An Introduction to Blockchains

What It Is All About

An Overview into Encryption

To fully understand the concept of Blockchains, one must first have a basic primer into what Encryption is all about, as the Blockchains heavily rely upon this. A formal definition of Encryption is as follows:

"It is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key."

(SOURCE: https://searchsecurity.techtarget.com/definition/encryption).

Let us illustrate this definition with an example. Suppose Person X wishes to send Person Y some confidential data. Obviously, they will have some apprehension of sending the message in the format that it is already in. The original, written message that is decipherable is known as the "Plaintext". The only way secure that this data can be sent is by converting it over into a garbled state, which is completely incomprehensible.

This is very often done by using what is known as a "Private Key" (this is essentially a mathematical algorithm – the more sophisticated the Private Key is, the complexity of the mathematical algorithm also increases). Once the Plaintext has been converted over into this state, it becomes known as the "Ciphertext". Now, the data can be sent safely over to Person Y. Even if this Ciphertext were to be intercepted by a third party, there is no way that it can be unscrambled, because they do not have the Private Key to do so.

But once the Ciphertext reaches Person Y, it can now be translated back into a readable format, because this entity is in possession of the Private Key that is required to unlock it. This simple example of Encryption can now be used to illustrate what the concept of Blockchain is all about.

Blocks, The Blockchain, and Encryption

Suppose that you work in the finance department of ABC Corporation. You are working on a very important financial spreadsheet, and it needs to be accessed by your co-workers, as well as upper management. As you are creating this document, it will obviously go through a series of edits and revisions by this group of people before it is finally approved.

But you need to keep a lock on these different versions in order to prevent any unintentional or intentional modifications/alterations from being made to it by other people who are not authorized to do so. In other words, you are creating a version history of this financial spreadsheet that is secure, and which will be accessed by a much larger audience.

For example, suppose that Version 1 of this document has been created, and it has been through its first round of edits and revisions. It will now be locked and made more secure by adding an extra piece of code to it which is called the "Block". This is essentially the same Private Key that was described in our earlier example. In other words, this first version of the financial spreadsheet becomes totally undecipherable unless the appropriate party (such as your co-workers, or upper management) possesses this Private Key.

Now, let us assume that over a period of few days, there has been further discussion about Version 1 of your financial spreadsheet, and that the appropriate parties are now ready to make new changes and revisions. With the Private Key that they have been assigned, they will be able to unlock Version 1, and add in these changes and revisions. This updated document will now become Version 2. It too will be locked and made secure by adding a new Block to it (which will be essentially a new Private Key, and be different from the one that was implemented for Version 1).

This same process as just described will keep continuing until the final version of your financial spreadsheet has been approved. In other words, Version 3, Version 4, etc. will be locked down and secured by adding new Blocks to them (once again, these will be newer Private Keys, different than the ones that were assigned to Version and Version 2).

The Blocks that have been assigned to all versions of your document now form a chain, also known as the "Blockchain".

Important Considerations of the Blockchain

However, there some important things to keep in mind about the Blockchain, which are as follows:

- It is used in large, collaborative environments, such as those used in our example. In other words, Blockchaining allows for parties who do not know physically know each other to be able to engage into a series of trusted transactions with 100% confidence in the Integrity and Security of the Digital Assets that are being exchanged.
- It is used primarily on digital media, not on actual physical documents. In these instances, watermarks, signatures, embossed seals, etc. can used to confirm the authenticity.
- Blockchaining is typically used in computerized, closed loop systems (prime examples of this are Dropbox and the Microsoft OneDrive) that are decentralized. In other words, these are synchronized file-sharing systems. So, as changes and revisions are made to each and every iteration (or versions) of a particular document, all of the relevant parties are provided with the latest version, as well as the appropriate Private Key to unlock it.
- No alterations, revisions, or edits can be made to previous versions of a document – only the latest version can be modified. Using our previous example, Version 1, Version 2, and Version 3 of the financial spreadsheet cannot be modified in any way shape or form. Only Version 4 can be changed.
- With Blockchaining, a Distributed Record Keeping system is utilized, called a "Ledger". This is not centralized by any means, but it is distributed to all of the relevant file sharing systems, thus creating an irrefutable audit trail.
- The integrity of all of the document versions are confirmed by using the Digital Signatures that are provided by the Private Keys that have been assigned to them. If all them are the same, then the appropriate parties that are involved with creating the document are ensured that no unauthorized changes or revisions have been made. But however, if all of the Digital Signatures do not match up with another, this is then evidence that a non-authorized party had (or has still has) access to the various document versions.
- Depending upon the level of sophistication of the Private Key, it could take more processing power of the relevant parties' computer to solve the underlying mathematical algorithm of it. Once this has been accomplished, the Private Key is then unlocked, and the latest version of the

document can then be accessed and modified (this is where the concept of "Mining" starts to come into play.

- There are two types of Blockchain environments:

  *Public Blockchains:

  In this particular situation, there are no restrictions as to whom can view, download, and modify and/or revise the document (or any other Digital Asset for that matter). This type of environment typically implemented in those making use of Virtual Currencies, such as Bitcoins and Ethereum.

  *Private Blockchains:

  This is where explicit permissions are required and established to the relevant parties that need to have access to a document (or any other Digital Asset). This is the kind of environment that is typically by most businesses and corporations, as well as used in our illustration of the Blockchain.

The Industries That Make Use of the Blockchain

As mentioned, since Blockchain is used in those environments where a large of amount of collaboration and feedback is required amongst people, it works best in the following types of industries:

1) Supply Chain Management:

   When Blockchain is applied here, there is a much greater threshold for traceability, and making production processes cost effective. For example, it can be used by the large freight and trucking carriers such as UPS and FedEx in order to track packages, their points of origination and destination, the total number of products ordered, etc.

2) Quality Assurance:

   In these instances, Blockchain works very well for such industries as manufacturing and pharmaceutical. It can enhance the existing QA checks in place, by providing details every step of the way in which a certain product was produced. As a result, any defects can be tracked from the very beginning, and corrected early on instead of waiting until the very end, which can be very costly.

3) Accounting:

   The use of Blockchaining drastically reduces the chances of any mathematical errors from being made, as there is now a system of checks and balances being put into place, which also provides a detailed audit trail. High levels of accuracy will also be ensured, because the financial information and data is confirmed and checked as they are passed from one Block Node to the next. As a result, a business or corporation will not have to maintain financial documents and records in different electronic locations, they can all be centrally stored.

4) The Creation and Execution of Electronic based Contracts and Agreements:

   There is no doubt that developing and executing contracts can be a very time-consuming process for any organization. The trend now is to create these types of documentation

electronically. By using the concepts of Blockchain here, Contracts and Agreements can be very quickly validated, signed, executed, and even legally enforced. In the case of any disputes, there is a secure version history in place that cannot be altered in any manner, and can thus quickly provide any evidence that is required by a court of law.

5) Electronic Voting:

   One of the biggest Security issues here is that of fraud, and the lack of trust amongst the many polling places. When Blockchaining is used here, not only will fraud go down, but the levels of trust will also correspondingly increase as well, because there is now a record of each and every vote that was cast, which cannot be maliciously altered in any way. This concept was recently tested in the local elections that were held in Moscow, Russia; as well as the NASDAQ for conducting shareholder votes.

6) Conducting Electronic based Trades on the Stock Exchanges:

   Blockchain is already being used quite heavily here in the United States to secure the financial transactions that are taking place with the Virtual Currencies, with the prime example being that of the Bitcoin. This concept is also being tested in the financial institutions of other countries, with another example being that of the Australian Stock Exchange.

7) Energy and Power Consumption:

   The principles of Blockchain can be used to track the levels of energy/power consumption at the local, state, and even national level. The ability to accurately keep accurate records on all of this can lead to what is known as the "Microgeneration of Energy Resources." For example, households all over the world are now starting to create their own power supplies and turning over to Solar Energy to fill in those gaps where traditional electrical supplies may not even exist. In this instance, the Blockchain can be used to keep a close eye on the "Smart Meters" which are being used to record the levels of power that are generated and consumed by Microgeneration. Some of examples of this are Powerpeers (based out of the Netherlands) and Exergy based out of New York City.

8) Healthcare:

   The secure sharing of confidential information and data of patient records is becoming of utmost concern today amongst hospitals, healthcare providers, healthcare workers, and even the medical insurance industry. By making use of the Blockchain here, the authenticity as well as the integrity of Digital Signatures are guaranteed, thus allowing only authorized individuals and entities to gain access and view patient records. With this, the chances of fraudulent medical insurance payouts taking place is greatly reduced.

The Benefits of the Blockchain

The overall benefits of the Blockchain can be summarized as follows:

1) It is highly transparent:

Since a larger group of people can now access any documents (or any other Digital Media based assets), the entire process of making revisions and modifications now becomes completely transparent to everybody that is involved in this process, as well as the entire version history.

2) It is highly secure:

   As it has been described earlier, Encryption is used to protect previous versions of a particular document as well as the final version. Past versions cannot be altered or modified in any way, only the current version of it can be edited. In fact, it takes a consensus or a majority of the people involved to approve the alterations before they can even be implemented onto the document.

3) It improves the current levels of efficiency:

   The use of Blockchaining can greatly streamline the document management process, thus virtually eliminating the chances of any administrative mistakes or errors from being made. In fact, there is no need to maintain multiple types of documents, which in turn can lead to a greater level of trust amongst the collaborators that are involved in the reviewing process.

4) It can trace products all the way back to the point of origination:

   As it has been reviewed in the last section, the ability to track goods all the way from their point of origination to their ultimate point of destination (with all of the transitory stops being recorded as well) is a huge advantage to the Supply Chain and Logistics Industry. The use of Blockchaining in this regard also helps to greatly reduce the probability of any covert and malicious interception of the product(s) from taking place.

5) An irrefutable Audit Trail is provided:

   Since the version history of the document is literally locked down at each and every step of the entire process, a detailed and complete Audit Trail is thus created without any question being made as to its authenticity or integrity.

Cloud 9 Infosystems and the Blockchain

Cloud 9 Infosystems is currently working on some use cases with regards to the Blockchain. If you would like more information, or have requirements, please contact Chetan Melavia, CEO at 855-225-6839, or chetanm@cloud9infosystems.com.

We look forward to hearing from you and how we can best serve your Blockchain needs.