

## **1. INTRODUCTION**

### **1.1. History**

Over the past few years, an important innovation colloquially known as the “Blockchain” has emerged as a potentially disruptive technology. The core of the innovation is built around the concept of a distributed cryptographic database. The database, also referred to as the ledger, is maintained by a network of computers.

The ledger makes it possible for the entire network to create, evolve and keep track of an immutable record of transactions. The most successful blockchain application thus far has been Satoshi Nakamoto’s cryptocurrency known as Bitcoin, which he outlined in his seminal paper, “Bitcoin: A Peer-to-Peer Electronic Cash System” in 2008. This powerful technology has so far been implicated in the numerous cryptocurrencies that exist online. Financial institutions are only beginning to understand the potential applications of blockchain in conventionally regulated industries.

### **1.2 Understanding the Blockchain**

At a fundamental level the blockchain is a data structure that cryptographically links blocks of transactions or any potential transfers of value. As a paradigm, the blockchain allows for true privacy to exist between those involved in a transaction. This characteristic of the blockchain makes its most significant implementation in the financial industry. Its structure allows for automation, immutability, and decentralization. These characteristics were carefully chosen by Nakamoto in order to create a digital mechanism of trust.

For the financial world this would result in a more limited reliance on third party trust mechanisms enabling a direct contractual interface between two parties involved in any transfer of value. This technology has the power make such exchanges safer, faster, and cost effective.

Ownership of value stored in the blockchain is established through asymmetrical cryptography. Digital keys, wallet addresses, and digital signatures are all created cryptographically to ensure total privacy in transmission of transactional data.

Every transaction on the blockchain needs to be 'signed' using digital keys. Whoever owns these keys, owns access to the value stored in the wallet. All keys generated by the wallet software come in pairs; a private key, which is kept secret and a public key. The public key is akin to a bank account number and the private key is like the secret pin used to control the account. The idea behind digital signatures is that private and public key pair shares a mathematical relationship such that a message (transaction) signed by a private key can be verified by a public key without revealing the private key.

### **1.3 Public Blockchain**

The Bitcoin's blockchain network is structured as a peer-to-peer network architecture. In this network implementation, all nodes are equal or symmetric. There is no server, no centralized service, and no hierarchy in the Bitcoin's network. Blockchain implementations for the financial industry however, cannot allow for such an open and symmetric network structure. Bitcoin enthusiasts advocate, therefore, that the blockchain and Bitcoin are fundamentally linked. This is a short sighted view taking into consideration that the Bitcoin technology stack exists to solve the problem of an unregulated digital currency. The same stack can be evolved to solve similar transfers of value over an asymmetric network.

The development of the Ethereum blockchain was a major milestone in the blockchain ecosystem. The focus shifted onto system state and virtual machines that could run smart contracts across the network. With the availability of Turing complete smart contracts, the limited functionality of the Bitcoin scripting language was overcome and a number of different applications became possible.

### **1.4 Private Blockchain**

Private Blockchains came into prominence with the Hyperledger Project that saw participation from IBM and Intel in 2016. Another major private blockchain developed by R3 called Corda also raised significant amounts of money. Since then, R3 has also joined the Hyperledger Project. Fully private blockchains make the case that centralized and trusted implementation of the core data structure of the blockchain along with significant changes to the consensus mechanism are meaningful value propositions for enterprise applications.

### **1.5 Hybrid Blockchain**

Hybrid blockchains are fairly unexplored and only few implementations exist; even in development. Quorum developed by JP Morgan is designed to be the hybrid blockchain in a fully permissioned environment. Truly Hybrid blockchain must necessarily be able to connect public blockchain with a private blockchain implementation running in a fully permissioned environment. The XDC hybrid blockchain aims to be exactly that, leveraging the power of both the public and private blockchain paradigms.

---

## 2. LITERATURE SURVEY

### 2.1 Ethereum

The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of tradeoffs that we believe will be very useful for a large class of decentralized applications, with particular emphasis on situations where rapid development time, security for small and rarely used applications, and the ability of different applications to very efficiently interact, are important. Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions. A bare-bones version of Namecoin can be written in two lines of code, and other protocols like currencies and reputation systems can be built in under twenty. Smart contracts, cryptographic "boxes" that contain value and only unlock it if certain conditions are met, can also be built on top of the platform, with vastly more power than that offered by Bitcoin scripting because of the added powers of Turing-completeness, value-awareness, blockchain-awareness and state.

#### 2.1.1 Ethereum Accounts

In Ethereum, the state is made up of objects called "accounts", with each account having a 20-byte address and state transitions being direct transfers of value and information between accounts. An Ethereum account contains four fields:

The nonce, a counter used to make sure each transaction can only be processed once

The account's current ether balance

The account's contract code, if present

The account's storage (empty by default)

"Ether" is the main internal crypto-fuel of Ethereum, and is used to pay transaction fees. In general, there are two types of accounts: externally owned accounts, controlled by private keys, and contract accounts, controlled by their contract code. An externally owned account has no code, and one can send messages from an externally owned account by creating and signing a transaction; in a contract account, every time the contract account receives a message its code activates, allowing it to read and write to internal storage and send other messages or create contracts in turn.

Note that "contracts" in Ethereum should not be seen as something that should be "fulfilled" or "complied with"; rather, they are more like "autonomous agents" that live inside of the Ethereum execution environment, always executing a specific piece of code when "poked" by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables.

## 2.2 Ripple

Ripple is a cryptocurrency, which aims to enable “fast, scalable, and stable” and nearly free cross-border payments of any size with no chargebacks through their real-time gross settlement system (RTGS), currency exchange, and remittance network.

First released in 2012, Ripple fundamentally differs from Bitcoin.

The later relies on a network of “miners” who run code that validates transactions and keeps the network secure. The network incentivizes the miners by rewarding them with bitcoins as incentives.

But in case of Ripple, “mining” does not generate new coins. All of the 100 billion coins (XRP) were released by the network in 2012. The creators of the XRP coins kept 20 billion and gave the rest to the company.

Since then, Ripple has been methodically distributing tokens to its clients, but it still holds nearly 50 billion in an escrow account.

### 2.2.1 A Simple & Real-World Example of How Ripple Works

On Jan, 2018, Ripple partnered with MoneyGram (a cross-border money transfer company) who are now using XRP to speed up and reduce the cost of transferring money by using Ripple’s xRapid payment network.

Fig.2.2.1 Ripple transfer between banks.

The status quo is that when you send money (in one currency; USD for example) to another currency (let's say, Indian Rupees) using MoneyGram or banks, this conversion takes several business days and involves multiple stakeholders who get their cut.

Ripple changes this by acting as a central currency, XRP.

So now if you were to send USD to your friend in India (INR), the US bank would trade USD for XRP and then trade XRP for INR.

### 3. XDC PROTOCOL

#### 3.1 XinFin Blockchain Platform

XinFin Hybrid Blockchain platform is built on the paradigm of consortium Blockchain. Its architecture combines best of private & public Blockchain.

Fig.3.1 The XDC Protocol

#### XinFin Blockchain

##### Public Blockchain

1. Easily available
2. Creates a well-defined relationship between the developers and the end users
3. Higher participation due to open source code
4. Protection from single entity possessing majority control over the network

##### Private Blockchain

1. Secure and private transactions
2. Trusted validators
3. Lightning fast speed of transaction
4. Availability to revert transactions, if necessary
5. Scalable
6. Cost effective operations

---

### 3.2 The XDC protocol is supported by its two native tokens; XDC and XDCE

Fig.3.2.1 XDC Ticker

1. The XDC token is the underlying utility token of the XinFin hybrid blockchain. The XDC token acts as a settlement mechanism for DApps built on the XinFin hybrid blockchain.
2. Our first DApp, the TradeFinex platform, uses this settlement layer to finance infrastructure projects and other procurements.
3. Efforts are ongoing at getting the XDC token listed on larger exchanges.
4. The XDC token can be currently procured from the AlphaEx exchange.

Fig.3.2.1 XDCE Ticker

1. XinFin has launched an Ethereum token, XDCE that can be traded with XDC utility token on a 1:1 ratio. This allows token holder the flexibility to hold tokens in either form for utility.
2. The ERC-20 token can be swapped for the XDC token at a ratio of 1:1. This swap can be made on the AlphaEx exchange.
3. 15 B (15%) of total token pool of 100B have been made available for the XDC-E pool of tokens. Of the 15 billion possible XDC-E tokens, only 6 billion are available for the ICO and the ones not purchased will be returned to the XDC hedge pool on the hybrid blockchain.
4. Pre-ICO investors and XDC token holders can convert their XDC tokens to XDC-E

### 3.3 XDC Protocol for DApps

XDC protocol is architected to support development of DApps, adherence to regulatory compliance and use currency of choice for customer needs

Fig.3.3 XDC Protocol for DApps

XinFin has developed hedge pool that protects participants from the fluctuations in the price of XDC tokens.

**How it works:**

Value of transaction to be mutually agreed in FIAT currency

Sender to buy tokens equivalent to agreed transaction value (on day of smart contract creation)

At the time of settlement, Xinfin to ensure payment to receiver as per the agreed FIAT currency value

In case of any appreciation of tokens, tokens equivalent to surplus amount to be taken out by Xinfin and in case of any shortage, tokens equivalent to short fall amount to be funded by Xinfin from hedge pool

**Applications:**

Trade and Business Efficiency Solutions

In case of repayment, tokens equivalent to FIAT currency value to be transferred for each installments



There are multiple Blockchain implementations today, however XinFin's hybrid blockchain protocol makes it ideal enterprise ready use case

#### Fig.3.3.1 Comparison with other Blockchains

Using our proprietary Blockchain platform, XinFin will offer three major services for real world applications

#### Fig.3.3.2 Services Offered

Utility for XinFin's XDC protocol is sector agnostic and our Application teams will be assisting clients in developing customized solutions

Fig.3.3.3 Areas for Solutions

## 4. TRADEFINEX

TradeFinex is a global marketplace platform for peer to peer trade and financing. The primary objective of XinFin is to minimize global infrastructure deficit by enabling peer to peer financing between Governments, corporations, buyers and suppliers to make efficient use of capital and deploy projects without burdening the Government Treasury. TradeFinex platform will help buyers secure capital at globally competitive rates, give suppliers visibility on global tenders & customer base and finally it gives financiers real time visibility on their investments using digitization and IoT integration of their assets. We will be rolling out TradeFinex platform that enables buyers, sellers and financiers around the globe to trade and finance projects that banking institutions are unable to take up. This applies specifically to critical public infrastructure projects that the Government needs to undertake for economic wellbeing of the citizens.

### How is TradeFinex platform different from others?

TradeFinex platform is a global marketplace that connects global beneficiaries, suppliers and financiers for trade, finance and real time settlement. TradeFinex platform has the capability to create legally binding digital smart contracts between participants over Blockchain. The platform simplifies the process in trade and financing, thereby making it more efficient. The platform also has capability to carry out real time cross border payments and settlements using a globally accepted token (XDC). The platform incentivizes participants in form of XDC tokens to carry out commerce using TradeFinex platform.

### How TradeFinex helps in cross border trade and financing?

The use of XinFin's XDC fueled tokenization scheme, permits trade and financing to be truly global in nature eliminating the funding gap owing to disparate currencies spread across the world. Moreover, investors in developed countries are averse to financing underdeveloped countries due to high currency depreciation risk, but with XinFin's common world token it makes it easier for them to lend money providing more stability and confidence to any cross border investment or debt.

#### 4.1 Who are the Participants?

1. **Beneficiary**
2. **Supplier**
3. **Financier**

1. **Beneficiary:** Beneficiary is an individual, an institution, a community or the government that is looking for project finance or to procure goods and services. The financing could be for procuring assets and setting up infrastructure (i.e. Hospital equipment, farm equipment, solar plant, roads, railways etc.)

2. **Supplier:** A supplier is an individual or a company that supplies goods or/and services to another organization. A supplier could be a product manufacturer, services provider or even a distributor. Using TradeFinex, the suppliers will get access to global customer base that is willing to undertake trade and financing activities.
3. **Financier:** Financier is an individual, an institution or a company whose business is providing, investing, or lending money. A financier is someone who is actively looking to invest in projects according to his sectorial alignment for attractive return on investment (RoI). On TradeFinex platform, a Financier may finance full project or a part of the project along with other financiers.

## 4.2 Contracting

### 4.2.1 What are smart contracts?

Smart contracts are self-executing, legally binding contracts with agreement terms between different parties like buyer and supplier, buyer and financier, financier and supplier respectively, written into lines of code. These codes and agreements constituted therein; are present across a distributed, decentralized, and secure blockchain network. Smart contracts enable trusted transactions & agreements to be performed among different, anonymous parties without any need of a central authority, legitimate system, or external implementation mechanism. Therefore, these kinds of contracts ensure transparent, traceable, and irreversible transactions.

### 4.2.2 What are the benefits of smart contracts?

The benefits of smart contracts include: Autonomy: Since the participants are the one making the contract, the need to have an intermediary, broker or lawyer is crossed out. Therefore, the participants enjoy complete authority over the agreement without any manipulations from third party. Trust-Since all of the participants' documents are encrypted and put on a shared ledger, all the unreal excuses of their documents being lost are automatically ruled out. Backup-Since all the participants' documents are duplicated many times over TradeFinex blockchain, they always enjoy free backup. Safety-Cryptography (the technology of encrypting websites) ensures TradeFinex is never hacked and therefore, participants are safe in every aspect. Speed-Since smart contracts deploy a software code to automate tasks, participants save hours of time that would otherwise go towards manually processing all paperwork. Savings-Since there is no intermediary or third party, participants save big on fees paid to notary and more. Accuracy-Since everything is done digitally, the possibility of human error is automatically ruled out, hence the accuracy.

### 4.2.3 Will the smart contracts be legally binding?

Smart contracts or blockchain contracts or digital contracts over TradeFinex platform create and enforce an agreed upon performance between two parties, much like their traditional counterpart.

The only difference being the smart contracts that are computer-generated and it is the code itself that explains the obligations of the parties. In many cases, the parties to a smart contract are essentially strangers on the internet bound by the digitally-produced but binding agreement. Hence, the smart contracts over TradeFinex blockchain will be legally binding.

#### **4.2.4 How do I negotiate with others on TradeFinex?**

TradeFinex comes with one-of-its-kind messaging board that is user-friendly, effective and prompt. You can use this messaging feature to chat with other suppliers and financiers. You can exchange files, drawings, documents, and other information on real time basis with other parties. Messages pertaining to techno-commercial details can be exchanged to negotiate a deal with the other parties. Contact information of the registered users will be visible to other registered users. They can reach out to each other on their phone numbers and email ids stated in the contact information.

TradeFinex Video Presentation: <https://www.youtube.com/watch?v=QHvmkEsAiX0&t=104s>

### 4.3 Traditional methods of Trading and Financing

Today, inefficiencies in the trade and financing increases the cost of doing business and deprives access to the capital for the deserving

Fig.4.3 Previous methods

#### Beneficiaries

1. Limited avenues for raising funds
2. High cost of capital
3. Low clarity on supplier credentials
4. Long wait for access to basic infrastructure needs

#### Suppliers

1. Lack of visibility of prospective global buyers
2. Multiple intermediaries in cross border trade
3. Processing delays due to disjoint systems
4. No real time visibility on trade and recourse if conditions of trade are not met

#### Financiers

1. Limited visibility on global investment opportunities
2. Lack of visibility on health of investments
3. Cost escalation and completion delays
4. Low returns and limited incentives to finance infrastructure projects

#### 4.4 XinFin solution for Trade and Finance

XinFin will deploy Blockchain technology for improving efficiency in trade and financing

Fig.4.4 Xinfin Solution

**We help beneficiaries**

1. Raise funds
2. Minimize financing cost
3. Connect with credible suppliers and financiers
4. Achieve tech enabled sustainable living

**We help suppliers**

1. Find market for your product and services
2. Facilitate trade through global payment standards
3. Reduce cost and improve trade efficiencies
4. Improve trade visibility through real time information

**We help financiers**

1. Find global investment opportunities
2. Get real time MIS through digitization of assets
3. Monitor health of your investments and get visibility on repayment
4. Achieve healthy return ratios through our incentive programs

## 5. TRADEFINEX WORKFLOW

### 5.1 Finance Workflow

Fig.5.1 Finance Workflow

1. Beneficiary raises finance query on TradeFinex.org
2. Financiers review query and submit proposals
3. Beneficiary and Financiers accept proposal
4. Beneficiary and Financiers enter in to Blockchain based smart contract
5. Beneficiary and Financier wallet integration in smart contract
6. Milestone based disbursement of fund by Financiers to Beneficiary
7. Beneficiary makes supplier payments
8. Milestone based repayment by Beneficiary
9. Repayment completion and closure of smart contract

This is the basic workflow between Beneficiary and Financier for Financing of project.



Beneficiary Dashboard from where he can raise Finance:

Fig.5.1.1 Create Project

Financier Dashboard for submitting proposal:

Fig.5.1.2 Finance Proposal

Facilitating cross border trade and finance using TradeFinex platform, digitizing the assets and integrating over Blockchain.

Fig.5.1.3 Cross Border Trade & Finance Process

**Blockchain workflow:**

- Beneficiaries, Suppliers and Financiers will be connected through XinFin's TradeFinex platform and they can upload, view, bid and finance projects
- Digital smart contracts will bring transparency in disbursement and utilization of funds.
- Users will pay directly to IoT integrated smart assets, which in-turn will repay the financiers using digital smart contracts.
- All parties will have real time access asset's health and financial performance and visibility on repayment.
- Alerts pertaining to default, NPA can be configured.
- Our target customers are those governments who have limited avenues to capital

## 5.2 Trade Workflow

Fig.5.2 Trade Workflow

1. Buyer raise trade query on TradeFinex.org
2. Suppliers review query and submit proposals
3. Buyers and Suppliers accept proposal
4. Buyer and Supplier enter in to Blockchain based smart contract
5. Buyer and Supplier wallet integration in smart contract
6. Buyer deposits funds into escrow account of smart contract
7. Supplier completes contractual milestones and submits to smart contract
8. Milestone based supplier payment released from escrow smart contract
9. Trade completion and closure of smart contract

This is the basic workflow between Beneficiary and supplier for Trading of project.

Supplier Dashboard for submitting proposal to beneficiary:

Fig.5.2.1 Proposal page for Supplier

Facilitating cross border trade using XinFin's "Token of Trust"

Fig.5.2.2 Cross border Trade

**Blockchain Workflow:**

Blockchain enables merchants to share information on a secure private distributed ledger. The trade can be executed automatically through a digital smart contract that will be executed automatically once certain conditions of the trade are verified. The parties will have access to real time data and can perform peer to peer payments and information transfer without intermediaries.

---

## 6. MODULAR FLOW DIAGRAM

### 6.1 Beneficiary Module Diagram

Fig.6.1 Beneficiary Module Diagram

1. Beneficiary post a project
2. Notifications are sent to both Supplier and Financier or invitation to both Supplier and Financier.
3. Beneficiary gets proposal from Supplier and Financier
4. Beneficiary accepts proposal of Supplier
5. Smart Contract gets started
6. Supplier:
  - 5.1 Supplier Submits delivery confirmation
  - 5.2 If beneficiary confirms the shipment then payment is released
  - 5.3 If beneficiary rejects the confirmation then it goes back to supplier

- 5.4 Contract ends between beneficiary and supplier
- 7. Financier:
  - 7.1 Financier Release the finance payment
  - 7.2 Beneficiary submits EMI payment
  - 7.3 If financier accepts then contract ends
  - 7.4 If financier rejects then proposal goes back to beneficiary.

## 6.2 Supplier Module Diagram

Fig.6.2 Supplier Module Diagram

1. Supplier receives invitation from beneficiary or browse for projects posted
2. Supplier submits proposal
3. Proposal is then accepted by the beneficiary
4. Smart Contract is initiated
5. Supplier can invite sub-contractor
6. If supplier invites sub-contractor then sub-contractor submits the proposal and waits for confirmation from main supplier



7. If supplier accepts the sub-contractor proposal then smart contract for sub-contractor is initiated
8. Sub-contractor submits the delivery
9. If supplier confirms the delivery then supplier delivers that product to beneficiary
10. Beneficiary will then release the payment and the Contract ends
11. If supplier does not confirm the delivery then it goes back to supplier.

### **6.3 Financier Module Diagram**

Fig.6.3 Financier Module Diagram

1. Financier receives invitation from beneficiary or browse for projects posted
2. Financier submits proposal
3. Proposal is then accepted by the beneficiary

4. Smart Contract is then initiated
5. Financier then releases fund amount
6. Beneficiary then submits EMI payments
7. If financier accepts/confirm the payment then contract ends
8. If financier does not confirms the payment then it goes back to beneficiary dashboard.

## 7. TradeFinex Screenshots



## 7.1 Home Page

## 7.2 Beneficiary Dashboard



Fig.7.3 Supplier Dashboard



Fig.7.4 Sub-Contractor



Fig.7.5 Financier Dashboard

Fig.7.6 Contract Dashboard

## **8. TECHNOLOGY USED**

- PHP ( Code Igniter MVC frame work V. 3.1.7), for front end business logic development
- MYSQL, for backend database.

## **REFERENCES**

- [1] Ethereum White Paper
- [2] Ripple White Paper
- [3] Bitcoin White Paper
- [4] XDC White Paper