Project Development Phase

Exception handling

Team ID	NM2023TMID04427
Project Name	Project – Tracking Public Infrastructure And Toll Payment Using Blockchain

History and Background

Although some of the principles incorporated in Blockchain technology were already described in earlier cryptography papers, the basis for the Blockchain technology used today was first published in an October 2008 White Paper on a cryptography mailing list. The paper was called, “Bitcoin: A Peer-to-Peer Electronic Cash System” and was published by an author, or a group of authors, under the pseudonym Satoshi Nakamoto. Interestingly, the term “Blockchain” was never used in the original paper, but rather expressions such as “chain of blocks” and “blocks are chained”. The first use of “block chain” appeared on the same mailing list in subsequent discussions linked to the original Nakamoto paper.

Blockchain: how it works

At its heart, a Blockchain is a cryptographic protocol that allows separate parties to increase the trustworthiness of a transaction because the ledger entries in its database cannot be easily falsified (i.e. once data is written it is extremely difficult to change, albeit provided the data was correct from the outset). This “immutability” is due to a combination of factors including the cryptography used in a Blockchain, its consensus/validation mechanism and its distributed nature.

First, some nomenclature:

a) Block: Data that is appended to the ledger after validation. Once a block is written to the chain, it cannot be changed or deleted without replacing all subsequent blocks.
b) Consensus: An important characteristic of Blockchain systems which allows users to know that transactions have been executed and to evaluate the

trustworthiness of the information about and in those transactions (for example, the date/time of execution and content). In the case of public Blockchains, the umpire that decides consensus is the society of all nodes that choose to participate. In the case of private Blockchains, the umpire is the consortium of nodes given permission to create consensus. There will be more about the different ways in which consensus can be reached in the text below.

c) Fiat or Fiat Currency: These are currencies backed by a central bank such as United States dollars, euros, yen, etc.
d) Hash: The result of mathematical operations carried out on the numeric representation of data – all data in a computer consists of numbers that are deciphered in order to create the words and images you see on a screen. This result has a fixed size and is a unique cryptographic fingerprint of the underlying data. A hash is a one-way function; this means that given the data, it is easy to verify that the hash is the correct one for that data. This is done by performing the pre-defined mathematical operations on the data that supposedly created the hash – if the result is the same, the data is the same. This is a key feature because it allows users to quickly confirm that no changes, at all, have been made. For example, even an additional space or empty line in a text would change its hash. At the same time, and this is what makes it a one-way function, it is almost impossible to recreate the original data if all one has is the hash (i.e. reverse engineer it).
e) Node: A system that hosts a full copy of the Blockchain ledger. In some Blockchains, such as Bitcoin and Ethereum, all nodes participate in the consensus process, in others it may be only be selected nodes.
f) On-chain transaction: An automated procedure that creates or updates the status of a Blockchain asset in the Blockchain database by appending new data to the ledger. Examples include digital asset exchange, or execution of an automated business process. g) Validation: Work performed by nodes, in parallel, that verifies transactions using a consensus algorithm. Different networks may use different consensus algorithms. When mutual validation results in a consensus, then the nodes all commit (record) the verified transactions onto their Blockchain as a new block.

It writes transactions

Each block of data written to a Blockchain ledger contains at least one record of a transaction, although most blocks contain many records of transactions. A simple example of a transaction would be “debit one coin from account A, and credit one coin to account B”, although many other kinds of transactions are possible. Some Blockchains support a limited sub-set of transactions (operations or

algorithms) such as this simple double-entry bookkeeping operation. Some Blockchains support a much wider set of transactions covering any solvable algorithm (i.e. a Turing-complete computer programming language4).

The block is written to the ledger after it is verified

When consensus is reached, which includes agreeing that a block contains legitimate data, and that it is the block that should be written next, each node adds the agreed block to their local copy of the ledger. In this way, all nodes maintain an identical copy of the ledger each time a block is written. This is proven by the next block to be written, because it will contain a hash of the block before it.