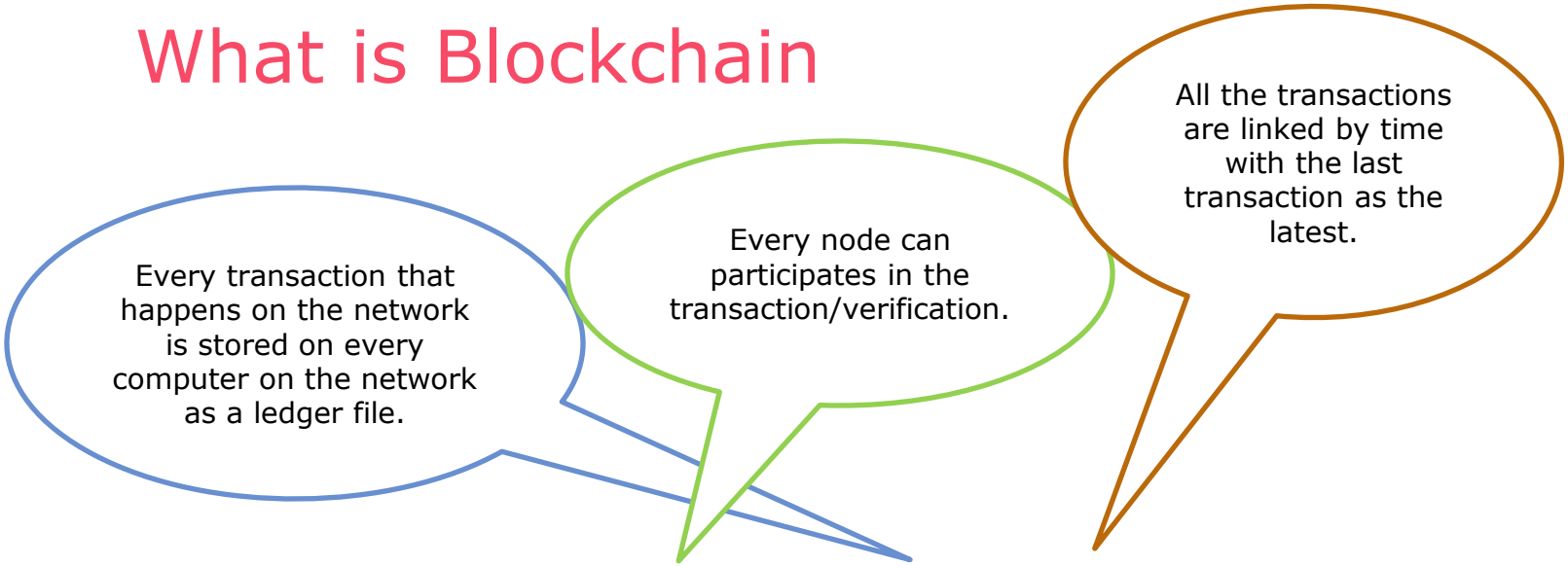
Blockchain and Wells Fargo iGnite@EGS

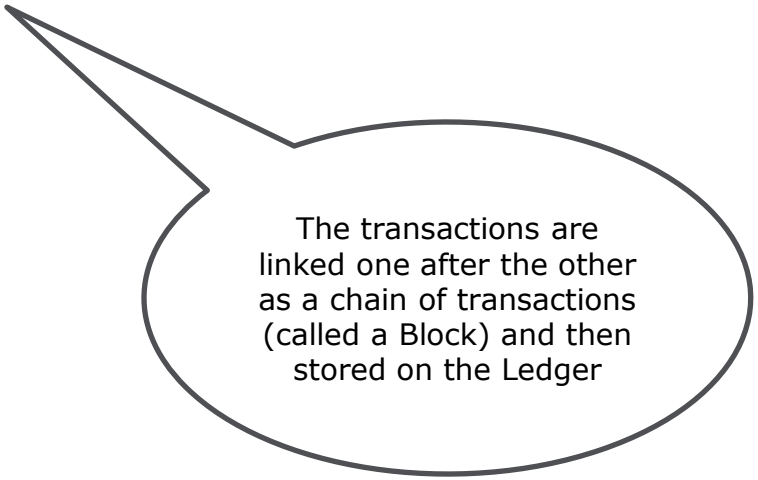
Sudheen Bhatt and Krishna T

Aug 9th 2016

What is Blockchain



A blockchain is a distributed shared ledger that maintains a continuously-growing list of data records secured from tampering and revision.



What is a Cryptocurrency

A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature.

Traditional Currency	Cryptocurrency
Assets have a physical or digital form – Currency, Bank Notes, Promissory Notes etc.	All assets a user holds are only in digital form.
Money flow & generation is controlled by a Central Authority like RBI, etc.	Money is generated by the system itself. Money is allocated to a public key (person) by the network or by trade.
Assets are held against an Account with respective Party (eg., Money -> Bank, Shares-> Demat etc)	All assets have only digital form and assets are held against a Public Key. A Public Key represents a User on the system.
I can access my account by using an UserId/Password.	My wallet can be accessed using my Private Key (Each Public Key will have its combination of Private Key)
Governing Bodies like Bank etc. holds responsibility for my Account and the assets in it	Responsibility lies with self. If a Private Key is lost, all the Money on the account is lost
Verification of funds/assets is done by the Bank or Governing Bodies in a transaction	As the ledger is stored on every node on the network, each node does the verification of funds on the source account by tracing the transaction chain on the Ledger until the Genesis Block.

Blockchain explained – Shared Ledger

A Peer-to-Peer Network

- ✓ A Block chain network of has multiple node (computers) that are connected in a peer-peer fashion that maintain the execution of blockchain transactions.
- ✓ These network nodes validate transactions, add them to their copy of the ledger, and broadcast these ledger additions to other nodes.

Blockchain

- ✓ A blockchain is essentially a distributed database of records or public ledger of all transactions that have been executed and shared among participating nodes.

Blocks

- ✓ A group of transactions linked together to form a Block

Transactions

- ✓ A transaction comprises of
  - i. One or More Inputs
  - ii. For the transaction to be valid, every input must be an unspent output of a previous transaction. Every input must be digitally signed
  - iii. One or More Outputs.

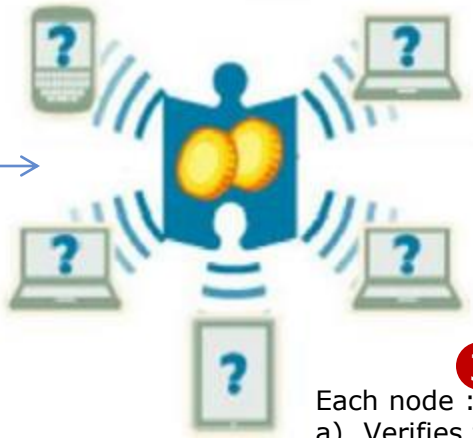
Mining

- ✓ *Mining* is a record-keeping service.
- ✓ Miners keep the blockchain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a *block*.

Blockchain explained – sequence flow

1 User A transfers 100 BTC to User B

2 The transaction gets propagated over the network.



3 Each node :

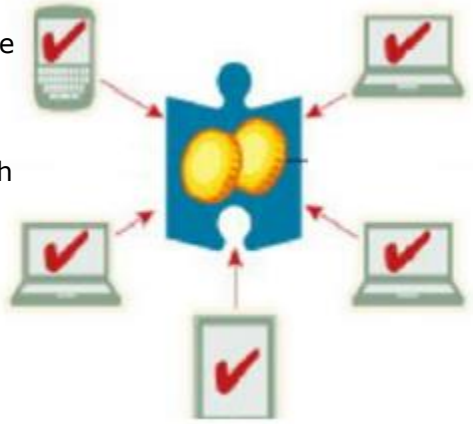
a) Verifies the signature of the Transaction whether it is legitimate.

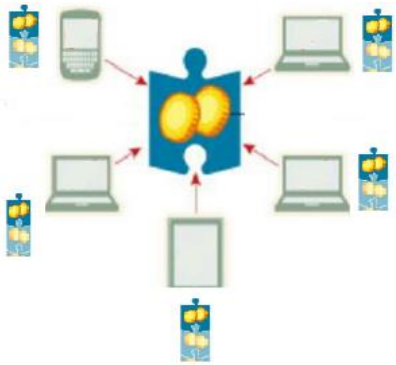
b) Verifies the Transaction balances by tracing the blockchain of the inputs all the way up to the Genesis(first) block

4 Once the transaction is verified, the nodes start a process called Mining.

Any Miner who wins the bid gets to propose the set of transactions onto the blockchain.

The block will then be propagated through out the network and all other nodes sync their local ledger with the new block.





5 The balances on the nodes will reflect: User A balance by -100 BTC and User B balance is increased by +100 BTC.

Double Spend Problem

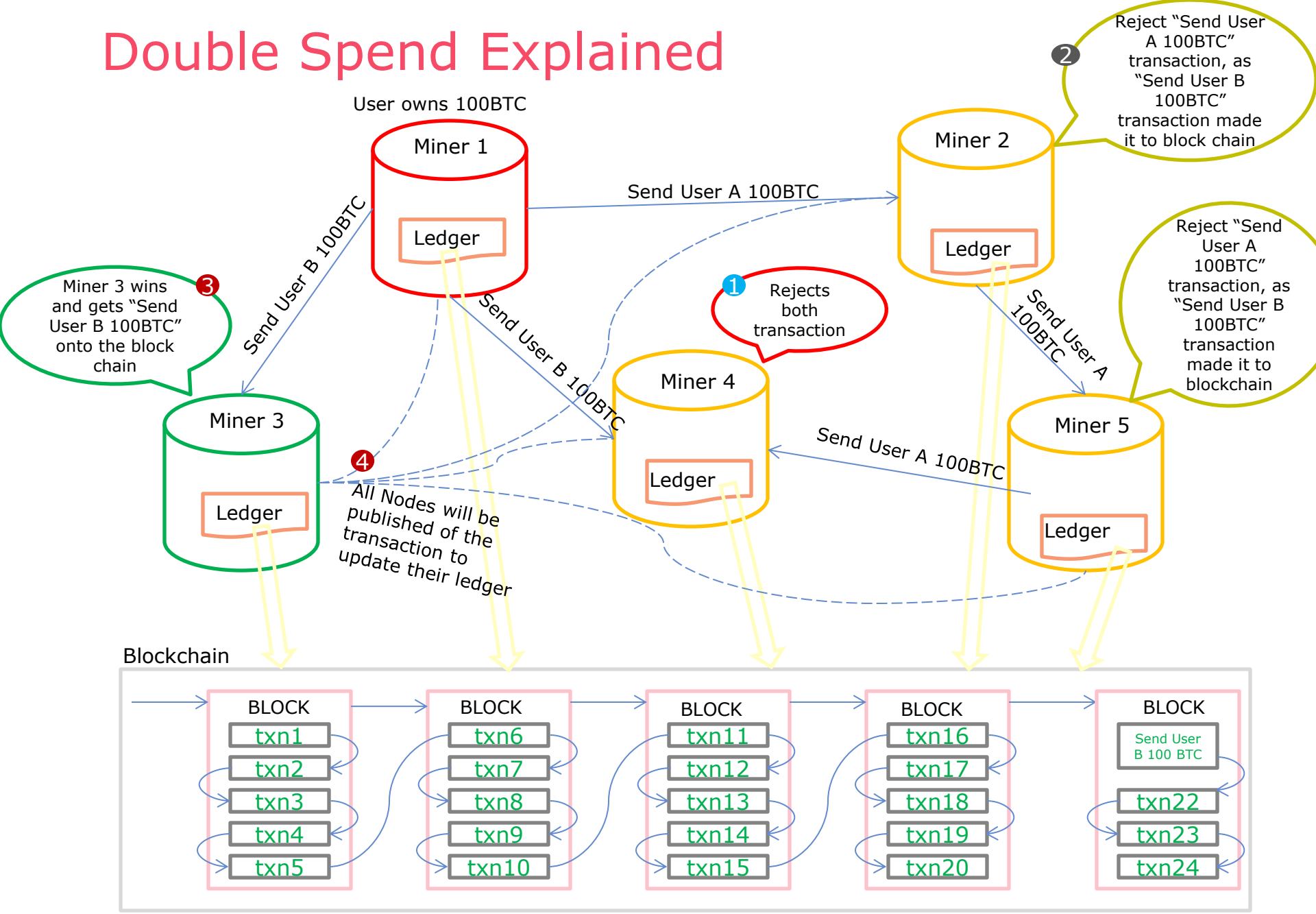
- Lets say a user has 100 BTC in his Block chain Wallet. He sends 100BTC to another user and he tries to send the same 100 BTC to himself. This is a Double Spend.

- As both the transactions have valid signatures of the User, both are valid transactions legitimately.

- There is no way to restrict the double spend because of the anonymity of the node in the de-centralized system. (In traditional banking, the Bank can detect this and can take appropriate action.)

- In the bitcoin world,
  - It is a good heuristic to wait for 6 confirmations (6 blocks added to the block chain after the block that has the transaction).
  - In bitcoin network, a bid is won every 10 mins and hence every block gets chained to the blockchain every 10 mins.

Double Spend Explained



51-percent attack

- The Block Chain decentralized network works on consensus mechanism. That is, for a transaction to be valid, it has to be verified by the nodes and added to the block chain and the more confirmations the better probability for the transaction to be valid.

- 51-percent attack is when a particular central authority (or a group of nodes) collaborate together to insert invalid transactions as part of the blocks to the block chain or in solving the algorithms to gain incentives.

- It is deemed to be highly improbable, as the amount of Hardware costs involved in having 51% of network nodes is very less in compared to the block rewards received for solving the algorithms

Few Bitcoin Stats

- The Total number of Bitcoins that can exist is fixed as **21 million BTC**. This limit will reach by 2140.
- Bitcoins mined so far = **15.8 million BTC**
- 1 BTC = 590.53 US Dollar (today)
- A block is mined every 10 minutes.
- Miners are rewarded 25 BTC for successfully mining a block. This amount reduces in half after every 210000 blocks are added to the chain.
- Each block has a size limit of 1,000,000 bytes. There is no limit on the transaction count.
- After 21 million limit is reached, the miners can only get to collect the Transaction Fees as the reward for mining a block.

Few Bitcoin Stats

- Miners are rewarded 25 BTC for successfully mining a block. This amount reduces in half after every 210000 blocks are added to the chain.
- 1 BTC = 571.82 US Dollar (today)
- The Total number of Bitcoins that will be generated is 21million. This limit will reach by 2140.
- After 21 million limit is reached, the miners can only get to collect the Transaction Fees as the reward for mining a block.
- Each block has a size limit of 1,000,000 bytes. There is no limit on the transaction count.
- A block is mined every 10 minutes.

Public vs Consortium vs Private Blockchains

Public blockchain

- In a public blockchain anyone in the world can read, send perform transactions, and can participate in the ***consensus process.***

Consortium blockchain

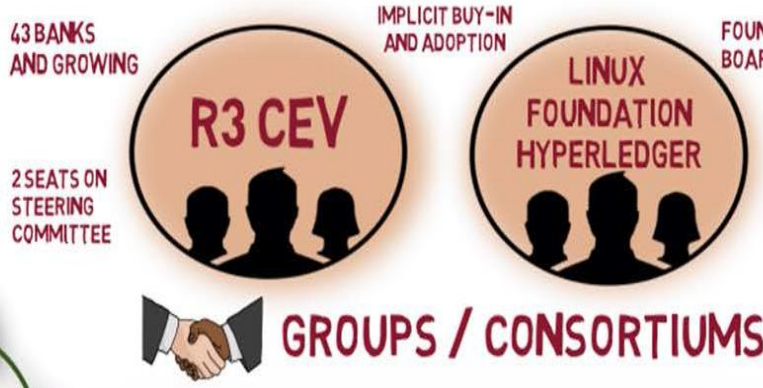
- In a consortium blockchain the consensus process is controlled by a pre-selected set of nodes that only participate in mining and cannot transact.

- A pre-selected set of nodes can only transact and cannot mine.

Private blockchain

- In a private blockchain write permissions are kept centralized to only pre-defined nodes. Read permissions may be public or restricted to an arbitrary extent defined by a centralized Admin.
  eg., Hyperledger

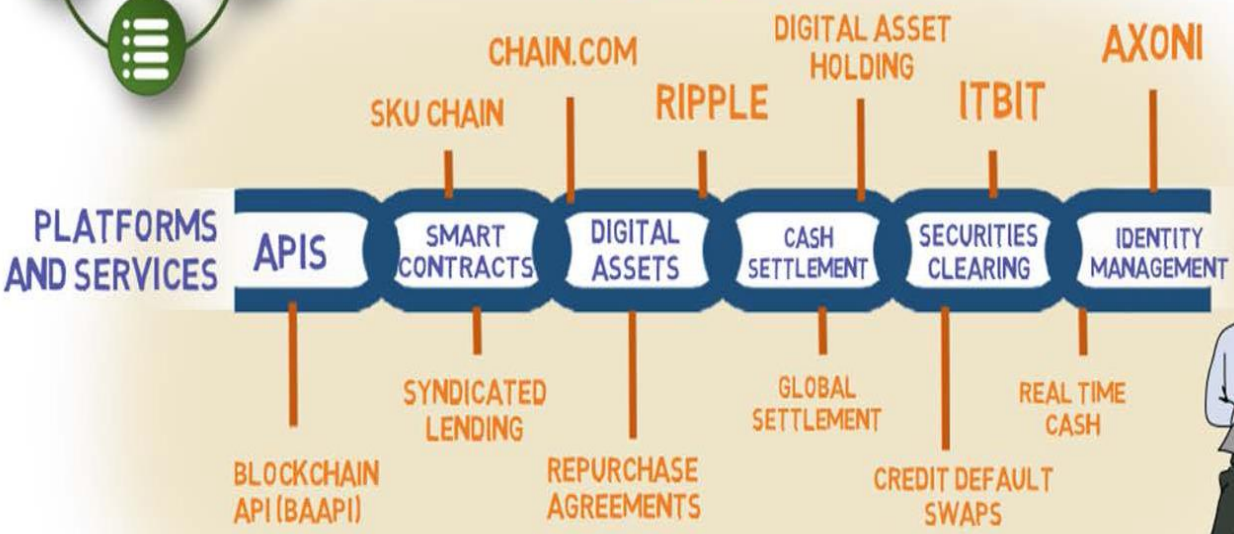
WELLS FARGO DISTRIBUTED LEDGER BANKING



CURRENT PROJECTS

BLOCKCHAIN API	POC FOR A BLOCKCHAIN APPLICATION PROGRAM INTERFACE (API) LAYER
ARGENT	GLOBAL CASH SETTLEMENT POC THROUGH R3CEV USING ETHERIUM
HERMES	INTL SUPPLY CHAIN FINANCING POC WITH SKUCHAIN, WAVE AND FLUENT

KEY VENDORS



LOB PARTNERSHIPS

- INTERNATIONAL
- CAPITAL MARKETS
- SECURITIES
- WHOLESALE
- WEALTH MANAGEMENT

SOLUTIONS & USE CASES

Proof of Concept – WF & ANZ

Swift based Correspondent Bank Network

- ✓ ~4 MM cross border payment transactions using Swift based Correspondent Bank Network
- ✓ Settlement in 1-2 days depending on CCY, Originating and Bene Bank location, etc.
- ✓ Manage Nostro relationships and maintain routing rules

2. Interbank (Nostro) Funding.

- ✓ 100s of Nostro Accounts across the globe. Cash monitoring and projections maintained throughout the day.

- ✓ FX / MM Settlement and counter party trades

3. Nostro Account Recon (Financial Risk Control)

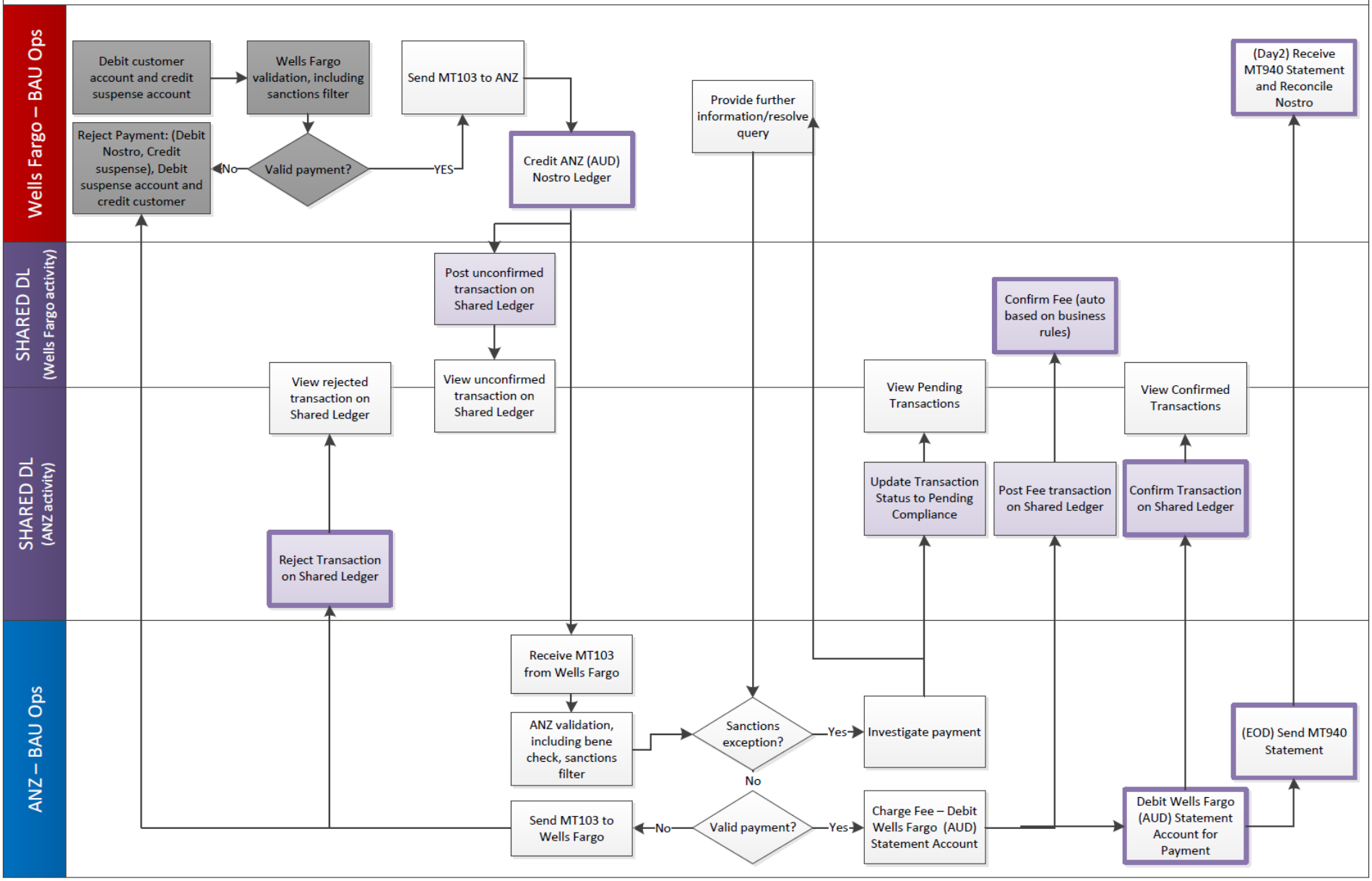
- ✓ Majority of Nostro transactions reconciled overnight automatically.

- ✓ Unmatched transactions resolved with manual effort. Breaks may be due to delay in fee assessment by correspondent bank, time delay in settlement or other reasons

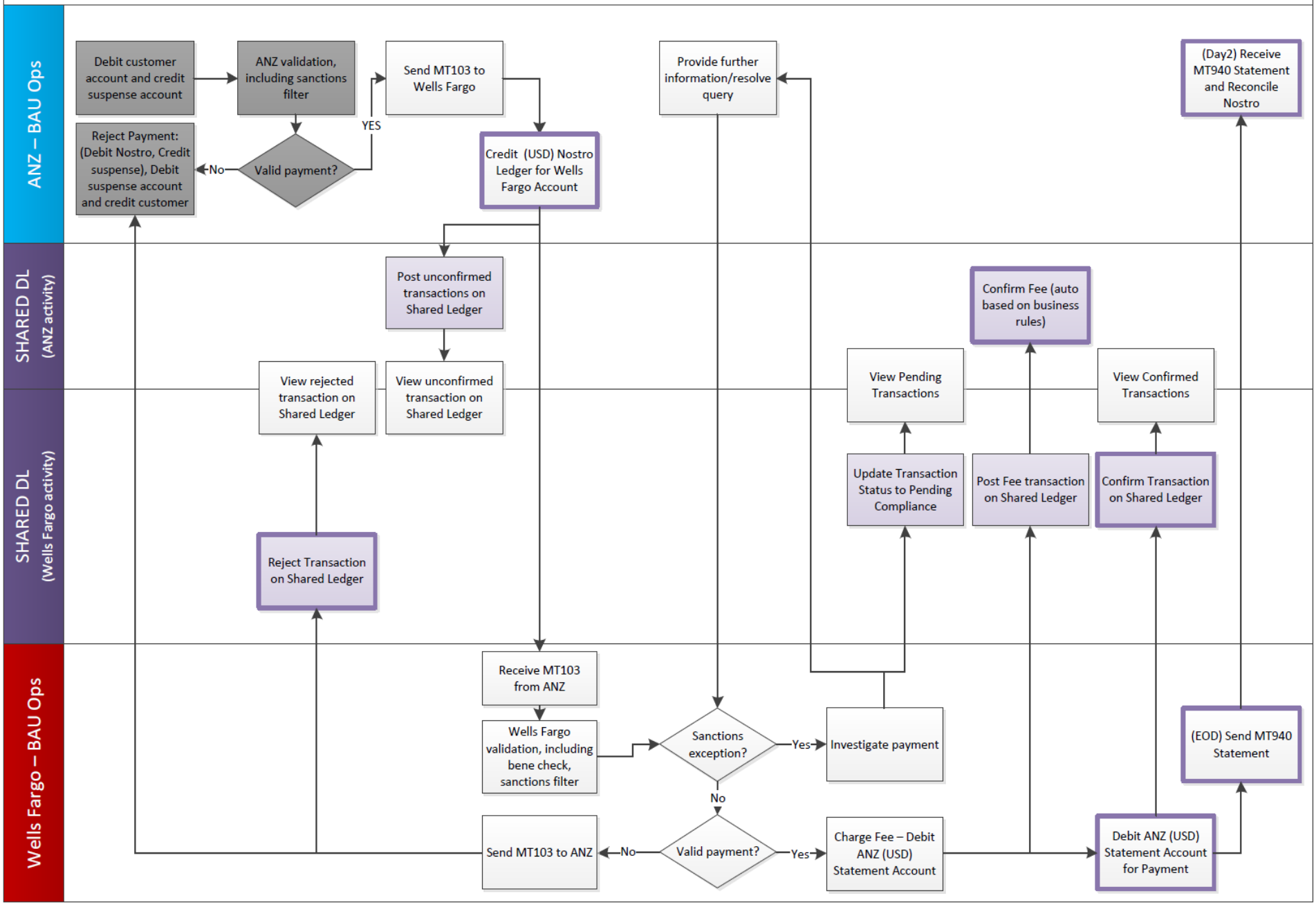
Scope - Proof of Concept

- ✓ Continue to use Swift based messaging for all payment transactions.
- ✓ Post transactions in parallel on the Block Chain Ledger.
- ✓ Use Block Chain Ledger for tracking Vostro account balance.
- ✓ Use API based interface with Core Payment Systems to run the POC in parallel.
- ✓ The futuristic goal of the POC is to get the Inter Bank transactions to be confirmed and recorded on Blockchain and the transactions happening on Swift network will be turned Off.

Process: AUD Payment Wells Fargo to ANZ



Process: USD Payment ANZ to Wells Fargo



Reference

http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

https://github.com/ANZ-Blockchain-Lab/Corres-Bank-POC/blob/master/docs/WF%20ANZ%20POC%20Approach.pdf

Thank You