TOPIC OF THE WEEK

FEB'18 (22 to 28)

Topic: Block chain Technology

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology.

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." - Don & Alex Tapscott, authors Blockchain Revolution (2016)

Blockchain is the digital and decentralized ledger that records transactions without the need for a financial intermediary, which in most cases is a bank. A blockchain is an anonymous online ledger that uses data structure to simplify the way we transact. Blockchain

allows users to manipulate the ledger in a secure way without the help of a third party.

Blockchain enables two entities that do not know each other to agree that something is true without the need of a third party. As opposed to writing entries into a single sheet of paper, a blockchain is a distributed database that takes a number of inputs and places them into a block. Each block is then 'chained' to the next block using a cryptographic signature. This allows blockchains to be used as a ledger which is accessible by anyone with permission to do so. If everyone in the process is pre-selected, the ledger is termed 'permissioned'. If the process is open to the whole world, the ledger is called unpermissioned.

A blockchain is anonymous, protecting the identities of the users. This makes blockchain a more secure way to carry out transactions. The algorithm used in blockchain reduces the dependence on people to verify the transactions.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

"The traditional way of sharing documents with collaboration is to send a Microsoft Word document to another recipient, and ask them to make revisions to it. The problem with that scenario is that you need to wait until receiving a return copy before you can see or make other changes because you are out of editing it until the other person is done with it. That's how databases work today. Two owners can't be messing with the same record at once. That's how banks maintain money balances and transfers; they briefly lock access (or decrease the balance) while they make a transfer, then update the other side, then re-open access (or update again).

With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people.

Blockchain Durability and robustness

Blockchain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the blockchain cannot:

1. Be controlled by any single entity.
2. Has no single point of failure.

The blockchain network lives in a state of consensus, one that automatically checks in with itself every ten minutes. A kind of self-auditing ecosystem of a digital value, the network reconciles every transaction that happens in ten-minute intervals. Each group of these transactions is referred to as a "block".

Two important properties result from this:

1. **Transparency** data is embedded within the network as a whole, by definition it is public.
2. **It cannot be corrupted** altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

A network of so-called computing "nodes" makes up the blockchain.

Node: (computer connected to the blockchain network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the blockchain network. Together they create a powerful second-level network, a wholly different vision for how the internet can function.

The blockchain potentially cuts out the middleman for these types of transactions. Personal computing became accessible to the general public with the invention of the Graphical User Interface (GUI), which took the form of a "desktop". Similarly, the most common GUI devised for the blockchain are the so-called "wallet"

applications, which people use to buy things with Bitcoin, and store it along with other cryptocurrencies.

Blockchain & Security: By storing data across its network, the blockchain eliminates the risks that come with data being held centrally.

Its network lacks centralized points of vulnerability that computer hackers can exploit. Today's internet has security problems that are familiar to everyone. We all rely on the "username/password" system to protect our identity and assets online. Blockchain security methods use encryption technology.

The basis for this is the so-called public and private "keys". A "public key" (a long, randomly-generated string of numbers) is a users' address on the blockchain. Bitcoins sent across the network gets recorded as belonging to that address. The "private key" is like a password that gives its owner access to their Bitcoin or other digital assets. Store your data on the blockchain and it is incorruptible. This is true, although protecting your digital assets will also require safeguarding of your

private key by printing it out, creating what's referred to as a paper wallet

Blockchain is still a (relatively) new technology and is not without its problems. For a start, there are ongoing concerns about privacy in the settlement and storage of securities – blockchain providers are working hard to address.

Banks are also at threat with block chain, since more and more firms (using their IT service providers from India and elsewhere) will build systems that can create and exchange 'blocks' with one another completely legally, without ever having to use the banks as a financial intermediary.

Block chain is not a panacea for all issues facing the banking system today. However, block chain is an ideal technology to ensure proof of integrity to the data and reduce incidents of fraud.

Week: 22nd to 28th Feb2018

Suggested Reading:

- ✓ https://www.coindesk.com/information/what-is-blockchain-technology/

- ✓ https://blockgeeks.com/guides/what-is-blockchain-technology/

- ✓ http://www.thehindu.com/business/blockchain-tech-could-help-prevent-frauds-like-at-pnb/article22818844.ece