Blockchain: Financial Applications

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 cyrptocurrencies 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. It's 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 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).

Mobile Banking on the 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.

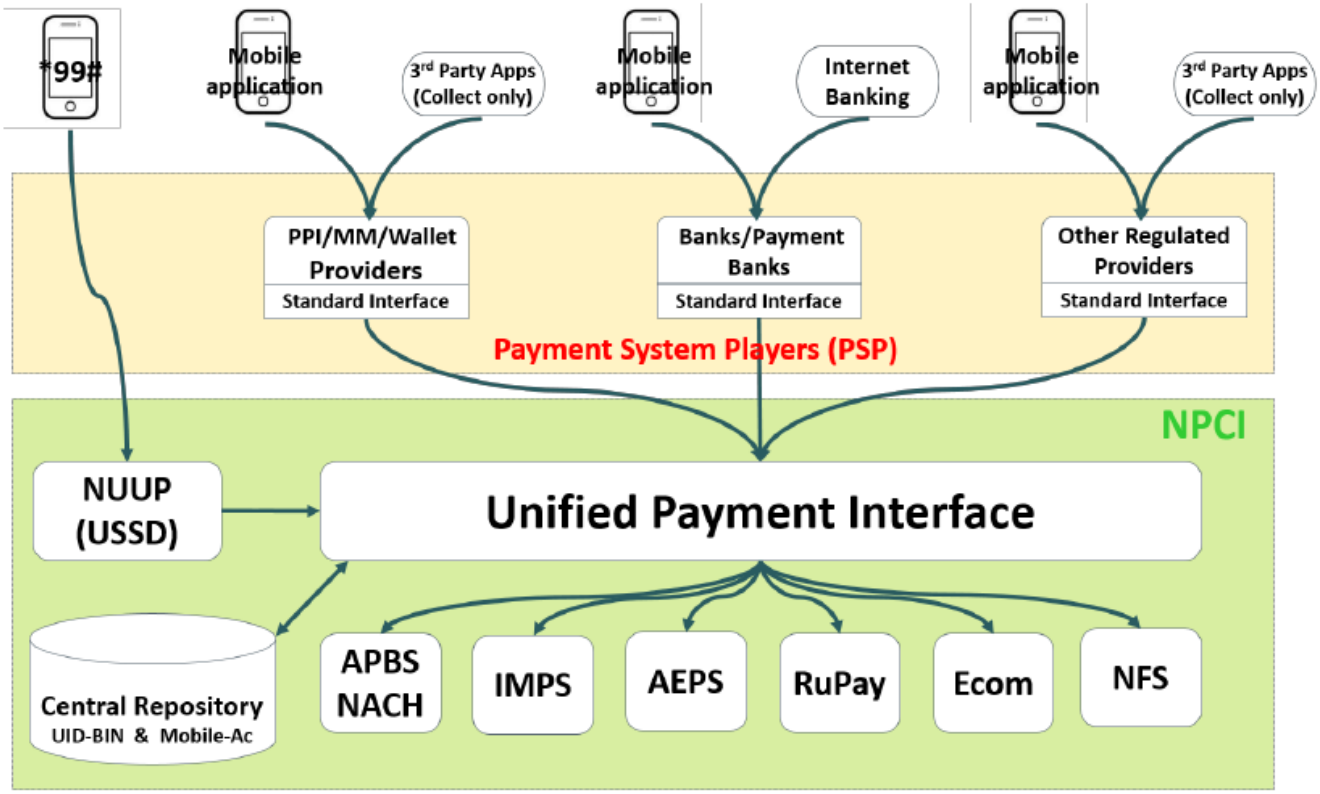
1. Paying and receiving payments should be as easy as swiping a phone book entry and making a call on mobile phone. Everyone who has an account should be able to send and receive money from their mobile phone with just an identifier without having any other bank/account details.

2. 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.

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

developed by the NPCI will be made available to such institutions to create a mobile banking ecosystem based on the criteria set forth.

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. 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 such 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.



The graphic above shows the architecture of the UPI and the Payment System Players(PSP). APIs

Smart Contracts

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 fulfill 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 automatically 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.

Additionally smart contracts can be used to trade various assets beyond digital currencies.

1. Public records such as land holdings, vehicle registrations, and various licenses.

2. Identification such as drivers licenses, passports, and identity cards.

3. Private records such as bets, contracts, loans, and wills.

4. Intangible assets such as patents, trademarks, and copyrights.

5. Financial transactions such as private equity, mutual funds, and derivatives.

The Ethereum platform, developed one such generalized blockchain. At present it provides the most developed solution for creating smart contract based applications. With Ethereum based companies making fascinating innovations, a semi-private or fully private blockchain based smart contracts platform is not too far away.

References

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

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

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

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

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