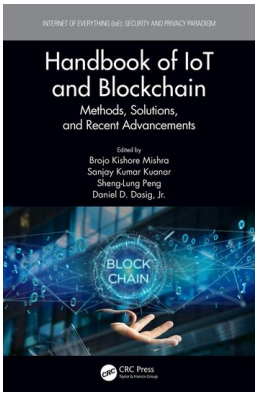
This article was downloaded by: *10.2.97.136*
On: 03 Jun 2023
Access details: *subscription number*
Publisher: *CRC Press*
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: 5 Howick Place, London SW1P 1WG, UK



Handbook of IoT and Blockchain
Methods, Solutions, and Recent Advancements

Brojo Kishore Mishra, Sanjay Kumar Kuanar, Sheng-Lung Peng, Daniel D. Dasig

Putting Blockchain into Practice

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780367854744-4
Preet Deep Singh Invest India
Published online on: 26 Nov 2020

How to cite :- Preet Deep Singh Invest India. 26 Nov 2020, *Putting Blockchain into Practice from:* Handbook of IoT and Blockchain, Methods, Solutions, and Recent Advancements CRC Press
Accessed on: 03 Jun 2023
https://test.routledgehandbooks.com/doi/10.1201/9780367854744-4

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://test.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

4 Putting Blockchain into Practice

Preet Deep Singh
Invest India

CONTENTS

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

4.1 WHAT ARE WE TRYING TO SOLVE?

Blockchain is a distributed immutable ledger that is encrypted. It is immutable for two reasons: time stamp and the encryption of preceding content. This looks simple enough. On face value, this does not solve much. Google sheets can be tweaked to become an immutable ledger with open access. We only need to find a way to introduce one-way encryption so that only the owner of the original node knows the verification.

It is surprising how hard it is to find all these in one system. Decentralization has been made possible in the past decade due to better internet penetration. Earlier, it would not be accessed in real time. Encryption has become very important in the past few decades and privacy is being equated with a fundamental right. People would not want someone to know their health records, their expenses, their purchases and so on. Some western jurisdictions have taken a very strong stance toward privacy and penalized corporates for their lapse.

Cambridge Analytica was a famous scandal highlighted in the light of the US Elections in 2016 where data from Facebook and other sources was used to target advertising in a way that it is said to have affected the outcome of the elections.

Opportunity flows from needs. Privacy is a need and cryptography is a solution. To recall, cryptography is one-way encryption. This means that all areas where privacy is required are places where blockchain has a natural application. Similarly, any place where ledgers are involved would have an application of blockchain. These cases might or might not require encryption. Immutability provides trust to any transaction. A buyer does not have to trust the seller (and with encryption, the buyer does not even need to know the seller). Transparency is needed wherever there is money involved and when the rest of the process is not in the hands of the initiator.

From this we deduce that health, finance, real-estate and governance can unlock value through implementation of blockchain.

Blockchain is at the back end in any process and no one gets (or needs) to see it. To understand this better, turn to WhatsApp. When you send a message to a new person you get a message saying that all messages are encrypted. This does not mean that the person at the other end cannot understand your message. It means that during transmission it is encrypted. Communication between the receiver and sender is not different, it is only the journey through the medium that is encrypted. Similarly, in the case of blockchain, the components and user interface are not affected by this. Just the log of all transactions is maintained on the blockchain and one can be assured of privacy.

4.2 SOME USEFUL DISTINCTIONS

4.2.1 Difference between Blockchain and Cryptocurrency

One is to put things in an immutable way, the other is to have that as currency. Cryptocurrency, as we know it, is currency that is based on the blockchain.

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

These can be understood as concentric circles where cryptocurrency is a token based on blockchain.

4.2.2 Public Versus Private

A public blockchain is one in which anyone can participate in any capacity whereas in a private blockchain the owner of the blockchain defines who all can participate and in which capacity. This means private blockchains are 'permissioned' blockchains where only participants selected by the owner of the blockchain can verify the information.

Since public blockchains involve anonymity, most of the blockchain solutions that are being developed for internal use by corporates would be private blockchains. Solutions for governance would have a combination of both where some data is available to the public and some other data is accessible based on permissions.

4.3 POSSIBLE APPLICATIONS

4.3.1 Finance

Since blockchain shot to fame with the bull run of bitcoin, the first application of blockchain is that of payments.

4.3.1.1 Know Your Customer

According to the Report of Steering Committee on Fintech[1] putting Know Your Customer (KYC) and Anti-Money Laundering (AML) systems on blockchain would reduce costs and effort by banks to comply with these requirements.

Similarly bill discounting could be made a lot easier. If a manufacturer has a work order, they could put it on the platform and a bank could verify the work order and discount the bill, providing finance to the manufacturer. In case of default the record of the buyer would reflect this and would be for all to verify. These records would also allow people to have a credit history, which is valuable for lending institutes.

4.3.1.2 Cross-Border Transfer

If you want to transfer money to a relative in another country, the payment is routed through multiple banks and intermediaries that receive, collate, net-off and transfer the money. This leads to a long time and consequently high cost in such a transfer. Application of blockchain in these cases would lead to intra-day and inter-bank liquidity. Use of digital tokens would further expedite the payment process but this assumes cryptocurrency (and not just blockchain). Some banks have worked with Ripple to explore inter-bank-cross-border transactions. Ripple is a cryptocurrency that reduces settlement times to less than a few minutes from a couple of days.

4.3.1.3 Securities Transactions

Stock market trading is famous for T+2 settlement and T+0 settlement. T+2 means it takes securities two days after the day of trade to reach the account of the buyer. Similar T+0 means the securities are transferred to the account of the buyer on the

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

same date. T+0 is available mostly in cases where the buyer has a bank account with the intermediary. This way the monetary transaction and the reverse securities transaction are done by the same intermediary for the same person. This cuts down on the KYC time. Application of blockchain would radically decrease settlement time for securities.

4.3.1.4 International Trade

Payments in international trade are the most important because of lack of trust between traders. Banks through 'Letters of Credit' (LC) bridge this gap to an extent. The Punjab National Bank Scam[2] involving Nirav Modi highlighted the lack of reliability of these LCs. Blockchain is a secure and fast way of ensuring that the issuing bank and the honoring bank would know about the intent and actions of relevant members.

4.3.2 Smart Contracts

A smart contract is a way by which conditions are fed to a machine and money is blocked therein. When the coded event occurs, payment is automatically transferred. This is similar to what PayPal was for e-commerce. Since all this is on a blockchain, there is little doubt about the payment. An external and independent source confirms the occurrence of the event. This source is called Oracle. A service that tracks flights is an Oracle in case of flight insurance. Similarly, the Met[3] declares certain districts as flood affected or drought affected. In case of crop insurance this could be used to trigger compensatory payments by the government.

In case of sports betting, the payment risk is assumed by the broker. If someone were to use ESPN or another sports application as an Oracle, then all wagers could be coded as smart contracts and counter-party risk would be assayed.

The scope for blockchain implementation in this is huge. Contract-related litigation is a huge component of Ease of Doing Business in any jurisdiction. Contracts have two sides, performance and payment. If either or both of those can be secured then the other can be tamed. In case of smart contracts, the payment is blocked and the performance is evidenced by an Oracle. This would lead to fewer disputes causing more and better trade.

Litigation, non-execution, non-payment. If we guarantee one side then the other would be solved automatically.

4.3.3 Property

Property Records are the most precious possession of most citizens. Any error in these could lead to revocation of property rights, problems in insurance claims and at time of sale/hypothecation. There is only one ownership record for all properties, and that is with the government. The process of change in ownership of property through sale/purchase/mortgage and the process of change in records are each carried out in different offices and come under different departments in certain cases. While property sale/purchase is a revenue item, that of land ownership is a record item. This divorce further adds to incorrect and incomplete updating of records.

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

Any error or malfeasance on part of someone with access to ownership records can lead to a lot of monetary loss and frustration. It is not easily possible to trace these changes to correct these. Title suits can take years to get resolved and in the interim period the property is useless.

If the two processes could be linked in a secure and verifiable way, it would solve a lot of problems. While some states have tried to link land registry through digitization and making the records open, blockchain can add a layer of security for land owners.

4.3.4 Healthcare

Having and maintaining medical records is beneficial for patients. They help doctors diagnose things better and prescribe a smoother medical route. It would lead to fewer experiments (by knowing what the patient has already gone through). Tracking of blood pressure and heart rate in our phones can provide a snapshot of the patient's wellbeing to a trained doctor. Family history would allow a doctor to target tests better and to monitor progress.

Accumulation of these benefits is prevented by privacy concerns associated with Electronic Medical Records. Health data is used by companies for designing solutions and to study the impact of interventions vis-à-vis a control group.

Data can be used for marketing new drugs to people which is at the boundary of ethically accepted practices. This data can also be used to malign someone or to prevent them from taking up public office. Because of all these use cases and concerns regarding medical data its cost on the black market is very high. Anecdotal evidence[4] suggests that medical data is thousands of times costlier than credit card data. This reflects a clear gap in the market. If there were a secure way for people to share anonymized data in exchange for money or credit (that can be used on the platform, in the form of tokens) it could be a win-win situation.

De-identification of data is a key component. Blockchain would ensure anonymity and control. The patient can decide who can view what component of the report and whether the updated content would be accessible. Cryptocurrency can ensure that people who consent get paid for sharing it.

4.3.5 Insurance

Insurance is one industry that requires a lot of documentation and verification. This is done multiple times. Insurance companies go to great lengths to ensure that they are paying the right person with the right set of documents for a covered event that happened during the insured period. All this verification takes time and effort. Efforts duplicated at different levels to ensure there is no wrong-doing on the part of the insured, inspector, processing staff and others.

Car insurance typically involves the following steps:

- Insurance cover
- Event which in this case is an accident
- Claim
- Claim verification

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

- Claim report
- Damage report
- Internal processing
- Bill submission by mechanic
- Verification
- Payment

For each claim, the company wants to assess

- Whether the same car was insured
- Whether the driver had a valid driver's license
- Whether the documents of the car are in order
- Whether a police report, if needed, had been filed
- Whether this damage existed before the insurance period
- Whether this damage existed after the insurance period
- Whether an independent party has seen the claim[5]
- Whether the correct claim has been filed by the mechanic
- Whether the part that had to be repaired was replaced or repaired
- Whether the prices of the parts are as per notified prices
- Whether the bills are for the right car
- Whether the dates on the bills and those on the claim match

Assessing all these basic things requires matching and verifying documents. This is subject to human error and malicious intent in some cases, to counter which it happens at multiple levels. While these checks seem simple, they are not so. Also, the number of claims processed by an insurance company is too huge for it to be done efficiently. There are anecdotes that a public sector general insurance company took over three days to verify that the vehicle for which a claim was made was in fact covered by the company.

In case this data were available in a digitized format, verification could be coded and conducted effortlessly. On blockchain, this could be immutable and distributed, which would ensure transparency.

4.3.6 Supply Chain

When goods are moved from the producer to the user, or when high-value items are resold, one major concern is their genuineness. Organic fruits and vegetables command a premium. The resale value of a Rolex is very high. Wine from certain vineyards is valued more. How can the end-user be assured of the origin of these products? Blockchain is being considered as a major solution.

If at each stage of processing or change in ownership through agents and transporters, the data is fed on to a blockchain, the end-user can simply scan the product and verify the origins. This would require the producer to enter all relevant details of the product on the blockchain and affix a code or engrave a microcode on the product that can be scanned and the information would be made public. This makes blockchain a good application wherever counterfeit goods are a problem. This

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

extends to pharmaceuticals as well as durables. Companies such as Walmart and Pfizer have conducted successful pilots with this technology.[6]

4.3.7 Governance

Government is the biggest spending entity in the country. Most of it is mired in processes. Tracking that money is a headache for most government departments themselves. The subsidies and grants disbursed by the Central Government pass through multiple hands before reaching the beneficiary. Blockchain can enable tracking of government funds and it is open to audit at all times by anyone who may wish to see it. Any claims made by beneficiaries can be quickly resolved by verifying them on the blockchain. Transparency and immutability would be very useful in ensuring that the money reaches the right people.

4.4 GOVERNMENT'S TAKE

The government is yet to formulate a concrete policy on the issue. There have been two reports that have examined blockchain and cryptocurrency. There is consensus on the use of blockchain and exploring its application in governance. In the 2018 Budget speech, the then Finance Minister Shri Arun Jaitely clarified the stand of the government in Parliament.[7] He said a distributed ledger system or the blockchain technology allows organization of any chain of records or transactions, without the need of intermediaries. The government will explore use of blockchain technology proactively for ushering in a digital economy.

The contentious point was regarding cryptocurrency. The Government constituted an Inter-Ministerial Committee (IMC)[8] in November 2017 under the Chairmanship of Secretary, Economic Affairs comprising Secretary, Ministry of Electronics and Information Technology, chairman of Securities Exchange Board of India and other members to study the issues related to virtual currencies and propose specific action to be taken in this matter.

4.4.1 Summary of IMC Report

While some countries have outrightly banned cryptocurrencies and some others have used them for barter transactions and even as a means of payment, no country has yet considered cryptocurrencies as a legal tender.

The Inter-Ministerial Committee (IMC) set up by the Indian Government to study the issues related to virtual currencies and propose specific actions,
recently recommended that all private crypto currencies should be banned in India except the ones issued by the Government.

While the Committee suggests that the Government keep an open mind on digital official currency and has highlighted the positive aspects of Distributed Ledger Technology (DLT) and its uses in banks and financial firms, it has proposed banning of all private cryptocurrencies given the risks associated with them.

The disadvantages of virtual cryptocurrencies have been further explained below with sources and rationale.

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

- Public blockchain needs decentralized verification such as in the case of bitcoin. People who verify the transaction and get some bitcoins are called miners. A complex mathematical problem is posed to verifiers and solving these problems takes up a lot of energy. Decentralization may help in keeping this process less cumbersome.
- Low scalability: To be used as a means of payment, the number of transactions that can be processed has to be much higher. At its peak, it would take bitcoin more than a day to verify a transaction.
- High cost: The cost of verifying transactions through the Proof of Work protocol is very high. The report says that 19 US households could be powered for a day by the electricity it takes to mine one bitcoin. If such currency mining is not prohibited in India, it would be catastrophic. Developed nations such as Canada have had to buy power in the open market. India is already power starved.
- Irreversibility: All transactions on blockchain are irreversible. While this gives it credibility, it penalizes mistakes. Anyone who has worked at a bank would tell you that mistakes are common even while transferring money.
- Security: Wallets and even exchanges have been prone to cyber-attacks thereby causing a security concern.
- Password: If one forgets the Private Key, there is no recourse. Currently, we have the provision of verifying the identity of the person and regenerating a PIN or an OTP. No central authority exists in case of cryptocurrencies.
- Monetary policy: cannot be enforced by central banks. This can cause unchecked inflation.
- Cross-border control over currency: cannot be exercised as there is no central clearing house.
- Anonymity: in transactions is causing cryptocurrencies to be used for criminal activities; from financing narcotics, as in the case of Silk Road, to terrorism.

Given the disadvantages, IMC proposes the enactment of a law to prohibit trading and mining cryptocurrencies and a fine of up to Rs 25 Cr and imprisonment of as much as ten years for anyone dealing in them. However, it does recommend official digital currency with the status of a legal tender and appropriately regulated by the Reserve Bank of India.

4.4.2 Report of the Steering Committee on FinTech Related Issues

The report of the Steering Committee on FinTech Related Issues, also within the Department of Economic Affairs, Ministry of Finance has taken a much softer view on the issue. It has encouraged the use of blockchain and has noted global interest in cryptocurrency. They acknowledge that virtual currencies through Initial Coin Offerings are revolutionizing fintech. it also talks about utility tokens and their potential to enable various industries.

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

4.5 SUCCESS STORIES

4.5.1 LaVis Wine

Counterfeit is a major problem for the wine industry. People want to be assured of what they are drinking especially when they are paying so much for each bottle. Ernst and Young (EY) has been the blockchain implementation partner for LaVis. LaVis is claimed to be one of the first to sell blockchain-certificate wine using EY Ops Chain[9]. The blockchain contains all details related to the story of the wine starting from the type and quality of the grapes, to the date of bottling and the quality of the sulfates. Each time the bottle changes hands between the producer to the wholesaler to the retailer, the status is updated.

4.5.2 TReDS Bill Discounting

TReDS or Trade Receivables Discounting System which is an RBI[10] approved platform for discounting bills for MSMEs, has started using blockchain[11]. This allows them to broadcast information across a shared network where not only is all information in the public domain, it is also sensitive as it deals with financials.

Blockchain allows them to operate while protecting privacy.

4.5.3 Travel Insurance

Axa has partnered with Fizzy to provide travel insurance on blockchain. As mentioned above, blockchain is at the back end and the insured have little or no visibility on that. The process of getting flight insurance or to get any insurance for that matter has always been easy. The problem is at the time of claims. Blockchain is solving that component. Insurance pays off in the event of that condition being met. The insured is supposed to file a claim and then that claim is processed internally by the insurer and payment is released. In case of flight insurance, the insured and the insurer check as to whether the flight was delayed by two hours or more, or cancelled altogether. The advantage in this case is that as soon as a flight is delayed by two hours, the information is relayed at the same time to the insured and the insurer. And since it is coded on Ethereum smart contracts, that information triggers payment of the sum insured without any human intervention. Even if the insurer wants, they cannot edit the contract once it is on the system. The contract address is: 0xdc3d8fc2c41781b0259175 bdc19516f7da11cba7 which can be accessed on etherscan.io and other such options for Ethereum Blockchain. Anyone can view the contract and the code.

The link to the website is https://fizzy.axa/en-gb/

Other good insurance use cases can be found at https://builtin.com/blockchain/blockchaininsurance-companies

4.5.4 Sweden Land Records

Since land record titles are susceptible to minor forgeries and clerical errors, the Swedish government has decided to experiment[12] with the use of blockchain. It is

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

called Lantmäteriet. Instead of signing papers, people could use digital signatures. Since these can be validated online, a transaction can be concluded. The system operates on a private blockchain and includes land registry and other parties that hold land records such as banks. However, even this system does not act like cryptocurrency where high-value transactions are easy. Nevertheless, just by removing paperwork and preventing forgery, Sweden would save more than $100 million.

4.6 CHALLENGES

4.6.1 Digitization

Driving licenses can be put online in a cryptic form only to check validity and if there have been any challans in the past due to traffic violation. This would allow insurers to decide premium based on the driving history of the person. The problem with this solution is that all the driver's license data is not available in one online database that is accessible and compatible with other databases.

Firstly all data would have to be digitized with a collaborative architecture. This is an exercise that has been undertaken in many developed economies and efforts for this are under way in India as well.

4.6.2 Property Records Complete

Property records on blockchain would ensure that there is no amendment to land ownership without consent (and in some cases, corresponding payment to the seller). The problem with this approach is that it is only prospective. In order to be retrospective, the land records have to be clean in the first place. In the absence of this, the legacy data cannot be digitized on to blockchain. While this may seem very simple it is not so. Even some of the best States in Government of India's Ease of Doing Business Ranking do not have even two years' worth of property records and transactions digitized[13]. Property is fraught with disputes, some in civil courts and others in criminal courts. It is mortgaged, pledged and rented. There are cases subject to Wills, Gift Deeds and Sale Deeds. This leads to too many ownership disputes. If this is not free of errors and disputes, it cannot be put on the blockchain as they would then be immutable.

4.6.3 Need for Scale

The benefits will only arise once the entire platform is on the system. We need everyone to use it. Imagine using emails only to find out that you need to take a print of each communication, respond in writing and each response will then be digitized. It would not add any value, right? Similarly blockchain will add value if all processes are present on it. Therefore the need for scale is high to unlock value.

4.6.4 Coders

The main platforms at the moment are

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

1. Hyperledger: by IBM
2. Corda R3: industry collaboration initiative with leading organizations as partners
3. Solidity: Ethereum blockchain
4. Others such as MultiChain, SmartChain and other chains: platforms to create your own blockchain

While Hyperledger and Corda require mostly Java knowledge, Solidity and other platforms require more sophisticated knowledge. There is a dearth of people who understand blockchain architecture and can implement it. Coders are in short supply for the entire industry but more so for blockchain.

4.6.5 Smart Contracts

Oracles: smart contracts require Oracles. These Oracles are assumed to be sources of truth for a contract to get executed. For smart contracts to be a reality, we would need many more Oracles. We would also need more reliable and consistent Oracles. For example, flight.com is a reliable source for flight data. However, it can get hacked. There might be an internal maintenance issue. The server might be down or it could have bugs. Since it is owned privately, one cannot rule out any interference. These issues hamper trust.

Non-repudiability of smart contracts is a welcome feature in many cases. However, in certain cases it can prove to be problematic. If someone were inebriated or under duress while they were writing a smart contract, it could have difficult consequences. The best software from the biggest companies also suffers from bugs. It is inconceivable that no smart contracts would have bugs. Further, both parties may agree to dissolve the contract, or there could be a *force majeure*. In these cases we would need an escape chute from the non-repudiable smart contract which is not possible currently.

4.7 DO IT YOURSELF

4.7.1 HyperLedger

Click and Build platforms such as Hyperledger by IBM are available free of cost for enthusiasts. The online program is free for all and leads to a decent working knowledge of the platform. The course helps you develop a small blockchain for trading cars. It does not require any coding experience. In order to build something useful for an organization, it has a Java component that needs to be understood and coded. However, this is a good place to start if you want to understand and see it in action.

Coursera and a number of other learning platforms provide free learning content hosted at www.coursera.org/lecture/blockchain-platforms/hyperledgerpart-1-87Qz4.

4.7.2 Bitcoin

Although Bitcoin and trading in any form of crypto is not recommended in India, it is possible to look at the blocks. Since it is open, you can look at all the blocks

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-

ever created. The hash of each block is available. If you click on one of these, you will see the number of transactions in each block which contains the amount of bitcoins transferred, the sender's address and the receiver's address[14]. For each address, you can also view the history of all transactions made by that address along with dates.

Each block also identifies the username of the miner (the one who successfully solved the mathematical problem before everyone else) as well. This miner would have received a reward for doing this as well. This keeps miners motivated and therefore the system has an in-built reward within it. Each block is about 1.2 Mb. The block height or the number of the block is in the 6,00,000 series. All these transactions would roughly add up to 72 Gb of data. Since all the transactions on each block are hashed, the entire chain, without the record of the transactions would occupy less than 1 Mb of space. This allows the system to be scalable.

Everything about bitcoin transactions is public. The identities of the sender and the receiver are encrypted. Each wallet (of sender and receiver) has multiple unique hashed identities. This ensures that no one can trace previous transactions to one person.

The same is true for all crypto currencies. The famous ones with higher volumes have their ledger accessible from multiple websites.

4.7.3 Ethereum Blockchain

Ethereum has been a successful blockchain in terms of diversifying beyond a currency. At time of writing it is considered to be the default platform for coding DAPPS (stands for Distributed Applications). Solidity is the platform where smart contracts can be coded on to the Ethereum blockchain. Learning Solidity has been made easy by CrytoZombies.io. This platform offers a gamified system of learning how to code for Ethereum. The course is free and has levels that one progresses through in the journey of dealing with zombies.

4.7.4 Generate a Hash

There are a number of hashing algorithms. They have varied complexity. Some have a private key that can be changed for each transaction.

If you are familiar with the statistics software called R, then you can try out *digest* package to generate hashes. You can use the following code to generate the hash for any content *hmac ("PrivateKey", "Content", algo = "sha256").*

You can change the Private Key to anything you want. The content can be whatever you want. The algorithm can be specified to any out of sha1, sha256, sha512, crc32, mda5. These would all generate a different hash of the same content but would be internally consistent.

Alternatively, you can visitwww.sha1-online.com/ to hash anything you type.

You can hash images as well. Right click any image file and click on Open With… and click Notepad or any text editor. You will see the textual representation of the image. It is this text that would be hashed. Try editing this image in Paint or any other picture editing software. You could add a small dot, that might even be imperceptible

to the naked eye. If you compare the text representation of this edited picture to that of the unedited it, you would be able to see the difference. Since the source text is different, the hash would also be different.

NOTES

1 DOA: October 10, 2019 https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech.pdf
2 https://en.wikipedia.org/wiki/Punjab National Bank Scam
3 India Meteorological Department (IMD)
4 www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-recordscan-be-worth-1000-to-hackers/#5e0e1b7250cf
5 Usually above INR 20k in most cases
6 Source www.cbinsights.com/research/what-is-blockchain-technology/
7 www.livemint.com/Money/o4bSQ6CiUfjCIWDFDyZjnJ/Cryptocurrency-notlegal-tender-in-India-but-blockchain-get.html
8 https://dea.gov.in/sites/default/files/Approved%20Press%20Release%20on%20the%20Report%20and%20Bill%20
9 www.ey.com/en gl/global-review/2018/restoring-trust-in-the-wine-industry
10 Reserve Bank of India
11 www.thehindubusinessline.com/money-and-banking/indias-first-blockchainimplementation-goes-live/article23422835.ece
12 https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-areality/
13 Rajasthan as accessed at eodb.dipp.in
14 These are encrypted.

Downloaded By: 10.2.97.136 At: 02:21 03 Jun 2023; For: 9780367854744, chapter4, 10.1201/9780367854744-