



DATA SECURITY FOR RECOVERY PHASE OF CRYPTO WALLETS USING CRYPTANALYSIS AND BLOCKCHAIN



by Astel George Nixon



Abstract

- Purpose: recovery phase is an integral aspect of cryptocurrency, and its security makeup helps to protect a user from theft and unauthorized access to funds. We must keep our recovery phase safe and secret. The traditional method of storing recovery phases are to write it down and store it in several places or take a picture with your phone as these digital copies, but these are not preferred methods. So we are proposing these project to store our recovery phase safe and secret.
- Objective: Main objective of these project is to provide a safest place to store, retrieve and secure the recovery phases
- Methodology: . Encrypting recovery phases using neural network and storing it in the blockchain, and then decrypted by user for accessing . So it can be only accessed by the user and makes it impossible someone to access the recovery phases.
- Results: Create an web based application for ui for user to store their keys which is encrypted using neural network (ANN) and stored in Storj blockchain and then it is decrypted automatically after confirming the identity of user.
- Keywords: recovery phases, cryptograph, Artificial Neural Network, Blockchain, storj database

Introduction

Cryptocurrency is controlled through a set of digital keys and addresses, representing ownership and control of virtual tokens. Anyone can deposit cryptocurrency in any public address. But even though a user has tokens deposited into their address, they won't be able to withdraw them without the unique recovery phase. recovery phase is an integral aspect of cryptocurrency, and its security makeup helps to protect a user from theft and unauthorized access to funds. We must keep our recovery phase safe and secret. The traditional method of storing recovery phases are to write it down and store it in several places as there is no way to recover it if you lose it or it gets into the wrong hands and another method is take a screenshot of it or take a picture with your phone as these digital copies, but these often targeted by hackers. We are proposing these project to store our recovery phase safe and secret. Encrypting and decrypting recovery phases using neural network and storing it in the blockchain. So it can be only accessed by the user and makes it impossible someone to access the recovery phases. Encrypting and decrypting recovery phases using neural network and storing it in the blockchain. So it can be only accessed by the user and makes it impossible someone to access the recovery phases.

Recovery phases

- Cryptocurrency uses a set of digital keys and addresses to convey ownership and control over virtual tokens. The public key is like an address. You can safely share a public key with others to let them know where they can send you funds.
- A recovery phase works like a password. It's known by the user and serves as their digital ID. It authorizes the user to spend, withdraw, transfer, and carry out any other transaction from their account.
- The public key allows anyone to deposit a digital token into any public address, but only the holder of the unique recovery phase can withdraw funds from the account. Because of that, it's crucial to prevent your recovery phase from being lost or stolen.
- recovery phases help secure digital money. Cryptocurrencies such as Bitcoin and Ethereum are decentralized, meaning that no bank or other financial intermediary holds your funds. Instead, crypto is distributed across a network of computers using blockchain technology. That makes all crypto blockchains -- including all public key and transaction information -- available for anyone to see.



[< Back](#)

Confirm your Secret Backup Phrase

Please select each phrase in order to make sure it is correct.

assault

episode

fence

finish

fragile

goose

nature

nest

pizza

reveal

second

squeeze

Confirm

Recovery Phase

- The recovery phrase – sometimes called the seed phrase or mnemonic phrase – is a 12, 18, or 24-word pattern generated each time a new wallet is created. Unlike your recovery phrase, which relates to just one blockchain address, the recovery phrase is a derivative of your entire wallet, and all recovery phrases stored there.
- In layman's terms, a recover phrase is the “master key” for all of your crypto accounts – it is your recovery phrases in mnemonic form. These words, when entered into another crypto wallet (in the correct order) will recover all of the recovery phrases you were storing on your original wallet. The purpose? Giving you control. Having this phrase means that even if you lose your physical hardware device, you'll still have access to your blockchain assets.

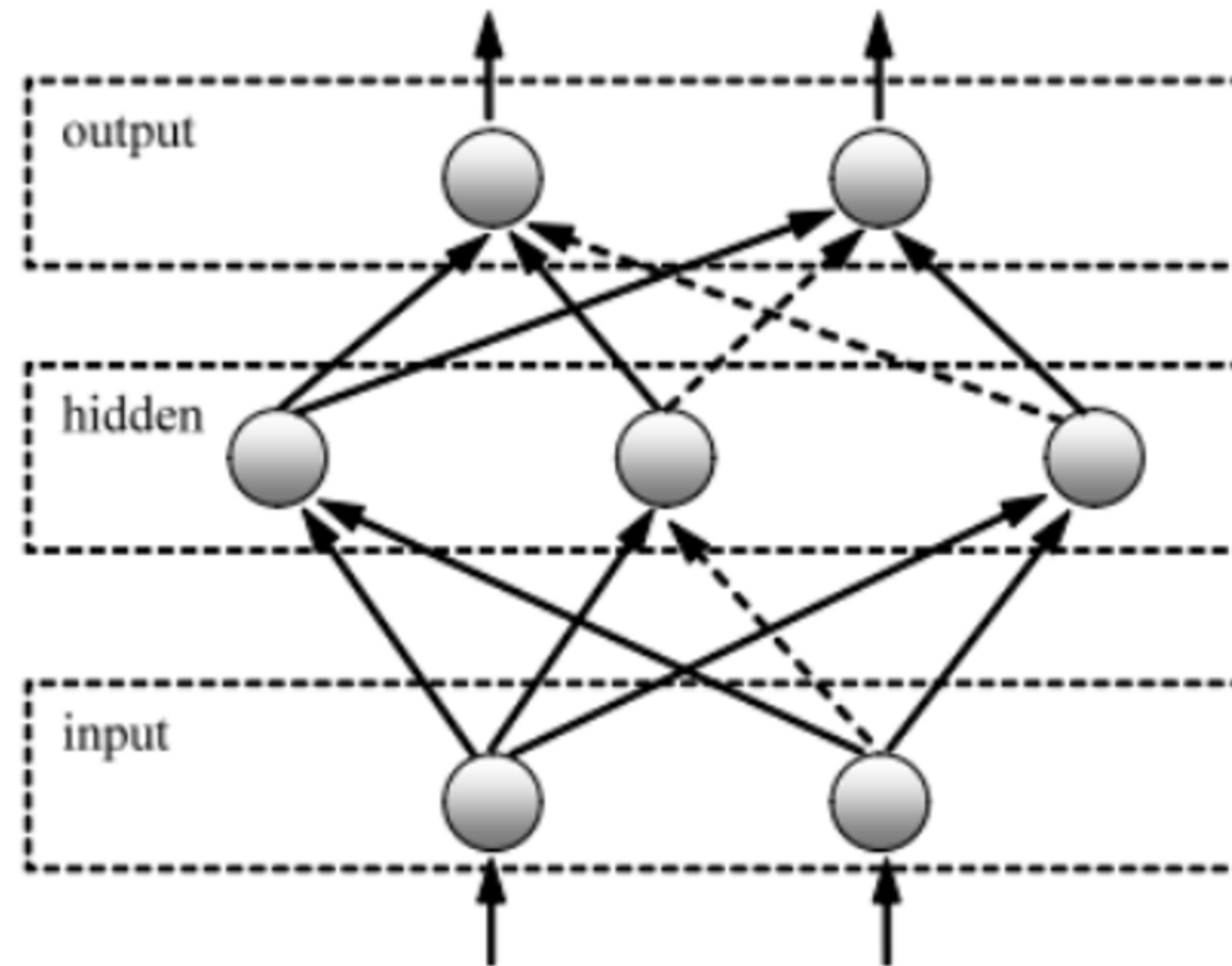
Cryptography

- Encryption and decryption are the two processes that are used to hide sensitive information from prying eyes while it travels over an insecure network.
- Cryptography Using a Public Key: It is an asymmetric cryptography model that is employed in this system . Because the public key is known to all the network's users for encryption of plain text, it is referred to as a "shared key" . As long as the receiver has access to the private key, they can decrypt the message [3, 4]. The term "Private Key" refers to a type of encryption key that is only visible to the individual people that have it.
- Cryptography Using a Single Key: The symmetric cryptography model is employed in this system. This secret key, which is a private key, is used both for encrypting plain text and decrypting cypher text . Because a single key is used for both encryption and decryption, the term "shared secret key" has become popular. The sender and receiver are the only ones who have access to the shared key in this instance

Neural network

- Artificial intelligence, machine learning, and deep learning all benefit from neural networks' ability to mimic the human brain's functioning. Deep learning methods rely on neural networks, often known as artificial neural networks (ANNs) or simulated neural networks (SNNs). Because they replicate the way biological neurons communicate with one another, their name and structure are derived from the human brain as well.
- Information processing paradigms inspired by biological nervous systems, such as the brain, are known as Artificial Neural Networks (ANNs). The information processing system's architecture is a critical component of this paradigm. In order to tackle certain problems, it is made up of a vast number of intricately coupled processing parts (called neurons). As with human beings, artificial neural networks (ANNs) learn by mimicry. A learning process is used to customise an ANN for a particular application, such as pattern recognition or data classification. Synaptic connections between neurones are altered during learning in biological systems. This is also true for ANNs.

Neural network



Neural network

- This neural network is one of the most complex for supervised learning. Multilayer feedforward neural networks are the topology of the network.
 - In our experimental study, the following are the parameters of both ANNs:
 - There are six nodes in each input layer, each representing a 6-bit block;
 - There are a total of six nodes in each concealed layer;
 - The decrypted output message is defined by six nodes in each output layer.
 - Full network connectivity; An activating function of the sigmoid;
 - A learning rate is equivalent to 0.03

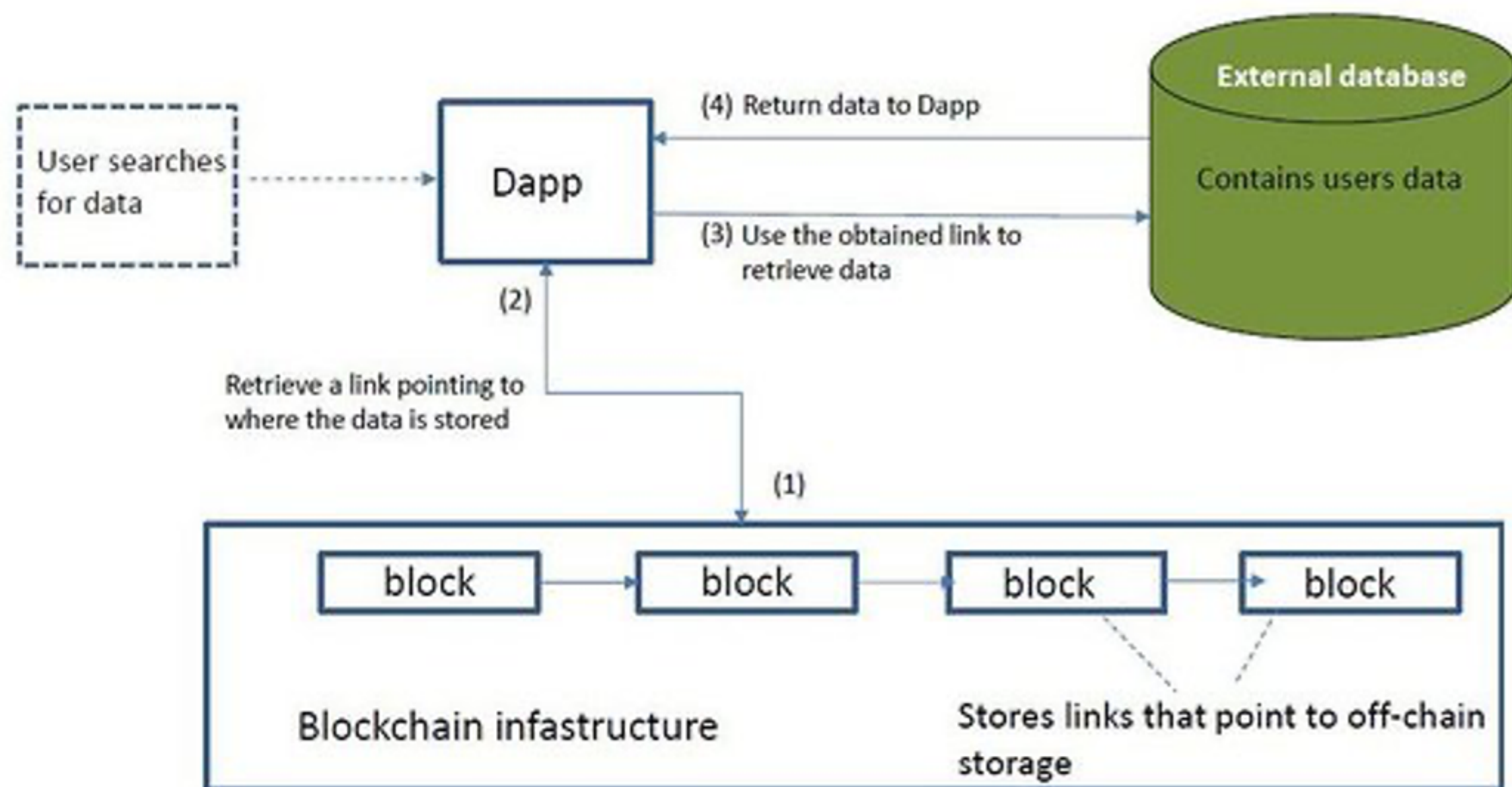
Blockchain

- A blockchain is a decentralized, public ledger for recording transactions and securing the network.
 - In order to access data on a blockchain, one must first become an authorized user of that system.
 - The data are openly shared to all nodes of the network and verified through consensus by participants called miners.
 - It has features such as encrypted transactions, time stamping, and proof of work.
- With Blockchain, no centralized agency or institution controls the data or ensures its security like a bank would do with a traditional database.
 - This means that data on Blockchain can only be accessed by those permitted to do so such as developers working with real Bitcoin addresses or users who can prove themselves using private keys from their respective cryptocurrencies wallets.

Blockchain

- The biggest disadvantage of cloud storage is that all data is centralized and is not usually encrypted during transactions
- Thus, there is a requirement for decentralized storage. Below are some of the reasons why blockchain is required for data storage
- Decentralization: The decentralized nature of blockchain ensures that there is no single central entity governing data-related decisions.
 - Security: Decentralized cloud data is difficult to attack as there are multiple nodes in the network with the same copy of data and any hacker must have to change data on the majority of nodes on the network to make the change look legitimate.
- Distributed: Blockchain is a distributed ledger where independent computers record, share, and synchronize the transactions instead of keeping data centralized in one location.

•



Proposed System


- Encryption and decryption algorithms using neural networks have proven to be effective.
- Keys for cryptography were created using parameters from both modified neural networks. Backpropagation was used to adjust multilayer neural networks. Each neural network's topology is determined by the data it has been trained with .
 - The input message is separated into 6-bit data sets throughout the encryption process, and 6-bit data sets are also produced following the encryption process.
 - This means that each system was built as follows: Six units on the input layer and six units on the output layer are available.
- In the buried layer, there is no prescribed number of units, but we used six. Binary symbol representations were used to train both networks.

- This means that each training set has chains of numbers and letters equivalent to binary values of their ASCII code, and each chain of punctuation symbols (e.g. 32) is equivalent to a binary value for the ASCII code of space.
- This random string of six bits becomes the encryption text
- A cryptographic key is the foundation of all encryption and decryption systems.
- For both encryption and decryption, SIMPLE systems rely on a single, unique key.
 - There are two keys in the best systems. Only the second key can decrypt a message encrypted with the first.
- In order to use the neural network as an encryption and decryption algorithm, the keys must be configured in accordance with both the topologies (architecture) and the configurations of the neural networks themselves (weight values on connections in the given order).

Data Storage using Storj

- Storj DCS (Decentralized Cloud Storage) is private by design and secure by default delivering unparalleled data protection and privacy when compared to traditional centralized cloud object storage alternatives, like Amazon Web Services (AWS).
- Decentralization delivers the highest possible levels of security and privacy for users who demand to own their data and control its use, integrity, and access.
 - By bringing decentralization to cloud-based storage, Storj DCS is able to deliver privacy and security benefits as well as providing inherently better economics than centralized alternatives.
- Storj incentivizes two parties to use the network — those with extra bandwidth and storage capacity on their computers (host Storage Nodes), and those in need of this excess capacity
 - Storj comprises a global network of independent nodes and a peer-to-peer communications protocol which allows the Nodes to communicate.

Storj interface

 **STORJ** | DCS

Projects ▾Resources ▾Settings ▾

✓ EU1

P

Disk ⋮

Dashboard

Objects

Access

Users

Disk Dashboard

Expect a delay of a few hours between network activity and the latest dashboard stats.

Storage

44.46GB Remaining

Storage Used 5.54GB / 50.00GB

Bandwidth

50.00GB Remaining

Bandwidth Used 0 / 50.00GB

Details

Users
1

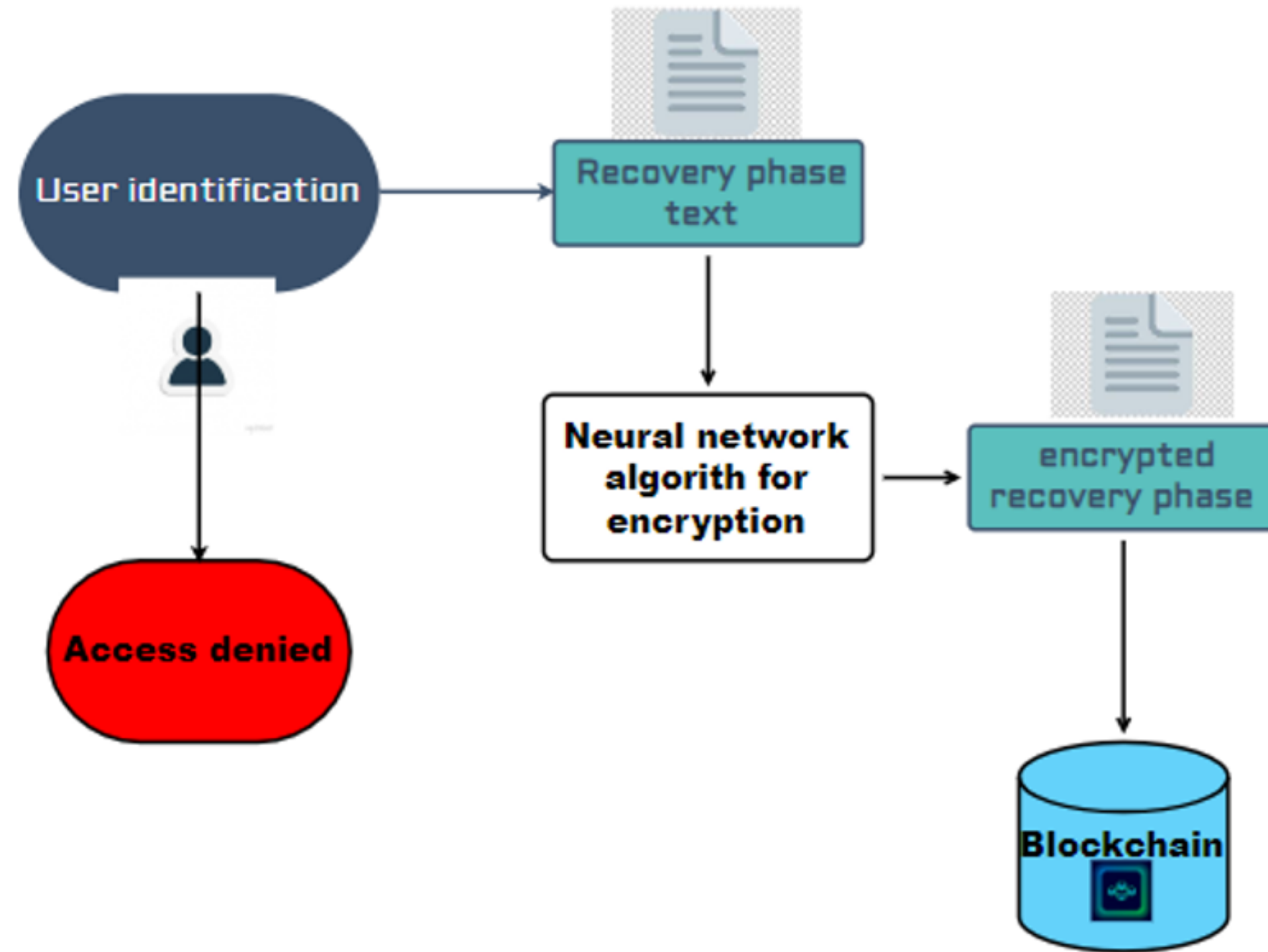
Access Grants
2

Buckets
1

Estimated Charges
\$0.00

Buckets

Architecture design



Literature Survey

- ENCRYPTION AND DECRYPTION ALGORITHM BASED ON NEURAL NETWORK

by Dr.Amarnadh S ,D.Prudhvi raju,N.Santosh Kumar and N.Sai charan

This paper discusses neural networks to encrypt and decrypt, the neural network will be trained with keys and plain text in this study.

- A Blockchain-based Decentralized Data Storage and Access Framework

by Saqib Ali[†], Guojun Wang,Bebo White and Roger Leslie Cottrell

In this paper the creator design a blockchain- based data storage and access framework to remove its total dependence on a centralized repository.

The Technology

- Hardware requirements

Storage – 100 GB or above

RAM – 4GB RAM

Internet – 100 mbps bandwidth

- Software Requirements

Frontend – Python framework called streamlit

Backend – Storj Blockchain database

- Operating System

Windows 7 or above, macos



**THANKS
YOU**

