BRIEFING PAPER

CUTS Centre for Competition, Investment & Economic Regulation
CUTS C-CIER

4/2018

Introduction to Blockchain Technology

The rapid evolution of Blockchain in the recent years has caused ripples in the economy and gripped the world's attention. By offering the possibility of dealing with third parties using a secure, shared, indelible decentralised ledger, blockchain technology has the potential to deliver significant value in transactions and is set to revolutionise everything from banking systems and stock exchanges to property registries, contract law and corporate sustainability.[1] The interest in this nascent technology emanated in 2009 from Satoshi Nakamoto's white paper on Bitcoins, a form of cyrptocurrency that operated on blockchain technology.[2] In 2017, it hit the peak of Gartner's 'hype cycle' of emerging technologies, leaving behind autonomous vehicles and smart robots.[3]

This Briefing Paper aims to introduce the concept of this emerging technology along with its ongoing and potential use cases, globally and nationally.[4]

What is a Blockchain?

A Blockchain is essentially a *'distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties'*.[9] It enables peer-to-peer transactions thereby eliminating third parties from the scenario (for instance, banks/financial institutions/state, in the case of traditional mode of exchanging currency) and ensuring transparency as well as cost effectiveness. The most recent and controversial example that has been intrinsically tied to this technology is its use in cryptocurrency transfers.

A Blockchain may be *public or fully private*.[10] The former is completely open for everyone to participate, i.e. anyone can join the network, request to transact or participate in the consensus process, as in the case of popular public blockchains such as Bitcoin, Ethereum, Litecoin etc.[11] The latter is a permissioned network that works on an invite basis wherein the write permissions are being centralised with one single entity/organisation.[12] Thus, it is not decentralised in its true sense and it places a restriction on the number of participants in a transaction as well as the validation process.[13]

Somewhere between a fully decentralised public Blockchain and a single highly trusted entity model of a private block chain, lies a *Consortium Blockchain* that provides a hybrid between the two types of Blockchains and is partially decentralised i.e. the consensus process is controlled by pre-selected set of nodes. For instance, in a consortium of thirty organisations, it may be pre-decided that sixteen of the selected members must sign every block in order for that block to be valid.[14]

Recently, four automobile giants, BMW, GM, Ford and Renault, along with other stakeholders, launched a consortium blockchain platform called Mobility Open Blockchain Initiative (MOBI) targeted at making mobility safer, greener and affordable.[15]

Decoding a Block in a Blockchain

A block includes the following three crucial elements[16]:

a. The **Data** stored on the block, for instance, a block of bitcoins includes the sender's address, receiver's address and the Bitcoin amount.

b. Each block contains a **Hash** which serves as its unique identification akin to a fingerprint. When a block is created, depending upon the data stored on it, it receives a hash, which changes if there is a change of data on the block.

c. Each block also contains a **Hash of the previous block** that creates a chain of blocks. Thus, making the chain tamperproof as any change in one block requires updating all the preceding blocks.

The Genesis Block
Also known as Block 0, it is the ancestor that every other block in the chain can trace its lineage back to. It is the first ever block of Bitcoin to be mined. The creator of Bitcoin, operating under the alias of Satoshi Nakatomo, mined the first block of Bitcoin or the Genesis block on January 03, 2009. The block's raw data contained a secret message: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*" One theory suggests that the text comes from a headline in the January 03, 2009 edition of The Times, a London-based newspaper. The article reported on the British government's failing to stimulate the economy following the 2008 financial crisis.
Source: Retrieved from: https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/ (last accessed on May 09, 2018)

How Does the Technology Work?

An individual wanting to become a part of the Blockchain or to transact using a medium that operates on the Blockchain Technology, needs to request a transaction and can then expect to be included if it is validated. The process for the same is carried out as follows:

- When a digital transaction is carried out, it is grouped together in a cryptographically protected block. This block contains a digital signature as well as a timestamp and other relevant information about the transaction, but not the identities of individuals involved in that transaction. This block is then transmitted to the entire network.[17]

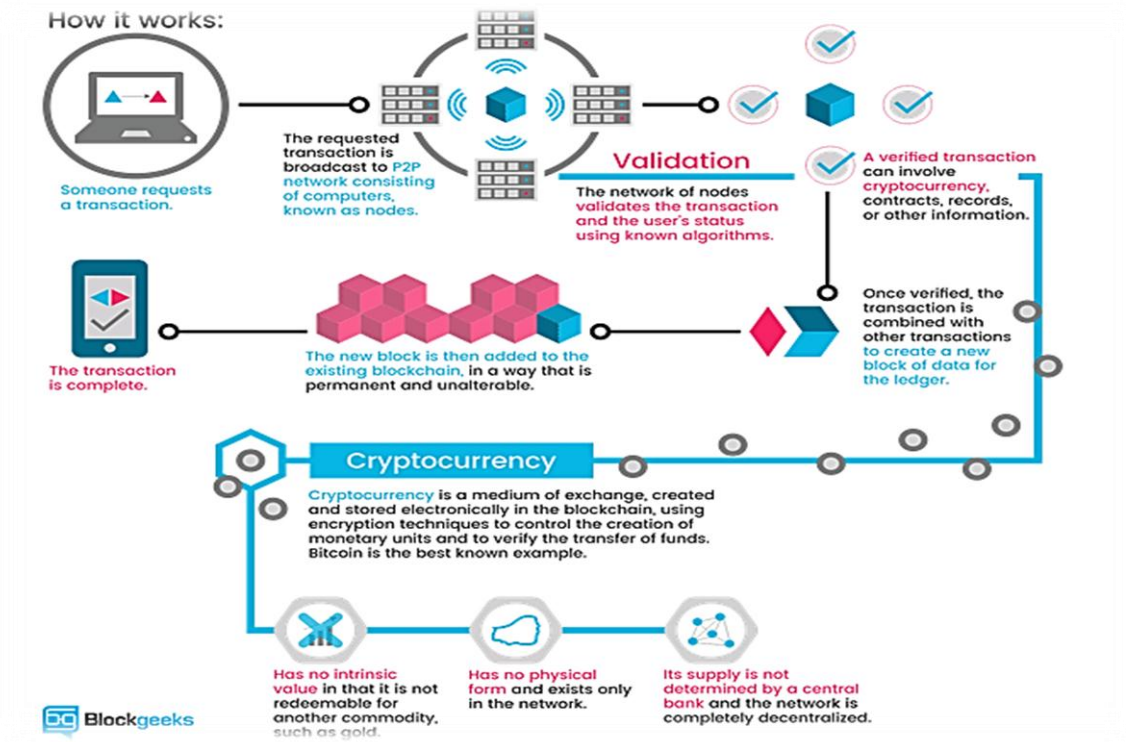
- Miners (members/coders in the network with high level of computing powers) then compete to validate the transactions by solving complex coded problems for which they are incentivised via a reward.[18] For instance, in the Bitcoin Blockchain network the first miner(s) who is able to solve the mathematical equation receives Bitcoins.

  This process validating the transaction by incentivising is based on the economic concept of *'tragedy of commons.'*[19] The entire process of validating a transaction on the blockchain requires huge amount of computational powers. Thus, incentivising ensures that every individual gives up a small amount of computational power to earn a reward and thereby serves the network.

- The validated block of transactions is then time-stamped and receives a hash. It is then linked to older blocks in a proper linear, chronological order with every block containing the hash of the previous block thereby making a chain of blocks that reflect all transactions made in that Blockchain.[20]

- The entire chain is continually updated so that every ledger in the network is the same, giving each member the ability to prove the credibility of others at any given time.[21]

How Blockchain Works



Source: Retrieved from, https://blockgeeks.com/guides/what-is-blockchain-technology/ (last accessed on 09.05.18)

Establishing Digital Trust, Privacy and Security

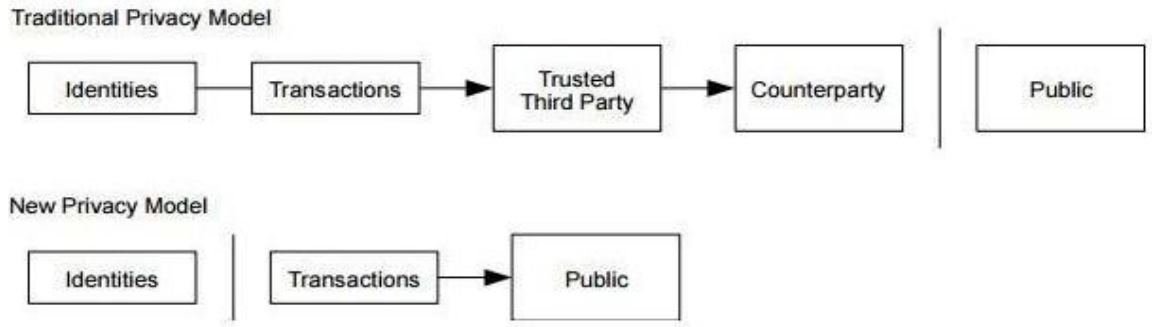
Whether it is the transacting party, banks/financial institutions acting as intermediaries or the State as the regulator, the underlying basis of any transaction is trust. In the digital world, this trust is determined by proving identity (authentication) and permissions (authorisation).[22]

Under the Blockchain technology, every individual has one private and one-public cryptographic key akin to a University's IP address comprising of a public and private IP. The private IP is visible to the university's users and the public IP is given to the network which is visible to other users. Similarly, one sign cryptocurrencies he/she send to others using hi/her private key to their public key and he/she receive cryptocurrencies that others send to his/her address through public key.[23] Together, two keys constitute a digital signature and the information sent/received forms part of a block.

When an individual authorises a transaction by using a private key in their possession and once the block chain confirms the same, it becomes a part of the public record (in case of a fully public blockchain) and everyone (all participants of the blockchain) can see what value is being transacted.[24]

However, privacy is still maintained by keeping the transactor's identity anonymous, i.e. the participants can see that an amount is being transacted but without information linking the transaction to anyone.[25] The privacy model can be best explained by the following graphic: [26]

Distinction between Traditional and Blockchain Privacy Model



Source: Retrieved from, https://bitcoin.org/bitcoin.pdf (last accessed on 09.05.18)

Blockchain is also claimed to be incorruptible, irrefutable and permanent record of transactions. It exhibits an edge over traditional mediums of exchange by introducing unprecedented security benefits. If one were to hack through a particular block of a Blockchain, a hacker would not only need to hack into that specific block, but all of the proceeding blocks going back the entire history of that Blockchain.[27] And they would need to do it on every ledger in the network, which could be millions, simultaneously.[28]

Thus, blockchain stores information in such way that it makes it virtually impossible for any change in the Blockchain, such as adding, removing or altering data, to go undetected by other users of the blockchain. For instance, in a bitcoin blockchain, any change needs to be validated

by 51 percent of all the users in the network through a consensus mechanism, which is unlikely to happen as they do not have an incentive to work on the 'old' blocks in the chain.[29]

State of Blockchain in the Public Sector

The governments at a global level are increasingly experimenting with blockchain use cases by running pilots and trials in various sectors to improve public service provisions and procurements. Some of the use cases have been discussed below:

a. Government Records

The volume of confidential information processed by any government makes it the perfect subject matter of blockchain technology. Globally, governments are experimenting in using the technology for maintaining public records pertaining to healthcare, voting, taxes, military *et al*.

Blockchain has been effectively operational in electronically managing health records of Estonian citizens. As a response to 2007 cyber-attacks, the Estonia became the first country to use Blockchain on a national level by deploying the Keyless Signature Infrastructure, a Blockchain technology developed to safeguard the citizens' data stored in government repositories.[30] It enables officials to detect and prevent any unauthorised tampering and manipulation of records by hackers or even system administrators and the government.

b. Voting

The security and immutability offered by Blockchain ensures prevention of casting fraudulent votes or rigged elections by changing the votes once they have been cast. Further, it enables efficient auditing as every record entered into a blockchain receives a unique time/date stamp as well as a hash of the previous block thereby overall improving election transparency.

Amidst the increasing spectre of election rigging and voting machine hacks, the Swiss City of Zug, also known as the 'Crypto Valley' has unveiled plans to launch an e-voting pilot that will tie in both polling system and residents digital identities with blockchain technology.[31]

c. Smart Contracts

Smart contracts are traditional contracts that contain the terms of the deal defined in code and trigger actions automatically through the blockchain technology when the pre-defined conditions are met such as making or missing payments. The records of these contracts on the blockchain will be irreversible and linked to each other thus enhancing trust and inter-operability. Further by being self-enforceable, they cut down the legal and administrative costs.

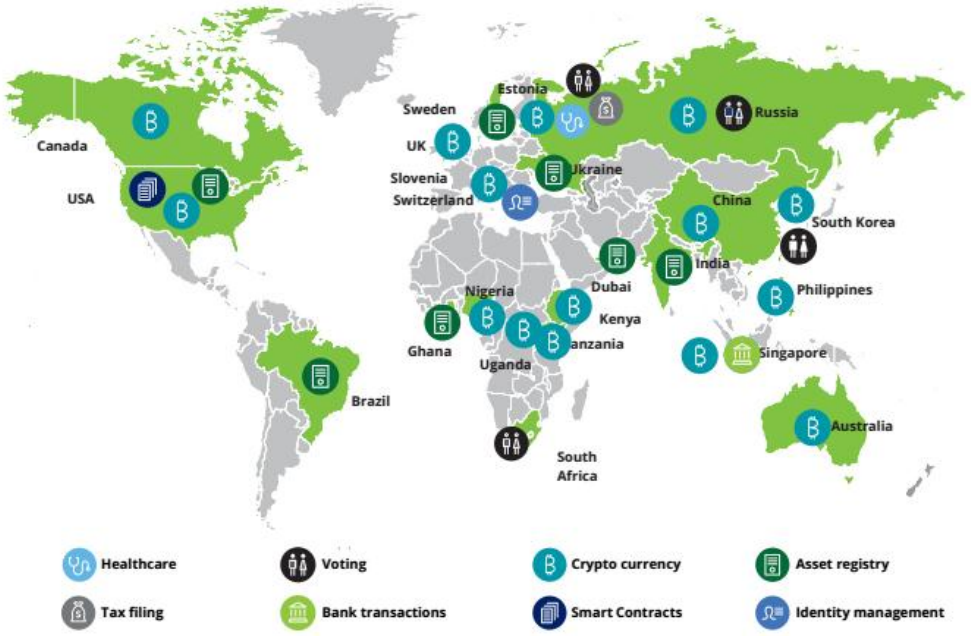
The Eastern European Country Belarus recently issued a decree to legalise smart contracts thus becoming the first jurisdiction to ensure a pro-active block chain framework for businesses.[32]

d. Asset Registry

The process of owning and transferring assets is marred by long paper trails, high propensity of fraud and interactions with multiple parties. Using blockchain technology to maintain asset registers can significantly address these drawbacks and provide for transparency across the system as well as an efficient mechanism for storing and transferring data.

The best use case is Sweden where the government is piloting a blockchain database to simplify real estate transactions.[33] Ghana and Kenya in Africa, Georgia in US and Dubai are exploring blockchain for land registration and property transactions.[34]

Indicative List of Blockchain Experiments in the Public Sector



Source: Retrieved from, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf *(last accessed on June 09, 2018)*

The Case of India

The nascent technology is gradually gaining momentum in India with experiments for integrating blockchain based solutions in governance. In his budget speech, Finance Minister Arun Jaitley announced that the government "will explore blockchain, to add muscle to the digital economy".[35] This will also be in line with the Digital India campaign launched by the government in 2015, which focussed on digital empowerment through building a digital infrastructure. To this end, the following use cases may be highlighted:

a. Bankchain[36]

Initiated by the State Bank of India, Bankchain is a blockchain comprising of 27 banks from India and the Middle East. It is aimed at exploring, building and implementing blockchain soutions in India's banking ecosystem. This consortium has been formed in collaboration with Primechain Technologies, a Pune based startup. Aside from the State Bank of India, Bankchain enjoys participation from the ICICI Bank, DCB Bank, UAE Exchange, Kotak Mahindra Bank, Federal Bank, DCB Bank, and the Deutsche Bank.

b. Indiachain[37]

Created and developed by *NITI Aayog*, Indiachain is a blochain platform for private as well as government organisations to facilitate blockchain-powered applications for indian masses. It seeks to deploy it in key areas such as health, education and agriculture. It is currently being

piloted in the education sector to address the issue of fake certification. For the same, IIT Bombay and Delhi University have been chosen for trials. India aims to successfully deploy the technology in issuing educational certificates for batches graduating from Universities in 2019.

c. Telecom Regulatory Authority of India (TRAI)[38]

In order to safeguard the privacy of telecom users, TRAI is considering the use of blockchain technology to deal with fraudulent calls to users. India is the first country to use blockchain to check pesky calls. Around 230 million subscribers have registered on the Do-Not-Disturb registry; however they continue to receive spam calls as spammers use the 10-digit mobile number and not the special numbering series allotted for telemarketing. As per the TRAI Chairman R S Sharma, 'Blockchain will ensure two things — non- repudiation and confidentiality. Only those authorised will be able to access details of a subscriber and only when they need to deliver service'.

d. Andhra Pradesh[39]

Andhra Pradesh has become the first State to launch pilot blockchain technology in two departments – land records and transport. In the former, the technology is used to prevent tampering of land records that have been digitised and placed online. In the latter, the government is using the technology to streamline titles of the vehicles. Eventually the government plans to deploy the technology across all sectors in its administration.

***e.* Maharashtra**[40]

The Maharashtra government is preparing to launch pilot projects in blockchain technology in collaboration with startups. The projects would be in the areas of financial inclusion, land records, supply-chain financing, insurance and motor vehicles registration. Following suit, Telangana, Karnataka, and Gujarat are also planning pilots and holding discussions with startups to explore the blockchain space.

f. Startups:[41]

Black Armour, a Mumbai based start-up is working towards using the technology to counter growing cyber-security challengers. Sofocle Technologies, a Noida-based startup is using blockchain-based solutions for supply chain financing, supply chain management and autonomous claim processing. KrypC, a Bengaluru based platform has developed KrypCore, a middleware platform for enterprises to create custom-built blockchain solutions without much coding effort.

Conclusion

While Blockchain may be widely popular for its use with Bitcoins, it is increasingly paving its way in other sectors too, such as insurance, finance, voting records, education, healthcare, asset registry etc. Companies like UBS, Microsoft, IBM and PwC are racing to adapt it while Silicon Valley venture capitalists are also queuing up to back it. The unique features of blockchain such as consensus, trust, immutability and provenance give limitless possibilities of its use cases. Thus, Blockchain technology, though still in its infancy, carries the promise to be the next big thing after the Internet, with its applications as wide as one's imagination. However, with its social, political and economic implications still unknown, the technology must be welcomed with caution.

Annexure-1

KEY TERMS		
S. No.	**Term**	**Definition**
1.	Block	A message sent by a participant in a blockchain system that has been authenticated and verified by that system and consensus reached on it, and which has then been added (as a block) to the previous block in the chain of blocks. Blocks typically record transactions or the change in status of something.
2.	Blockchain	A distributed ledger taking the form of an electronic database that is replicated on numerous nodes spread across an organisation, a country, multiple countries, or the entire world. Records in a blockchain are stored sequentially in time in the form of blocks. Each hash for a block depends on the block header for that block. The block header for that block contains a reference to the previous block in the chain. Accordingly there is a continuous chain back in time. In order to change one block in the chain it would be necessary to change every block that came after it.
3.	Consensus Protocol	A computer protocol in the form of an algorithm constituting a set of rules for how each participant in a blockchain should process messages (say, a transaction of some sort) and how those participants should accept the processing done by other participants. The purpose of a consensus protocol is to achieve consensus between participants as to what a blockchain should contain at a given time (including by the addition of new blocks). Terms used to describe consensus protocols in the context of blockchain technologies include "proof of work" or "proof of stake".
4.	Distributed Ledger	A collection of data (making up a database), an identical copy of which is held on numerous computers across an organisation, a country, multiple countries, or the entire world. A blockchain is a form of distributed ledger, but not all distributed ledgers are blockchains.
5.	Hash/Hashing	The process by which a grouping of digital data is converted into a single number, called a hash. The number is unique (effectively a "digital fingerprint" of the source data) and the source data cannot be reverse engineered and recovered from it.
6.	Node	A single computer involved in processing a message in order to reach consensus. Nodes are connected to each other via the Internet.
7.	Off-chain transaction	A transaction occurring outside a blockchain.

KEY TERMS		
S. No.	**Term**	**Definition**
8.	Peer-to-peer	Where participants to a network send information to one another without using an intermediary or central point.
9.	Permissioned Blockchain	A blockchain is permissioned where its participants are pre-selected or subject to gated entry on satisfaction of certain requirements or on approval by an administrator of the blockchain. A permissioned blockchain may use a consensus protocol for determining what the current state of a blockchain should be, or it may use an administrator or sub-group of participants to do so.
10.	Permissionless Blockchain	A blockchain is permissionless when anyone is free to submit messages for processing and/or be involved in the process of reaching consensus. While a permissionless blockchain will typically use a consensus protocol to determine what the current state of the blockchain should be, it could equally use some other process (such as using an administrator or sub-group of participants) to do so.
11.	Private Key	An instance of code, privately held, and paired with a public key to initiate algorithms for text encryption. A private key is created as part of public key cryptography during asymmetric key encryption.
12.	Public Key	An instance of code, available to anyone, paired with a private key to decrypt text as part of public key cryptography during asymmetric key encryption.
13.	Smart Contract	Smart contracts are made from software coding and have the ability to self-perform autonomously. Depending on a range of factors, they may sometimes amount to binding contracts in the legal sense or otherwise affect legal relations between parties. Smart contracts that are linked to blockchains could move value or information across blockchains.
14.	Time Stamp	A number representing a point in time at which something was created or done.

Source: Reproduced from: http://www.nortonrosefulbright.com/files/unlocking-the-blockchain-chapter-1-141574.pdf (last accessed on 09.05.18)

Endnotes

1 http://www.eco-business.com/opinion/blockchain-and-sustainability-should-you-believe-the-hype/ (last accessed on May 09, 2018)
2 The paper titled Bitcoin: A Peer to Peer Electronic Cash System was published pseudonymously by Satoshi Nakatomo. The actual author(s) remain a mystery.
3 http://www2.caict.ac.cn/zscp/qqzkgz/qqzkgz_zdzsq/201708/P020170831493337899927.pdf (last accessed on May 09, 2018)
4 Refer to Annexure A for definitions of key terms used in the paper.
9 http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf (last accessed on May 09, 2018)
10 https://www.ibm.com/blogs/Blockchain/2017/05/the-difference-between-public-and-private-Blockchain/ (last accessed on May 09, 2018)
11 Ibid.
12 https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains/ (last accessed on May 09, 2018)
13 https://coinsutra.com/private-Blockchain-public-Blockchain/ (last accessed on May 09, 2018)
14 Supra Note 4.
15 https://cointelegraph.com/news/car-giants-bmw-gm-among-30-members-of-new-mobi-blockchain-group (last accessed on May 09, 2018)
16 https://medium.com/@nabeelxy/how-does-blockchain-work-5e8b3328338e (last accessed on May 09, 2018)
17 https://medium.com/Blockchain-review/how-does-the-Blockchain-work-for-dummies-explained-simply-9f94d386e093 (last accessed on May 09, 2018)
18 https://www.linkedin.com/pulse/what-Blockchain-why-so-important-mark-van-rijmenam (last accessed on May 09, 2018)
19 The tragedy of the commons is an economic problem in which every individual tries to reap the greatest benefit from a given resource. Retrieved from: https://www.investopedia.com/terms/t/tragedy-of-the-commons.asp (last accessed on June 26, 2018)
20 http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf (last accessed on May 09, 2018)
21 *Ibid*
22 https://www.coindesk.com/information/what-is-Blockchain-technology/ (last accessed on May 09, 2018)
23 https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76 (last accessed on May 09, 2018)
24 https://bitcoin.org/bitcoin.pdf (last accessed on May 09, 2018)
25 *Ibid*
26 https://www.bbntimes.com/en/technology/bitcoin-what-s-in-the-whitepaper (last accessed on May 09, 2018)
27 http://www.ted.com/talks/don_tapscott_how_the_Blockchain_is_changing_money_and_business/transcript?language=en(last accessed on May 09, 2018)
28 *Ibid*
29 https://www.linkedin.com/pulse/what-Blockchain-why-so-important-mark-van-rijmenam (last accessed on May 09, 2018)
30 https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/ (last accessed on June 26, 2018)
31 https://www.coindesk.com/swiss-city-plans-to-vote-on-blockchain-using-ethereum-digital-id/ (last accessed on June 26, 2018)
32 https://blokt.com/news/belarus-issues-decree-to-regulate-and-legalize-blockchains-and-smart-contracts (last accessed on June 26, 2018)
33 https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/ (last accessed on June 26, 2018)
34 https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf (last accessed on June 26, 2018)
35 https://www.livemint.com/Technology/UZIex6fPPyAqVuTHqpzZiN/Transforming-India-through-blockchain.html (last accessed on June 26, 2018)
36 https://www.livemint.com/Industry/plB1lU0booCDVWyIkd8rOM/Banks-link-up-on-BankChain-to-exploit-blockchain-solutions.html (last accessed on June 26, 2018)
37 https://economictimes.indiatimes.com/news/economy/policy/niti-aayog-eyes-use-of-blockchain-technology/articleshow/62360134.cms (last accessed on June 26, 2018)
38 https://www.business-standard.com/article/companies/trai-s-weapon-to-check-spam-communications-blockchain-technology-118052900493_1.html (last accessed on June 26, 2018)
39 https://www.firstpost.com/tech/news-analysis/andhra-pradesh-to-become-first-state-to-deploy-blockchain-technology-across-the-administration-4125897.html (last accessed on June 26, 2018)
40 https://economictimes.indiatimes.com/tech/internet/maharashtra-plans-a-pilot-to-try-out-blockchain-technology/articleshow/62896305.cms (last accessed on June 26, 2018)
41 https://factordaily.com/blockchain-india-market-map/ (last accessed on June 26, 2018)

This Briefing Paper is written by **Swasti Gupta**, Research Associate, CUTS International