IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SYSTAMETIC APPROACH OF ENHANCING IMAGECHAIN USING BLOCK CHAIN

Dr.R. Elankavi, M.Tech Ph.D.[1] M.Sandhya[2] S Omsai[3] B Pavani[4] E Prasad[5]

[1]Associate Professor, [2345]UG Student, Department of Computer Science and Engineering.

[12345]Siddharth Institute Of Engineering & Technology, Tirupathi, Andhra Pradesh, India,

ABSTRACT

Digital images are linked together in an image chain using hash connections in a cryptographic structure. The main characteristic that sets it apart from block chains is that the images are not kept inside the blocks. Instead, the embedding procedure combines the block with the picture. The image chain is made up of normal graphic files that may be utilised in the same way as other images but also each of which has a data block that connects it to an earlier link in the chain. Apart for the photos themselves, the proposed approach doesn't call for any other files. It is portable and user-friendly due to the variety of file formats and embedding techniques it supports. The plan also offers a substantial amount of security and forgery resistance. This is accomplished by hashing the entire file with embedded data, making it impossible to change or remove the picture from the chain without the integrity being compromised. This project explains the fundamental idea of an image chain along with its components and uses. Block structure and embedding techniques are the two most crucial challenges.

Keywords: *picture watermarking, image chain, and cloud technologies*

INTRODUCTION

A ground-breaking technique used to build distributed databases is block chain. The information is recorded in a chain that expands incrementally, and once saved, it cannot be changed. A cryptographic hash function is used to link each block of data to the one before it in order to protect data integrity and prevent data manipulation (in fact, modifying even a single bit in the chain would require re computing all hashes from the altered block to the last one, which is a power-consuming task). Block chain's distribution is its key strength since it makes the database directly accessible and DDoS-resistant.

Textual data is typically stored in block chains. Nonetheless, there have been attempts to connect several data structures together. One suggestion was to add a digital image to Steemit [1], which typically just keeps texts on the block chain. The author attempted to embed base64-encoded binary image material into HTML rather than using the standard method (uploading the image to the server). Regrettably, technical difficulties prevented this effort from succeeding. The storage of healthcare data was the subject of some other projects. The authors of [2] proposed a public and a private block chain with two distinct block structures. The solution shown in [3] combines cloud infrastructure with block chain technology. The storage of transaction records and index data was significantly improved by both publications, but not the storage of the actual photographs. It is also important to explain some more block chain application concepts. [4] sought to incentivise resource sharing, do away with the need for pointless middlemen between owners and users, encourage collaborative work, and provide genetic privacy by storing genomic data in a block chain. In [5], medical data are stored in a block chain and are accessible when at least t individuals work together. The data are shared between n servers. The servers can also analyse the data using homomorphic calculations. To identify fake and inferior pharmaceuticals, the authors of [6] suggest a block chain-based system of drug distribution. Instead, they make up the chain on their own. That is accomplished by directly saving the data in a graphical file. Hence, the ledger is an embedded object rather than a separate one. In Sections 2 and 3, the concept of an image chain is explained with a use case. Part 4 of the document, which also provides information on block structure and embedding techniques, contains the system's architecture. Security concerns are covered in Section 5; the analysis is covered in Part 6. Many potential applications are shown in Section 7. Section 8 makes comparisons to alternative strategies and offers some findings. The entire material is summarised in the final part.

LITERATURE REVIEW

Block chain is the foundational technology for digital crypto currencies like Bit Coin. The block chain is a shared, distributed database that contains records of every digital event or transaction that has ever taken place. Every transaction is confirmed by the vast majority of system users. It includes every single transaction record. The most well-known cryptocurrency is Bit Coin, which serves as an example of a block chain. When a person or group of people going by the name "Satoshi Nakamoto" released a white paper in 2008 titled "Bit Coin: A Peer to Peer Electronic Cash System," the world first learned about block chain technology. Block chain technology stores transaction information in a distributed digital ledger that is uncorruptible due to network distribution. Any item of value, including cars, real estate, and other items, can be recorded as a transaction on the blockchain.

❖ Distributed ledger technology (DLT) that uses a block chain consisting of an expanding list of records,

blocks, which are safely connected by means of encryption. Each block includes transaction information, a timestamp, and a cryptographic hash of the preceding block (generally represented as a Merkle tree , where data nodes are represented by leaves).

❖ The timestamp demonstrates that the transaction data was there at the moment the block was produced. Each block links to the blocks before it, forming an effective chain (compare linked list data structure), because each block carries information about the blocks preceding it. The data in any given block cannot be changed retrospectively without also changing all following blocks, hence block chain transactions are therefore irreversible once they are recorded.

❖ A peer-to-peer (P2P) computer network typically oversees block chains for use as a public distributed ledger, whereby nodes cooperate to add and validate new transaction blocks according to a consensus algorithm protocol. Block chains may be regarded safe by design and serve as an example of a distributed computing system with high Byzantine fault tolerance even if block chain records are not unchangeable and block chain forks are conceivable.

❖ Based on earlier work by Stuart Haber, W. Scott Stornetta, and David Bayer, a person (or group of individuals) going by the name (or pseudonym) Satoshi Nakamoto constructed a block chain in 2008 to act as the public distributed 5 ledger for bitcoin cryptocurrency transactions. Bitcoin was the first digital currency to successfully solve the double-spending issue without the aid of a central server or trusted authority thanks to the implementation of the block chain within it. Several applications and publicly visible block chains that are frequently utilised by crypto currencies have been influenced by the bitcoin concept. One kind of payment rail may be the block chain.

❖ For corporate purposes, private block chains have been proposed. Others have suggested that permissioned block chains, if well built, may be more decentralised and consequently more secure in practise than permissionless ones, notwithstanding Computerworld's description of the marketing of such privatised block chains without a sufficient security architecture.

❖ The integration of blockchain technology is possible in many fields. Block chains are mostly used as a distributed ledger for digital currencies like bitcoin; however, there are a few other operational products as well. It, by the end of 2016, has developed from proof of concept. In order to assess the impact of block chain technology on organisational efficiency in their back office, various firms began testing the technology in 2016.

❖ According to estimates, $2.9 billion was invested in block chain technology in 2019, an increase of 89% from the previous year. Furthermore, the International Data Corp predicted that by 2022, corporate spending on blockchain technology will total $12.4 billion. Furthermore, The second-largest professional services network in the world, PricewaterhouseCoopers (PwC), estimates that by 2030, block chain technology will have the capacity to produce more than $3 trillion in annual economic value. Added to PwC's estimate is a 2018 study.

- With the rise in popularity of cryptocurrencies like bitcoin, Ethereum, litecoin, and others, the examination of public block chains has gained more and more significance. If a block chain is open to the public, anyone with the necessary skills can view and analyse the chain's data. For many crypto currencies, crypto exchanges, and banks, it has been difficult to comprehend and access the movement of cryptocurrency. This is due to claims that block chain-enabled crypto currencies facilitate the illegal trade in drugs, firearms, and other goods on the black market as well as money laundering. Cryptocurrency has been used for criminal purposes by various actors because to the widespread misconception that it is private and untraceable.

2.1.1 WORKING OF BLOCK CHAIN TECHNOLOGY

Bitcoin is a well-known example of a block chain application. A cryptocurrency called bitcoin is utilised for online exchanges of digital assets. In order for two parties to carry out transactions over the internet using Bitcoin, cryptographic proof is used in place of third-party trust. With the use of digital signatures, every transaction is secure. There is no central server or system that maintains the data for a block chain, as seen in Fig. 2.1 of the workings of block chain technology. The data is dispersed among millions of computers connected to the block chain worldwide. Data can be notarized in this system because it is accessible to the public and is present on every node.

2.1.2 BENEFITS OF BLOCK CHAIN TECHNOLOGY: Time-saving: Settlements do not require central Authorities authentication, which speeds up and lowers the cost of the procedure. Cost-saving: A blockchain network lowers costs in a number of different ways. No requirement for independent verification. Direct asset sharing is possible. There are fewer intermediaries. As each participant has a copy of the shared ledger, transaction efforts are kept to a minimum. Tighter security: As block chain data is shared among millions of participants, no one can tamper with it. The system is secure from fraud and online crimes.

2.1.3 INITIATION:

1. Data is obfuscated in an image using cryptography 2. The following is the encryption and decryption process. 3. Following that, data is processed using a blockchain smart contract. 4. The Remix IDE and the Metmask wallet are connected. 5. Use of smart contracts

2.2 DIGITAL IMAGES: A digital image is a representation of an actual image in the form of a collection of data that can be saved and retrieved. The image is broken into tiny sections known as pixels so that it may be converted into numbers (picture elements). The imaging equipment stores a number, or a limited group of integers, that identify a pixel's characteristics, such as its brightness (the amount of light it emits), or colour. The rows and columns of the numbers' arrangement represent the vertical and horizontal positions of the pixels in the image. Digital photographs have a number of universal traits. The first is the image's kind. For instance, a black-and-white photograph merely captures the light's intensity as it hits the pixels. Typically, a colour image has three colours: RGB (Red, Green, and Blue), but it can also have four: CMYK (Cyan, Magenta) While CMYK images are utilised in colour printers, RGB images are typically used in computer monitors and scanners. Moreover, there are non-optical images that record the strength of sound or X-rays, such as ultrasound or X-ray. Range images measure each pixel's separation from the observer. The resolution is measured in pixels per inch (ppi). An image with a greater resolution is more detailed. A printer's resolution can range from 300 ppi to more than 1440 ppi, while a computer monitor normally has a resolution of 100 ppi. Because of this, an image appears considerably more impressive in print than on a monitor. The quantity of "bits per pixel" or "colour depth" (of a colour image) is bits in the numbers that specify the hue or brightness. Additional bits allow for the recording of more hues or grayscales. A RGB image with 8 bits per colour, for instance, has a total of 24 bits per pixel ("true color"). We have a total of 16,777,216 potential colours because each bit can represent two different colour possibilities. A typical web page GIF image has 256 colours and 8 bits for all of the combined colours. However it downloads more rapidly because it is a much smaller image than a 24 bit one. Only one bit or two "colours," black and white, are included in fax images. Further information about the numbers' format is provided by the image's format. include the type of compression employed, if any. TIFF, GIF, JPEG, PNG, and Post-Script are a few of the dozens of formats that are offered that are the most common. It is a particular kind of image made up of pixels. Each pixel serves as a representation of the image and has a defined size and intensity. The pixels are organised in a neat rectangular array. The dimensions of the pixel array can be used to calculate the image size. It has x- and y-coordinates, which are finite coordinates. It comes in two varieties: raster and vector. The raster picture primarily serves as a digital image's point of reference.

2.2.1 AN IMAGECHAIN IDEA:

This paper's goal is to suggest a new technique for chaining digital image.

The fundamental presumption is that no external database should be needed for the solution. Consequently, the goal of this effort is to develop a system where photographs are linked to one another directly without the use of any additional files. The idea behind an imagechain is generally similar to that of a block chain. They both form a linear structure linked together by hash links, as seen in. But now, instead of text blocks, each link in the imagechain is an image that is connected to the element before it. 12 Fig 2.4 Comparison of the Imagechain and Block chains Hash values are used to create the linkages (fixed-length digests of arbitrary-size input). Each image has a bit of information encoded in it that may be viewed as a data block. These data blocks contain a hash of the preceding image file that connects them to one another. The block chain paradigm is somewhat reversed by imagechain, which embeds chain information into images rather than storing them in linked blocks. The embedding and extracting functions are two techniques that are utilised in imagechain architecture. Their jobs complement one another. The block is inserted into the image using the embedding function. On the other hand, the extraction function takes the data directly from the image. Both techniques are

2.2.2 IMAGECHAIN EXAMPLE:

to be made available to the public and other system parameters to all participants (like a hash function).

A clear example that demonstrates the described system in action has been developed. Simple blocks and well-known images are employed.

The hash function of choice is SHA256. We choose the first image in an imagechain, "climbing moss," to begin the chain. It has no predecessor because it is at the beginning of the chain, hence its prior hash is zero. The block containing all pertinent information is then created and embedded in the picture (more technical details of this procedure are presented in the next section). The chain is one length after this stage. The previous hash is then saved using this value in the following image. When new photos are added to the chain, the same procedure is always performed. Each of the elements has precisely one antecedent, and they are connected chronologically. Three photos are chained together to reveal the outcome. The last element's hash should be calculated, a new block should be created, and it should be embedded in the incoming picture in order to extend this imagechain. The new image would serve as a brand-new link in the chain.

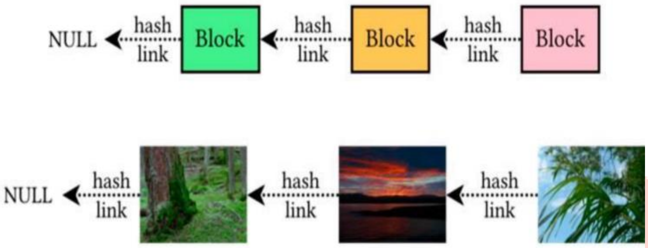


Fig 2.4 The comparision of the Blockchain and Imagechain

Fig 2.5 An example of a simple imagechain 14

2.3 DATA BLOCKS ARE CREATED:

When building the system, it is crucial to consider the imagechain architecture's block structure and embedding function. This section talks about them.

2.3.1 BLOCK STRUCTURE

A structured data item is referred to as a block. Although JSON is the most logical and popular option because each block comprises of (field, value) pairs, it is technically possible to have blocks encoded differently. A hash value is one of each block's fundamental components. It is essential to a chain link because it binds the components in a particular sequence. Depending on the application, the block structure could be more complicated and contain a number of fields. The following are the most typical fields that are used for various purposes: Index is a number that represents the order of the blocks. Every time a new link is added to the chain, it is increased by 1, and the timestamp indicates that the data was present at the specified time and date. The preceding hash is the key component of each block, and this field is typically expressed as a number of seconds from 1 January 1970 00:00:00 UTC. It is used to make sure the block's content hasn't been changed. As a result, the hash value's functions include fraud detection and prevention in addition to preserving the database's structure.

This is why any chain system must carefully consider the hash function to be used; A signature may be appended to a block when the system requires authorization or when the authorship is important. In such situations, individuals are aware of the algorithm in the open. Nonce is a value that is frequently used in crypto currencies; it has no specific meaning but can be changed to affect the block's overall hash. By placing certain constraints on the blocks, it is utilised in many public block chains to manage the difficulty of mining (for example, only hashes with a fixed number of leading zeroes are considered as valid). Finding hashes that meet additional requirements is a computationally demanding operation called mining. It serves to verify that the block inA comment, a description, etc. may be included in additional data. It solely depends on how the chain is used. This field may have a length restriction to avoid the creation of excessively big blocks. The system may implement more complex functionalities the more information that is present in the block. Nevertheless, larger blocks are not advantageous because they cause storage issues and a rapid increase in chain size. As a result, it is wise to create systems with few, purpose-built blocks. Because of the carrier's capacity, the block size in the imagechain is also significant. 15 The system architect should make sure that the block size is suitable for use with the selected algorithm and provide some details about the suggested configuration.

RECENT WORKS

The author attempted to include binary picture content that was base64-encoded in HTML. Regrettably, technical difficulties prevented this effort from succeeding. The storage of healthcare data was the subject of some other projects. The authors of [2] suggested two distinct block chains with differing block structures: public and private. The solution shown in [3] combines cloud infrastructure with block chain technology. The storage of transaction records and index data was significantly improved by both publications, but not the storage of the actual photographs. It is also important to explain some more block chain application concepts. [4] sought to incentivise resource sharing, do away with the need for pointless middlemen between owners and users, encourage collaborative work, and provide genetic privacy by storing genomic data in a block chain. In [5], medical data are stored in a block chain and are accessible when at least t individuals work together. The data are shared between n servers. The servers also have the ability to homomorphically process the data. To identify fake and inferior pharmaceuticals, the authors of [6] suggest a block chain-based system of drug distribution.

Figure Image collection with hidden imagechain (pictures with dark borders).

[7] discusses the use of blockchain in clinical trial data. It describes how the Ethereum network's smart contracts are used to handle data. The usage of Merkle trees in blockchains is a popular technique for ensuring the consistency of a group of files: all of the files' hashes are arranged into a tree, and the root of the tree is kept in the blockchain. It works well with huge data structures and is efficient. This notion by Ralph C. Merkle

3.1.1 DRAWBACKS:

At this time, digital image chains cannot embed block chains and image processing. A single file format is used for the digital image chain. The image chaining technique requires additional files and libraries. The drawbacks of the current approach are listed below.

1. The integrity of the image may be lost if it is changed or removed from the chain.

2. Image chaining does not use hashing.

3. Image chaining does not include the embedding procedure.

4. The image chain does not follow cryptographic structure

PROPOSED METHOD

This artical will suggest a fresh approach to linking digital photos. The fundamental presumption is that no external database should be needed for the solution. Consequently, the purpose of this effort is to develop a system in which photographs are linked to 3.1.1 DRAWBACKS: At the moment, block chains and image processing cannot be embedded in digital image chains. The digital image chain uses a single file format. Further files and libraries are needed for the picture chaining technique. Here are a few disadvantages of the current strategy.

1. If it is altered or removed from the chain, the integrity of the image can be compromised.

2. Chaining images does not employ hashing.

3. The embedding method is not a part of image chaining.

4. The image chain is not structured cryptographically.

BENIFITS

In this paper, a novel method for connecting digital photos will be proposed. The solution shouldn't require an external database, according to the essential premise. Hence, this project's goal is to create.

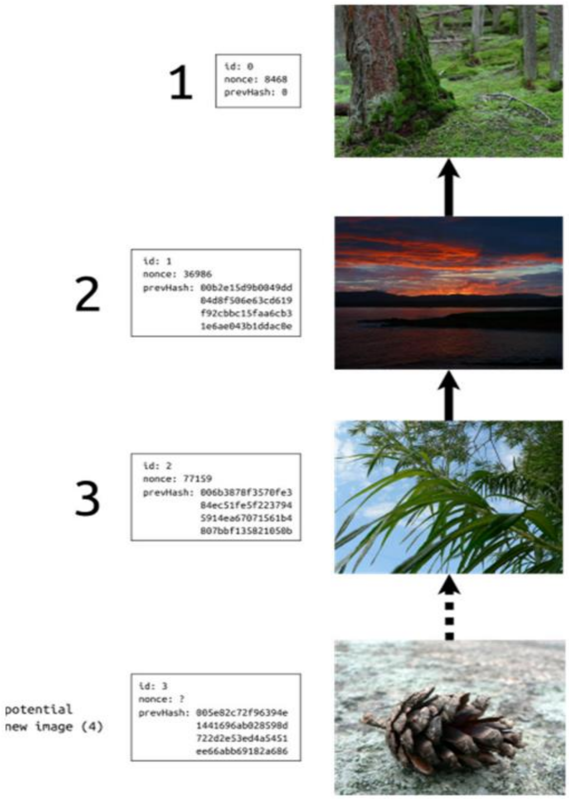


Fig: Archtecture of Image Chain

IMAGE CHAIN METHODS AND ALGORITHMS

This section of digital picture chaining. The fundamental presumption is that no external database should be needed for the solution. Consequently, the goal of this effort is to develop a system where photographs are linked to one another directly without the use of any additional files. The idea behind an image chain is generally similar to that of a block chain. They both come together to form a linear structure that is joined by hash connections, as seen in Figure 1. The image chain, however, no longer consists of text blocks; rather, each member in the chain is an image that is connected to the one before it.

DATA BLOCKS ARE CREATED

The image chain architecture's block structure and embedding function are crucial components that should be considered when creating the system. These topics are covered in this module. Although JSON is the most logical and popular option because each block comprises of (field, value) pairs, it is technically possible to have blocks encoded differently. A hash value is one of each block's fundamental components. It is essential to a chain link because it binds the components in a particular sequence. Depending on the application, the block structure could be more complicated and contain a number of fields.

Method of embedding

The embedding and extraction techniques are necessary for the imagechain to operate correctly. The first is used to encode the block into the image, while the second is used to retrieve it. These are complementary functions. Because the generated image is hashed and the digest is included in a new block that is later placed in another file, the embedding technique is crucial to the whole system.

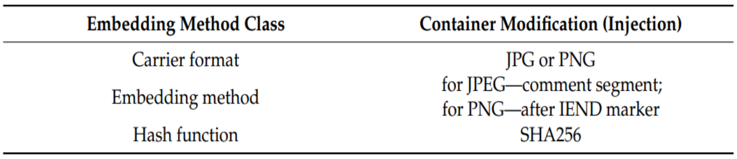
ALGORITHM MD5.

A string of any length can be hashed using the MD5 (Message Digest Method 5) cryptographic hash method to produce a 128-bit digest. The digests are shown as 32-bit hexadecimal values. This technique was created in 1991 by Ronald Rivest to enable the verification of digital signatures. In the end, it was included into a number of additional frameworks to strengthen security indices.

ANOLYSIS OF RESULTS

The primary characteristic of imagechain, which sets it apart from alternative methods, is the direct linking of digital images. There isn't a distinct chain that holds solely hyperlinks or metadata. Instead, the image itself expands the chain by adding a new link. It is accomplished by integrating a data block into the image. The verification procedure or adding a new image to the chain, on the other hand, both require the use of a programme. The proposed system's potential for use in conspiracies is another drawback. A select group of privileged individuals may be aware of the covert chaining of some photographs added to a sizable database. The right embedding procedure must be used in this circumstance; its detection should be as challenging as possible. A hidden imagechain that displays some relationships between linked photos that are then Although hidden messages can also be inserted into text transactions, their storage capacity is lower than that of images, which can hold far more data. Lastly, because the block structure can vary depending on the application and security needs, the proposed method is adaptable and suitable for usage in a variety of contexts. Also, many picture formats can be used, even within the same chain. Although the system architect determines the final configuration, it is wise to begin with the recommended first setup (Table 1).

Table 1. Recommended setup for general use.



Embedding Method Class	Container Modification (Injection)
Carrier format	JPG or PNG

Embedding method	for JPEG—comment segment;
	for PNG—after IEND marker

Hash function	SHA256

CONCLUSION AND FUTURE SCOPE

This article introduces imagechain, a new technique for connecting digital images to create a linear structure. The primary benefit of the suggested technique is that data blocks are directly stored in images, eliminating the need for separated ledger. A hash function makes it simple to find instances of data tampering, whether deliberate or unintentional. As a result, imagechain is anti-fraud in a way that the blockchain is not. Every image in the chain can also be used independently as a standard file. Even so, it is still a link in the chain and may be verified as real based on all earlier images. Public and private chains are two of the many types of chains that Imagechain offers. Also, it allows opportunity for a variety of solutions to meet different requirements. It could be in a basic or sophisticated form, with extra functions tailored to demands. As a result, we draw the conclusion that image chain is a versatile solution appropriate for a range of applications. Future research may examine alternative image chain-based systems as well as advancements to the framework itself. New data structures that link photos in a more complicated manner rather than sequentially are another potential option.

REFERENCES:

1. Bernstein, D.J.; Lange, T. eBACS: ECRYPT Benchmarking of Cryptographic Systems. 2019. Available online: https://bench.cr.yp. to/results-hash.html (accessed on 6 November 2019).
2. Aiqing, Z.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in E-Health Systems via Consortium Blockchain. J. Med Syst. 2018, 42, 140. [CrossRef]
3. Nawari, N.O.; Ravindran, S. Blockchain and the Built Environment: Potentials and Limitations. J. Build. Eng. 2019, 25, 100832. [CrossRef]
4. Ozercan, H.I.; Ileri, A.M.; Ayday, E.; Alkan, C. Realizing the potential of blockchain technologies in genomics. Genome Res. 2018, 28, 1255–1263. [CrossRef] [PubMed]
5. Wong, D.R.; Bhattacharya, S.; Butte, A.J. Prototype of Running Clinical Trials in an Untrustworthy Environment Using Blockchain. Nat. Commun. 2019, 10, 917. [CrossRef] [PubMed]
6. Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. JMIR Res. Protoc. 2019, 7, e10163. [CrossRef] [PubMed]
7. Maslove, D.M.; Klein, J.; Brohman, K.; Martin, P. Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study. JMIR Med. Inform. 2018, 6, e11949. [CrossRef]
8. Merkle, R.C. A Digital Signature Based on a Conventional Encryption Function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology; Advances in Cryptology—CRYPTO '87; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1988; pp. 369–378. ISBN 978-3-540-18796-7.
9. Ayoade, G.; Karande, V.; Khan, L.; Hamlen, K. Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment. In Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City,