Blockchain: Financial Applications

Karan Bharadwaj
Sahil Dhankhar

Contents

Introduction

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 been implicated in the numerous unregulated cryptocurrencies that exist online. Financial institutions are only beginning to understand the potential applications of blockchains in conventionally regulated industries.

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 that makes it's most significant implementation in the financial industry. It's structure allows for automation, immutability, and decentralisation. These characteristics were carefully chose 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 must be 'signed' by 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 pairs share 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.

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. In doing so, one is not necessarily throwing out the baby(the blockchain) with the bath water(Bitcoin).

Network access permission:

1. Permissionless: network access is free and anyone can set up a node to validate transactions. It is an open decentralised ledger which records the transfer go value. every transaction is cryptographically chained to the previous transaction. Bitcoin and Ethereum are the major examples. Incentive mechanism is required fir such networks.

2. Permissioned: network access is restricted to a set of known participants. Ripple 3 is an example of permissioned systems.

Each member of the network, called a node, has a chain of blocks which constitutes a total history of transactions performed on the network. Each block holds a set of transactions, the size of which depends on the number of transactions completed in a given time period.

The recording of transactions on the blockchain undergoes the following steps:

1. Transaction definition: Sender transmits the transaction to the network. It includes details of receiver's public address, transaction value and cryptographic digital signature that proves authenticity of the transaction.

2. Transaction Authentication: The nodes on the network authenticate the transaction by decrypting the digital signature.

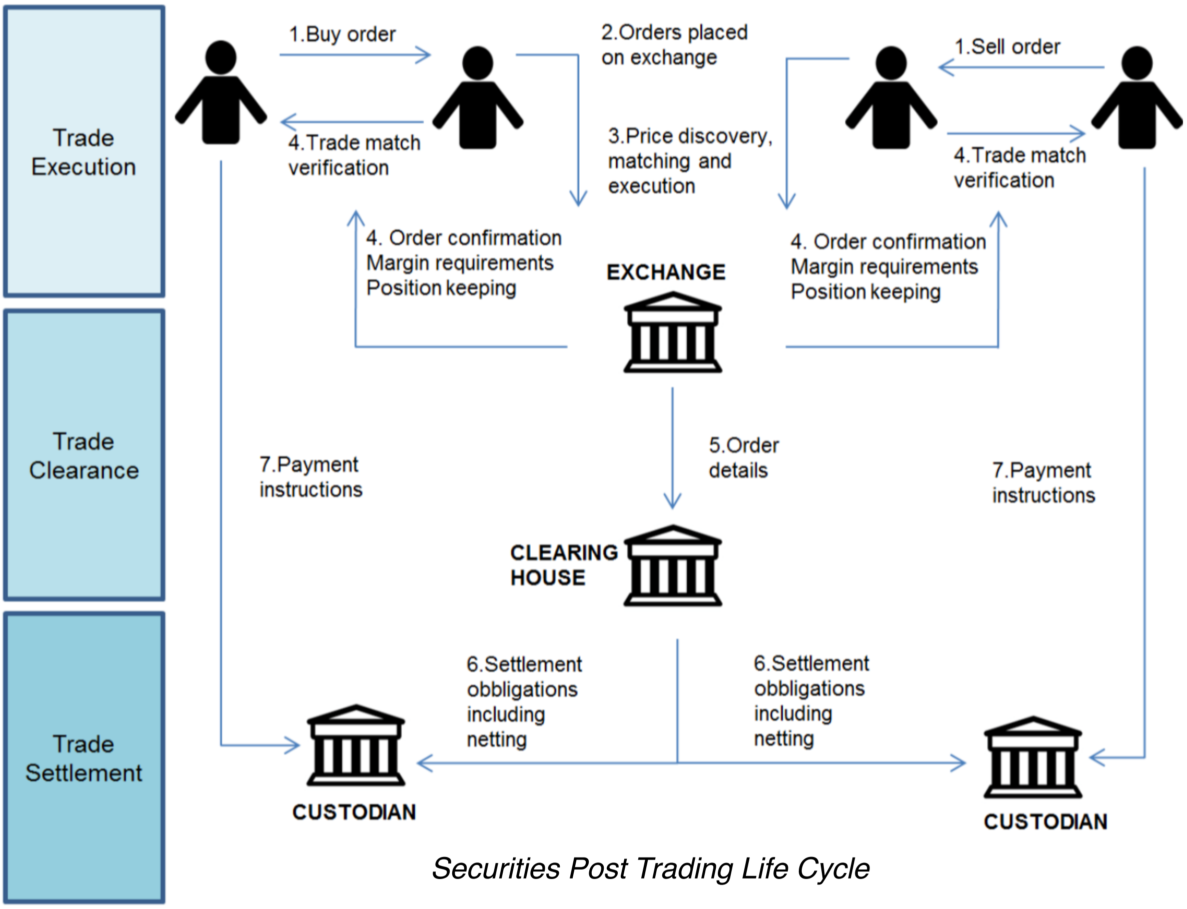
3. Block creation: The pending transactions are put in an updated ledger called block by one of the nodes in the network. At some time, the node broadcasts the block to the network for validation.

4. Block validation: The validator nodes of the network receive the block and work using iterative processes to validate it which requires consensus from the network. There are many validation techniques possible. For instance, Bitcoin blockchain uses “proof of work”, Ethereum uses “proof of stake” and Ripple uses “Distributed consensus”. The core idea remains the same, that is to prevent fraudulent transactions or double spending.

5. Block Chaining : After all the transactions are validated, the new block is chained into the ledger. The newly updated ledger is then broadcasted to the entire network.

Smart Contracts: This is a computer program that can automatically execute the terms of a contract. By being self-executing and having property ownership information embedded, they can solve the problems of counterparts risks. It is used to ensure compliance to legal and economic policy and regulations.

A contract is an agreement between two parties to do or not do something in exchange for something else. However a trust mechanism needs to exist between both parties in order to fulfil each side of the obligation. This is where the blockchain can be applied to create a trustless mechanism. The smart contract is both defined and executed by the code. Once a smart contract is launched and is running on the blockchain, neither side in an agreement require direct contact with the smart contract. Therefore the smart contract is autonomous in it's execution. For instance, a forwards contract encoded as a smart contract on a blockchain has the autonomy of executing automatically when the conditions of the contract are satisfied.


Trade Execution
Trade Clearance
Trade Settlement
1.Buy order
4.Trade match verification
2.Orders placed on exchange
3.Price discovery, matching and execution
1.Sell order
4.Trade match verification
4. Order confirmation Margin requirements Position keeping
EXCHANGE
4. Order confirmation Margin requirements Position keeping
7.Payment instructions
5.Order details
7.Payment instructions
CLEARING HOUSE
6.Settlement obbligations including netting
6.Settlement obbligations including netting
CUSTODIAN
CUSTODIAN

Securities Post Trading Life Cycle

Trading - Post trade life cycle

Securities trading lifecycle is a process which involves a large number of steps and stakeholders, which are introduced to mitigate different type of risks. This process today takes about three days between trade execution and settlement. Many market infrastructure institutions have explored the use of blockchain technology in this context. The trading lifecycle structure can be generalised in the following steps:

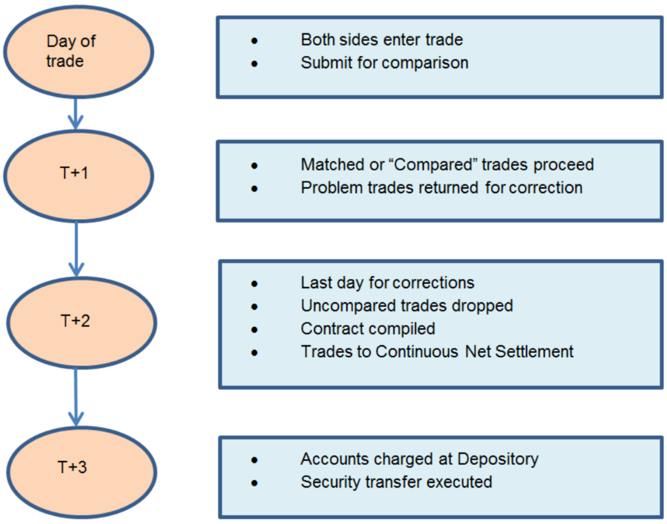
- **Trade execution:** in this phase buyer and seller request an order to their brokers, who act on clients behalf and submit orders to an exchange. When orders are matched, a confirmation is returned to brokers.

- **Trade clearance:** details about orders are sent to a clearinghouse, and original contract novation takes place. At this point clearinghouse acts as buyer to seller and as seller to buyer. In this way, clearinghouse will take settlement risk and guarantee trade execution for both counter parties. In front on that, clearinghouse requests adequate margins to their clearing members for mitigating their default risk.

- **Trade settlement:** in this phase obligations settlement is performed using netting. This involves orders grouping into a single transaction leveraging a custodian. In the end, buyer sets his obligation with the custodians throughout delivery versus payment and sellers get paid.

The entire trading process is made considerably more complex due to coordination between multiple necessary stakeholders. By adopting a shared distributed ledger platform, stakeholders could be eliminating the need for replication and duplication of the same data. As a consequence there will be reduced error rates, increased speed and cut cost associated with reconciliation and management of data. Speeding up the process of assets changing hands would result in lower capital requirements because there will be lower operational and counterpart risks.

Former JPMoragn top exec Blythe Masters, now the CEO of Digital Assets Holdings, said in a recent panel debating pain points of post trading processes: “We are spending a lot on keeping everything in sync, instead of having one truth and agreeing on it. We incessantly send it off to one another and attempt to reconcile, and go through extensive post-trade processes to remedy errors, fails and inconsistencies. distributed ledger technology could solve these points of pain.”


Day of trade
Both sides enter trade
Submit for comparison
T+1
Matched or “Compared” trades proceed
Problem trades returned for correction
T+2
Last day for corrections
Uncompared trades dropped
Contract compiled
Trades to Continuous Net Settlement
T+3
Accounts charged at Depository
Security transfer executed

Post Trading Life Cycle

Integrating BlockChain

The application of smart contracts along with the blockchain technology will allow the creation of any kind of token into the blockchain itself so that bonds, shares and other financial instruments can be represented. One possibility to simplify existing process is to represent securities and perform post-trade lifecycle on blockchain. Clearing and settlement will happen on blockchain, which will also be the depository for the assets. In this view, order matching is still done off-chain and then a clearinghouse can perform novation and split orders in a sell order with the original buyer and a buy order with the original seller. The entire process, as well as informations and rules representing securities will be encoded in smart contracts.

Let us consider a smart contract between a clearinghouse and a buyer. The clearinghouse will issue this contract once the trade is matched which will have the following methods to interact with the buyer:

- **Securities Order Details Method:** information about type, amount and securities rules can be requested by the buyer to review the order.
- **Settlement Method:** the buyer can call this method to pay the clearinghouse and receive securities. Settlement is triggered only if the buyer has the necessary funds. This may happen with the current DVP (Delivery Versus Payment).

In order to perform the payment, the buyer must have an account on the blockchain with adequate amount of funds. In case the buyer has not got enough funds on his account, a call to the DVP method would return an error and securities would not be settled. Other features can be added: the clearing- house can for example set a timeframe in which DVP can be executed or create margin accounts for clearing members, with custom rules defined in smart contracts. This solution reduces clearing and settlement time from days to minutes.
Furthermore, blockchain acts either as both clearing and settlement platform eliminating the need for reconciliation among different actors. Contract terms execution throughout code reduces back office workload and risk of errors.

Disruptive solution

A more sophisticated solution can also consider getting the trade matching and execution also on blockchain. In this case, the following participants would be involved:

- Brokers - which would have blockchain accounts and place orders for their clients in form of smart contracts.

- Clients among which payments can be done directly throughout accounts registered on the blockchain.

- Clearing firms - which can manage client identity through a KYC registry and would request brokers the margin requirements for trading activity.

A private permissioned blockchain in which nodes are controlled by a consortium composed by brokers and clearing firms is considered. The agents can put orders on the blockchain using the smart contracts, which automatically handle trading matching, execution and the terms of the contract. This solution will effectively reduce the reconciliation time and complexities while coordinating with the multiple stakeholders in the securities post trading lifecycle. Also, there will be significantly less capital requirement with lesser risk involved and no intermediaries present.

There are many companies trying to develop and deliver the blockchain software for the pre and post trading process that will run the future financial markets. Two of them are: NASADQ partnered with blockchain startup Chain and the other is, software delivered by Digital assets holdings.

Mobile Banking on Blockchain

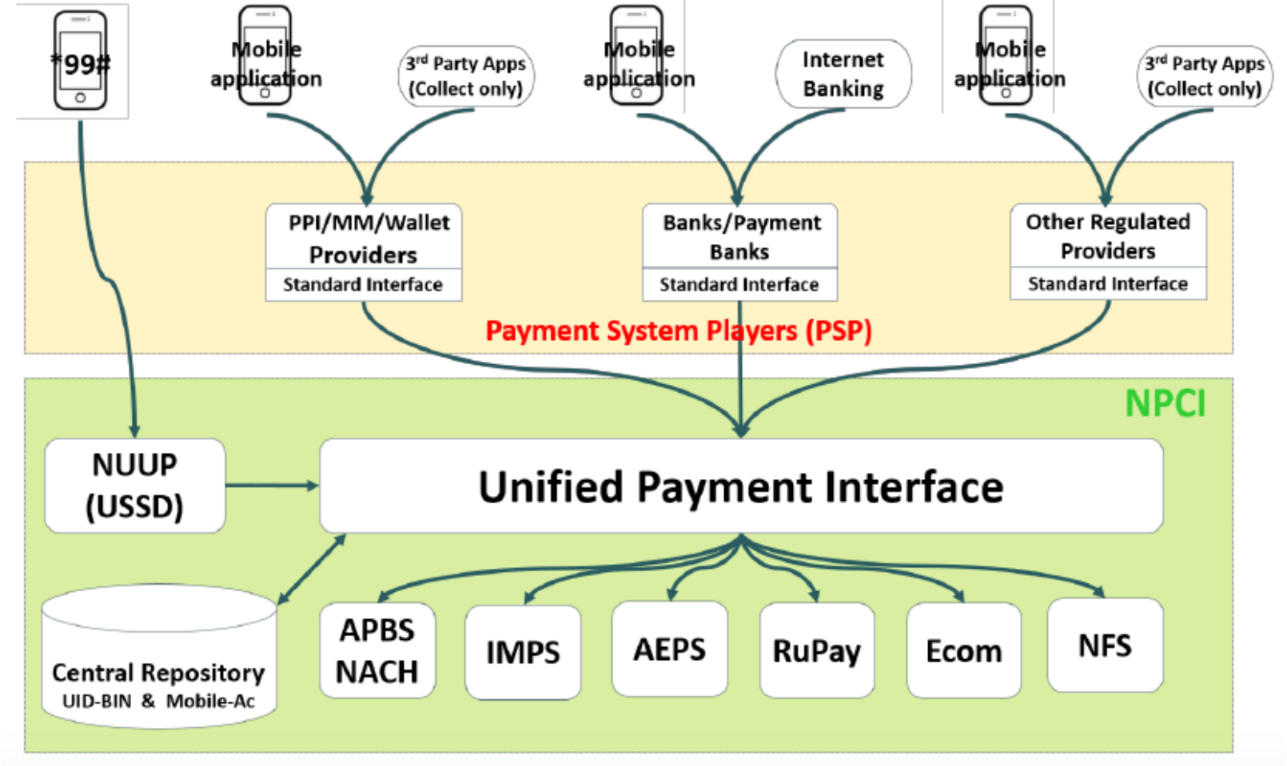
With the announcement of the Unified Payment Interface(UPI), India is on the brink of a revolution in the sphere of mobile banking. An explicitly stated goal of the UPI designed by the NPCI is to create an accessible, scalable, and secure payment and settlement system.

"Paying and receiving payments should be as easy as swiping a phone book entry and making a call on mobile phone. Everyone who has an account should be able to send and receive money from their mobile phone with just an identifier without having any other bank/account details."

"Solution should be scalable to a billion users and large scale adoption. This should allow gradual adoption across smartphone and feature phone users and provide full interoperability across all payment players, phones, and use cases."

"Solution should provide end to end strong security and data protection. Considering self-service mobile applications, data capture must be strongly encrypted at capture."

The graphic above shows the architecture of the UPI and the Payment System Players(PSP). APIs developed by the NPCI will be made available to such institutions to create a mobile banking ecosystem based on the criteria set forth.



Unified Payments Interface

This is where the blockchain comes in. Transactions over the a blockchain network is as simple as transmitting the transaction data to the nearest node. Even after complying with the regulatory standards of verification before transmission of transaction details, the network architecture connects the mobile application to the UPI. The blockchain network nodes will be privately owned and opaque to the outside world, which is a basic requirement for financial institutions. This greatly simplifies the consensus mechanism. In the case of the distributed bitcoin network, consensus is achieved by crunching numbers at a rate of 20 PH/s(petahash/s). This is a wasteful and unnecessary method of reaching consensus for private blockchains.

References

1. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System: Cryptography Mailing List, 2008.

2. Swan, Melanie. Blockchain: Blueprint For A New Economy: Sebastopol, O'Reilly, 2015.

3. Annexure T to RFP No. NPCI/RFP/2015-16/IT/001. Unified Payment Interface: API and Technology Specifications: 2015.

4. Copeland, Christopher and Zhong, Hongxia. Tangaroa: a Byzantine Fault Tolerant Raft: Stanford, 2015.

5. Castro, Miguel and Liskov, Barbara. Practical Byzantine Fault Tolerance: Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, 1999.

6. Blockchain Technology and Applications from a Financial Perspective: UniCredit, Feb 26, 2016.