operations

Ravindra is a seasoned Software Product Engineering & Program Management Professional with 25+ years of enterprise application experience in diverse domains with a proven track record of building and managing large global product development teams.

He has good functional knowledge of diverse domains like Rapid Application Development (DLEP), Security - Data Loss Prevention (DLP), Oil & Gas, Power Industry, Telecom (BSS/OSS)

He is expert in enabling Innovation, Collaboration and Quality for achieving business strategy while working with multiple constraints

He is a Blockchain Solution Architect and Technologist.

9 Disclaimer

Zoreum Labs understands that the business of running an exchange , as indeed other businesses is surrounded by risks. But the Zoreum Labs have a strong team with adequate abilities and skills to manage and overcome these risks. The content of this white paper reflects Labs' knowledge, accuracy about the **ZRS shares**, Decentralized exchange and platform for building dApps. **ZRS shares** are sold as digital assets. Zoreum Labs does not recommend that you purchase tokens unless you have prior experience with cryptographic tokens, block chain based software and operations and/ or unless you have taken independent professional advise.