Demystifying Blockchain for Islamic Finance

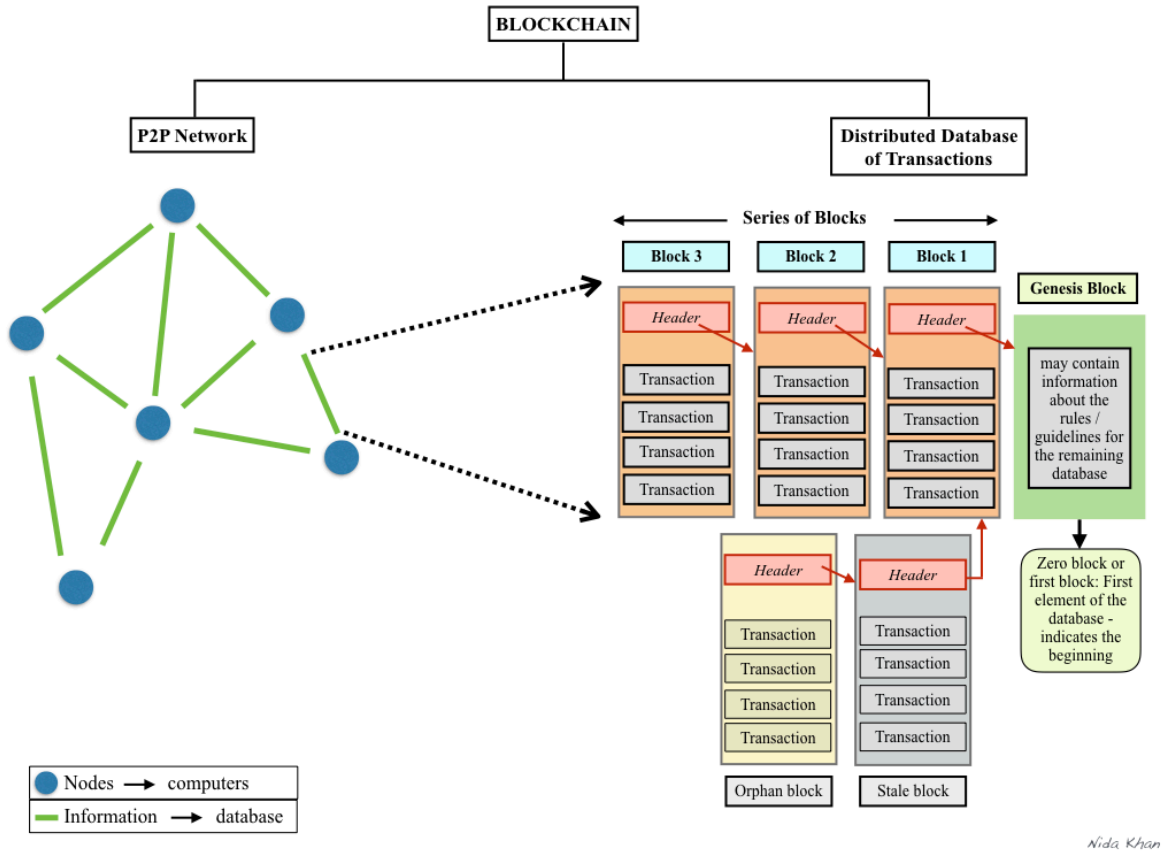
The financial crisis of 2007-2008 sowed the seeds for the support of a new revolution promising a way to finance that is more appealing to the much neglected segment of the customers. This revolution is spearheaded by a wave of fintech startups that are responding to the unique preferences and behaviours of the millennials in the area of finance and investment. This generation having witnessed the crashes of the stock market in 1981, 2001 and 2008 have lost trust in the public markets. Moreover with the advent of social media, technological aids for faster payments and startups like Mogo and others vying to become the 'Uber of the Financial Industry', the customer has become the one who decides what he wants to do and with whom, privileged with the ease to choose from among a plethora of services available. In this age it is essential to maintain trust through transparency and frequent communication. Since millennials are the largest of any generation and would be transforming every facet of the global economy it is but imperative to focus on their needs by incorporating the latest technologies that are transforming the financial services sector. The technology that is most promising and aptly suited to the needs of this generation is blockchain.

Understanding Blockchain

Blockchain is a public ledger of transactions that consists of a peer-to-peer network and a decentralised distributed database. It allows multiple parties who are not known to each other to safely and directly share a database without the need of a trusted third party working as an intermediary. Further it allows all participants to see all the transactions that are taking place. Cryptography and pseudonyms can be used to hide some aspects of the transactions but even then the amount of information leaked is more than traditional centralised databases. So a blockchain permits all users to read everything allowing no single user to control who can write in contrast to the centralised databases being used where a single entity is responsible for controlling read and write operations and all the other users are subject to this entity's decisions. Blockchain thus transfers the power in the hands of the users creating not just transparency but inculcating a feeling of trust.

The pictorial depiction of the blockchain with this article is an attempt to make the concept easy to comprehend. The ledger represented is ever expanding and is protected against revision, deletion and tampering. Any manipulation of data

would be easily discovered as the original hash would still exist on millions of nodes. Blockchain would not just add transparency and enhance trust but it would also provide security by blocking 'identity theft' and stopping 'denial-of-service attacks'. The block header hash is computed by using only the block header and serves as a digital fingerprint of a block. The block header contains a reference to the previous node, data related to the mining operation and information on all the transactions in the block.



When any new information enters the P2P network it is communicated to all surrounding nodes. When any node wants to add a transaction to the ledger a consensus is formed in the network to determine whether this transaction should appear in the ledger and this consensus is termed as a block. This requires a way or a consensus system to make everyone on the network agree to this addition and the algorithm implemented by the blockchain to achieve this is called the **proof-of-work** consensus using blocks. Transactions are grouped in blocks with each block referencing the previous one called its parent and there is only a single chain of blocks that is replicated in the entire network. In this network some nodes function as miners and create a new local block with pending transactions. They compete with other miners to see if their local block becomes the next block to be added in the chain that is available for the entire network. A decision is reached by declaring that node as the winner which is able to reach

the solution of a difficult mathematical problem based on a cryptographic hash algorithm involving guesses and finding a block to be added is rare for a miner. This solution is called **proof-of-work** and is included in the new block as a proof of the computing effort exerted by the winning miner. The node that wins publishes its local block and all the transactions in this local block become confirmed. It also brings in some form of money for that node as an economic incentive. A miner in the blockchain expends huge amount of computer resources as it has to test thousands of random strings every second to try to form a new block and this is the reason why a person has to pay to store data on the blockchain. Reading data is free. The default mechanism is that every node receives blocks mined by other nodes in the blockchain network and choosing to become a miner node is voluntary. According to Alex Tapscott, co-author of the book *Blockchain Revolution,* in order to mess with the blockchain technology *"**a hacker would have to access simultaneously every single computer on the ledger, an act requiring the same computing power as a googolian."*** This makes the technology a panacea for online fraudulent transactions as there is no single point of failure.

Financial Applications

The Islamic Finance (IF) industry can utilise the benefits offered by a blockchain for all those transactions where the loss of confidentiality is not desired / ignored for the transparency the technology offers together with the reduced infrastructure costs by elimination of the need for middle men. A few applications have been mentioned below:

1. Smart Contracts

Currently smart contract technology is being built on top of Bitcoin blockchain and other virtual currencies. Smart contracts are computer programs with the capability of unilaterally applying strict rules and consequences on the basis of fresh data inputs. Further the blockchain assures that everyone is seeing the same thing without the reliance on having to trust each other. Any kind of business logic relying on data can be coded by way of smart contracts. Securities that are based on payments and rights, which are executed according to predefined rules can be coded as a smart contract in capital markets. Experiments are ongoing on the issuance of smart bonds. Sukuk issuance follows a strict Shariah law and principles of permissible variance, cleansing, the balance-sheet ratios to be satisfied, the 'conglomerate' issue and the 'core' activities. These can be coded as **'if-then'** statements (where the **'ifs'** are preconditions that must be met in order to trigger the **'thens'**) to ensure both

compliance to the Shariah and transparency for all involved. Examples *Ethereum*, *RootStock*.

2. Supply Chains

Supply chain management comprises of tracking the origin and movement of items which can suffer from counterfeiting and theft. The financially critical items like bills of lading or letters of credit can be tracked by a blockchain taking away the possibility of a group of users from corrupting the documents and end users would have more trust in what they receive paving the way for a smart Shariah compliant supply chain finance (SCF) . Examples of companies using this technology are *Skuchain*, *Wave*.

3. Digital Assets

The conventional sector is using blockchain to create digital assets like stocks, bonds and land titles. The IF industry can also venture in these areas by creating Sukuk or Islamic bonds on top of the blockchain. Examples of companies using this technology are *NASDAQ*, *Chain*.

4. Payment Systems

Bitcoins are being used to send money to anyone across the world and merchants are accepting bitcoins as payments. Each bitcoin is related to a particular user secured by means of an encrypted electronic signature. The movement of a bitcoin from one user to another user is recorded in the distributed ledger and the exchange take place by changing of the bitcoin address of the sender to the bitcoin address of the receiver imitating the transfer of physical cash from one wallet to another person's wallet. The entire record of this movement is recorded in the distributed ledger similar to an International Payments System. A very apt use of this in the IF industry along with other predictable usages would be in Hawala. Blockchain based hawala banking would make the process more trustworthy, more legally appealing and transparent while providing an alternative to traditional hawala. Examples *BitPay*, *Abra*.

5. Digital Identity

The blockchain ID can be used to sign digital documents or sign in to websites. IF banks can be set up as authenticators for such blockchain ID's or they can

partner with blockchain companies working on the same for facilitating instantaneous cross-border transactions. An example of a company offering such services is *Keybase*.

6. Data-Driven Decision Making (DDDM)

DDDM is an approach to business governance that can be backed by verifiable data. It is a way to gain competitive advantage and a study conducted by MIT found that organisations using this approach had 4% higher productivity and 6% higher profits. Blockchain provides a very efficient way of creating this verifiable record of any data, file or business process on the blockchain. A few examples are a verifiable audit trail of insurance claims and archiving of communication to create a verifiable record of a company's online conversations. Examples are *Factom*, *Proof of Existence*. The IF sector can utilise the DDDM approach to back all major decisions including innovation and incorporation of new technologies separate from the blockchain to gain competitive advantage and deliver products and services tailored to the needs of the millennials.

The Way Forward

A few challenges need to be thought of before incorporating blockchain. It is a nascent technology, involves large energy consumption, has an uncertain regulatory status, involves high initial capital costs, needs cultural adoption, entails significant changes or complete replacement of existing systems and security and privacy concerns need to be taken care of. However technologically savvy innovative ideas are much needed in the IF sector to rise up to the dual challenge of providing financial services completely in sync with the Shariah and blockchain is a very good option to initiate the step towards establishing a strong foothold in this 4th industrial revolution.