Overview

CYPHER is a Blockchain technology Start-up bringing Cutting Edge Distributed Ledger Technology to varied industries.

CYPHER works with institutions like banks, insurers, regulators, credit bureau, auditors bringing benefits of secure and efficient multilateral contracts with full audit trail of transactions on a cryptographically secured distributed ledger platform.

Problem Statement

- ### Middlemen
  We live in a world of increasing economic activity. Starting a new Business relation with a new entity always comes with a caveat due to lack of trust. The need to avoid the counterparty risk results in the need to involve middlemen and increased execution cost.

- ### Fragmented workflows
  As the corporations grow bigger, they evolve their business processes and establish separation of concerns by creating divisions and sub-divisions and assigning roles. This also results in parts of a business transaction being e executed by different parties. Lack of proper communication across divisions causes the business workflows to be fragmented and results in increased effort and cost spent on reconciliations.

- ### Redundancy and Collaboration
  Competition is healthy for the industry and consumers. Multiple players offering similar products and services help keep the quality and prices in check. But this also means significant duplication of work by players in the same sector having similar processes setup to run their business functions.

Privacy and Information Security

- In the age of internet, with so many connected devices keeping private data secure and confidential is of paramount concern and corporations invest huge amounts of money and effort in ensuring information is protected. The problem extends to collecting and storing user data particularly when sharing the user's data with third parties. Users may not fully understand and control how their data is being shared and this may later result in lawsuits and loss of reputation and business.

IP ownership

- In today's age of internet, managing ownership of intellectual property is a very tough task. Ranging from technology to literature to media to entertainment, corporations invest huge capital to protect their IP and to share it with others including their staff and vendors. Copyright laws are in place, but more often than not, conflicts and litigations happen between players due to lack of clear-cut time-stamped proof of ownership. IP owner's consent to access and transfer the information needs to be clearly defined.
- For instance, a freelancer produces photos of some event to 2 media houses, who purchase it from her and thus claim the ownership and publish the material in their name. Later the individual claims the ownership to be hers and files a lawsuit.

Social Outreach and Financial Inclusion

- In a centralized system, taking public services including banking to remote and not so well connected areas is a big operational challenge. Even after deploying huge man power for certain government social welfare initiatives, for instance, collection of data and transferring full benefits to the end user is difficult, as the data has to be fed individually into various systems, which may not vary significantly from one another.
- There is a need to make the users owners of their information and providing them with a way to provide consent for it's use. The system needs to guarantee that the parties stringently abide by the consent clause.
- Also at the same time, wider participation from large number of smaller players is required, where large institutions become primary service providers and smaller vendors taking services to the public. Not that it doesn't happen today, most of it is in unorganized and unregulated space. Bringing this into an efficient decentralized realm would yield multi-facet benefits ranging from a much wider outreach and fraud prevention to increased employment in a more formal sector.

Distributed Ledger technology

- A distributed ledger is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage
- Distributed ledger technology (DLT) thrives to solve the problems around information, ensuring sound business.
- Distributed ledger design enables all the involved parties in a transaction/contract to have secure access to the relevant information. Access to the information is cryptographically secured. Operational requirements for inconsistencies and reconciliation of information will never be required, saving huge in operational costs. This design also ensures no-delay access to the latest information.
- Backup copy of the ledger is created at regular intervals, securing the history on tape. In wake of an attack which can wipe out data from the whole network, data will be retrieved from the latest copy of the tape and restored in the system. This ensures no loss of data ever.

- Maersk Not Petya Virus attack: Maersk was non-functional for many weeks because the data was wiped out from the whole organization. This design ensures quick recover of data and business.

How Cypher platform uses DLT to solve some of the problems

- CYPHER is a Distributed Ledger based Consensus building platform that enables parties to arrive at an agreement of certain shared facts. It employs complex and highly reliable principals of cryptography to securely share information between various parties for consent, where a business workflow proceeds through pre-defined or dynamically added steps and facts getting added to the ledger on completion. Updates to the contract are stored in a blockchain based immutable data structure to ensure audit trail.
- SMART CONTRACT manages the lifecycle of a business transaction on the platform. Cypher makes it easy to do business by enabling secure sharing information between parties involved in the transaction. The information is controlled through cryptographic keys for the bonafede users.

Salient features

- Node based architecture-Cypher services are deployed as a JVM based run-time environment using unified node based architecture. Each node is a peer on the cypher network assuming a well defined role/identity.
- No global broadcast-Cypher supports point-to-point communication between peer nodes such that each node, participating in the cypher network, receives the information on a need to know basis. Therefore a message sender node is well aware of the identity of the corresponding message receiver node.
- Contractual-validity - Transactions on cypher network are initiated based on the type of contracts. The contract contains the logic that can be invoked to verify if the given transaction is valid as per the contract life cycle. Cypher network supports notion of various types of contract and provides some of them out of box. The user of the cypher network, however, is not allowed to create such contracts. This prevents injection/execution of malicious code which otherwise can get invoked as part of transaction processing by various peer nodes in cypher network.
- Unspent Transaction Output-Cypher network supports the notion of input and output states which are part of a given transaction. Registrar peer node provides the functionality of verifying that none of the input states is already consumed and appropriately created respective output states.
- Auditability-As part of the cypher network one of the peer node service provides the functionality of storing all the transaction logs. This node acts as the repository of retrieving such transaction logs.
- Robust cryptographic layer- Cypher kernel supports thoroughly designed cryptographic layer which can be used to sign a given transaction on the network. Signed transactions are then sent to respective consumer node.
- Robust messaging layer-Cypher services use google provided GRPC based TLS enabled message channels to facilitate communication between peer nodes. This ensures fast and secure message exchange on the cypher network.

Adding value

- Transparency between peer nodes-Information on cypher network flows between nodes having well defined identity. Transaction initiator node is well aware of the corresponding transaction receiver node.
- Security- Safe contractual-validity, robust cryptographic layer and mechanism , in place, to identify unspent transaction output are the back bone of secured information exchange on cypher network.
- Regulatory-centric-Node based architecture supports the deployment of observer nodes in the cypher network that can monitor the information flow between functional nodes. Moreover such supervisor nodes can raise alerts after detecting breach of given regulation. In addition it's easy to retrieve audit information logs for various transactions from the transaction expository node.

Verticals

- The way we designed the platform was to make it generic and be able to handle practically any business process with clearly identifiable workflow boundaries and encapsulating data attributes.
- Having said that it becomes really important to understand where the platform can really add value and our goal is to focus on those areas. For example, the platform may not directly give you a investment signal (it can theoretically, but investment to reward may be too high when compared to traditional analytics systems), but it'll very efficiently execute the investment transaction, i.e. Purchase of the security.
- Keeping these in mind, we are putting some broad business verticals and use-cases we are focussing on.

Identity Management

- Identity management is so firmly entrenched in Cypher's way of handling transactions that it can be considered as an extension to the core platform itself. In any multilateral contract on the platform, parties should have well defined identities as captured and validated on the system.
- KYC: KYC, although sounds very common use case and every organization having defined some mechanism or the other to capture it, is a very cumbersome process. From the point of onboarding a new customer to their verification by the Organization's compliance department to managing regular changes in the profile involves multiple steps Cypher helps streamline the complete lifecycle of an individual's or corporation's identity.
- This identity, based on user's consent, can also be shared with other organizations bringing overall efficiency to the system. Receiving organization may not fully rely on the information provided by the first company offering the KYC details of some entity, but it's a good starting point saving a few days from the former's onboarding process. The system accommodates for the trust building between the 2 parties over time brining incremental improvement in efficient with more bilateral transactions between them over time.
- Anti-Money Laundering guidelines: AML compliance is built into the platform's identity management suite by way of mandatory post process rules run automatically as part of an onboarding/KYC workflow.

- Regulatory compliance: To keep up with changing regulatory environment, organizations make great deal of investments to have their systems up-to-date. Investments are also in generating reports sought by the regulators. Cypher solves the problems at 2 levels. One is when organizations share user data (with user's consent) with each other, they collaboratively update their systems for new regulations and second it's designed to make regulators part of the same network, so the they get the data in real-time.