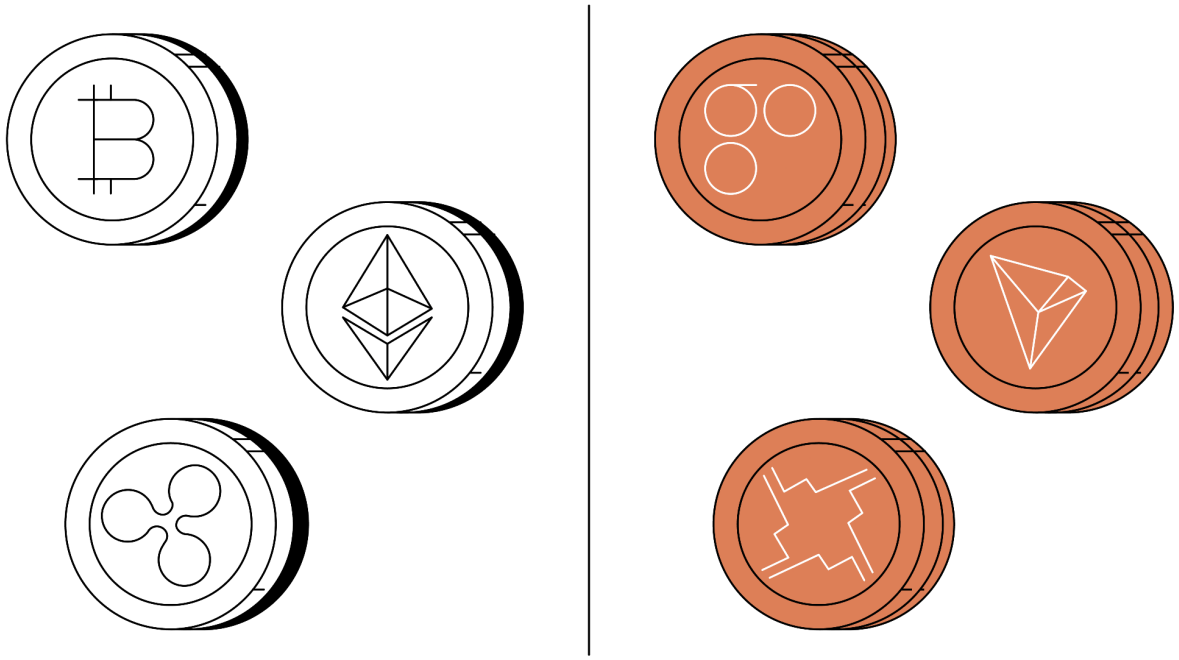
Cryptobase



Double Helix [Team 22]

Sai Praneeth | 2022101097
Sohan Gupta | 2022101061
Deekshitha | 2022101063
Bharath | 2022101044

Introduction to Mini-world

In the fast-paced and dynamic realm of cryptocurrencies, the need for an efficient and reliable database has become paramount. Our cryptocurrency database serves as a central hub for storing and managing information related to digital currencies. “This database is not exactly the one which is the center of all cryptocurrency, but rather we made it to make it easier for the users to transact, build miners, etc.”. Not exactly the central hub, but a database that is designed to store useful things in this decentralized network. Like a network for crypto-users.

Purpose of Database

The purpose of this database is to provide a comprehensive repository of data on market trends, user activities, and transaction histories within the cryptocurrency landscape. By offering an in-depth understanding of these intricate workings, the database aims to facilitate informed decision-making and analysis for various stakeholders..

Users of Database

a. Miners: Individuals or organizations engaged in the process of validating transactions and adding them to the blockchain using mining machines.
b. Government Agencies: Regulatory bodies, tax authorities, and law enforcement agencies might access the database to monitor and regulate cryptocurrency-related activities, enforce tax compliance, and investigate potential illegal activities.
c. Investors: Individuals and institutions that hold cryptocurrencies as investments or assets, tracking their portfolios and transaction history.
d. Developers: Individuals or teams involved in blockchain and cryptocurrency development, including those creating new cryptocurrencies, blockchain applications, or working on blockchain infrastructure.

e. Casual users: Everyday individuals who use cryptocurrency for transacting their money in a secure way, instead of relying on the fiat currency.

Strong Entity Types

Entity Type	Attributes	Attribute Type	Sub Attributes	Data Type	Constraints
Cryptocoin	Coin	Key attribute, composite	Coin name	VARCHAR	UPTO 25 characters
			Abbreviation	VARCHAR	UPTO 10 char
	Market cap	simple	-	INT	>= 0
	Current price	simple	–	INT	>= 0
	Total supply	simple	-	INT	>= 0
	Symbol	simple	-	SVG	UPTO 5MB
	Avg conversion rate	simple	-	INT	> 0
	All Time High	simple	-	INT	> 0
	Website URL	simple	-	VARCHAR	UPTO 100 char
Transaction	Exchanged Cryptocoin	simple	-	VARCHAR	UPTO 25 char
	Sender wallet	simple	–	VARCHAR	UPTO 50 CHAR
	Receiver wallet	simple	-	VARCHAR	UPTO 50 CHAR
	Transacted amount	simple	-	INT	>0
	Hash value of transaction	Key attribute	-	VARCHAR	UPTO 50 CHAR
	Time stamp	simple	-	TIME	Time

					constraints
Crypto-user	Username	Key attribute	-	VARCHAR	UPTO 25 CHAR
	avatar	Simple	-	SVG	UPTO 5MB
	mail address	SImple	-	VARCHAR	
	Creation TIme	Simple	-	TIME	Time constraints
	No of wallets	Derived	-	INT	>= 0, <= 10
	Most used cryptocurrencies	Multi -valued	-	INT	>= 0
Mining Machine	Coordinates	Composite	Latitude	FLOAT	-90 < x < 90
			Longitude	FLOAT	-180 < x < 180
	Machine ID	Key attribute	-	INT	> 0
	Model	simple	-	VARCHAR	UPTO 50 CHAR
	Computational power	simple	-	FLOAT	> 0
	Energy Consumption	simple	-	FLOAT	> 0
	Operating status	simple	-	ENUM	ENUM constraints
	Associated wallet	simple	-	VARCHAR	UPTO 50 CHAR
	Operational time (in hrs)	simple	-	INT	> 0
Crypto-Exchange	Exchange ID	Key attribute	-	INT	> 0
	Exchange Name	simple	-	VARCHAR	UPTO 50 CHAR
	Website URL	simple	-	VARCHAR(URL)	UPTO 100 CHAR
	Flat currency	simple	-	BOOLEAN	T / F

	support				
	Rating	simple	-	FLOAT	0 < x < 10
NFT	Token ID	Key attribute	-	VARCHAR	UPTO 50 CHAR
	Date of creation	simple	-	TIME	Time constraints
	Current owner of the token	simple	-	VARCHAR	UPTO 25 CHAR
	Creator of the token	simple	-	VARCHAR	UPTO 25 CHAR
	Description	simple	-	VARCHAR	UPTO 200 CHAR
	Royalty for creator	simple	-	FLOAT (%)	0 < x < 50
	Rating of the token	simple	-	FLOAT	0 < x < 10

Weak Entity Types

Entity Type	Attributes	Attribute Type	Sub Attributes	Data Type	Constraints
Wallet	Wallet Address	Partial key	-	VARCHAR	UPTO 25 CHAR
	Balance	Simple	-	FLOAT	>= 0.0
	Security Feature	Simple	-	ENUM	ENUM constraints
	Public Key	Simple	-	VARCHAR	UPTO 25 CHAR
	Wallet Status	Simple	-	ENUM	ENUM constraint
	Creation TIme	Simple	-	TIME	Time constraints
User Activity Log	Transaction hash	Partial key	-	VARCHAR	UPTO 50 CHAR
	Wallet used	simple	-	VARCHAR	UPTO 25 CHAR
	Receiver user	simple	-	VARCHAR	UPTO 25 CHAR
Price Data	Time stamp	Partial key	-	TIME	TIME constraints
	Price at that time	simple	-	FLOAT	>= 0
	Percentage in ATH	derived	-	FLOAT	0 < x < 100
Trading pairs	Cryptocoin 1	Partial key	-	VARCHAR	UPTO 10 CHAR
	Cryptocoin 2	Partial key	-	VARCHAR	UPTO 10 CHAR
	Conversion fee	simple	-	FLOAT	> 0
	Exchange ratio	derived	-	FLOAT	> 0

Relationship Types

Relationship Type	Degree	Entities	Cardinality	(min, max)
HAS (*)	2	USER HAS WALLET	1 : N	USER(1,N) WALLET(1,1)
SUPPORTS	2	EXCHANGE SUPPORTS COIN	M : N	EXCHANGE (1,N) COIN (1,M)
OFFERS (*)	2	EXCHANGE OFFERS TRADING_PAIRS	1 : N	EXCHANGE(1,N) TRADING_PAIRS(1,1)
OWNS	2	USER OWNS MINING_MACHINE, NFT	1 : N	USER(1,N) MINING_MACHINE (1,1) NFT(1,1)
CREATES_BLOCK	2	MINING_MACHINE CREATES_BLOCK TRANSACTION	1 : N	MINING_MACHINE (1,N) TRANSACTION(1,1)
USES	2	USER USES COIN	M : N	USER(1, N) COIN(1, M)
SENDS .. TO .. RECORDED_BY	4 (N-ary)	USER SENDS COIN TO USER RECORDED_BY TRANSACTION	1 : N : M : K	USER(1,N) COIN(1,1) USER(1,M) TRANSACTION (1, K)
BOUGHT .. WHEN	3 (ternary)	USER BOUGHT COIN WHEN PRICE_DATA	M : N : N	USER(1, N) COIN(1,M) PRICE_DATA(1,M)

(*) - Identifying relationship types

Functional Requirements

Modifications

- **INSERT:**
    - INSERT_CRYPTO_USERS: After registration of a new user, creates a row for the crypto-user and inserts the details into the database
    - NEW_WALLET: creates a new wallet & adds to the wallet list of the user who has requested this.
    - NEW_MINING_MACHINE: Creates a new row for a minning_machine. (Machine ID as key attr.)
- **DELETE**:
    - DELETE CRYPTO_USERS: When there is a request to delete a user from the database (based on username), delete the row of the given USERNAME(key) from the table. (after cleaning out all the necessary)
    - DELETE WALLET: When the user is deleted or a request from the user comes to delete the wallet, delete the row of the given wallet address, and username.
- **UPDATE**:
    - UPDATE COIN_PRICE: Called once every 'x' ms, updates the coin price (determined by the market)
    - UPDATE USERNAME: Upon request, update the crypto-user's username / email.

Retrievals

- **SELECTION**:
    - MINING_DETIALS_OF_USERS: Returns the details of all the MINING MACHINE HANDLED BY A GIVEN USER
    - TRANSACTIONS_OF_USERS: Returns all the transactions of a user given a particular cryptocurrency to another user

- **PROJECTION**:
    - HARAM_MINING: Returns Machine IDs / coordinates of Mining Machines whose energy consumptions exceed a given threshold.
    - RISH_COINS: returns the list of abbreviations of crypto-coins whose current price is greater than a given price.
- **AGGREGATE**:
    - TOTAL_TRANSACTED_CRYPTO: returns the SUM of amount in each block in the Blockchain.
    - ROYALTY_RULES: returns the NFT with maximum royalty for the creator
- **SEARCH**:
    - PARTIAL_TEXT_SEARCH: Search for entries in an entity, matching for sub-parts of the entries. (ex. Searching for a username in USERS, Searching for a cryptocurrency exchange with its name / website URL)

Analysis

- MOST_USED_CRYPTO: Given the username, returns the most used crypto of the user (by calculating count of each cryptocoin the user uses, in the transactions where the user's wallet is the sender. And finding the MAX of all counts)
- EXCHANGE_RATES: Returns the exchange ID, exchange rates / conversion_fees from all the *crypto-exchanges* given two cryptocurrencies (BTC = 'x' DOGE + conversion_fee)

Assumptions

1. Wallets typically depend on the user. If there is no user, there are no wallets. Users can have multiple wallets.
2. Each transaction has a unique hash, which it is identified by.
3. Mining machines are the machines in this decentralized network of cryptocurrency. These are the one which computes, and calculates the transactions and creates the blocks in blockchain.

4. For the creation of blocks in the blockchain, we assume that a single mining machine creates a block, and gets rewarded for the same.
5. We used data types like TIME when describing the entities, this TIME data type indicates the Timestamp (generally date + time) [ex. 12 OCT 2023 19:28:09:23 GMT]. The constraints for the same will be checking if the date is correct, time is correct and doesn't exceed the current timestamp.

Summary

Not exactly the central hub, but a database that is designed to store useful things in this decentralized network. Our cryptocurrency database is a blend of central organization and decentralization, reflecting the values of cryptocurrencies. It securely stores digital currency data, benefiting miners, government agencies, developers, and investors. Decentralized features promote transparency and robustness, fitting the cryptocurrency world's decentralized nature. And, we only store the public keys of the wallet, not the private ones, maintaining the decentralized nature of Cryptocurrency.

Edge over existing databases

- Unified Wallets for all cryptocurrencies: Currently, Each cryptocurrency needs a different wallet & we have to maintain a separate wallet address for each crypto. Instead of that, in this mini-world, there is a Unified Wallet for all cryptos, which makes it easier to maintain & share.
- Wallet belonging to only one user: Usually, in the current world, there is a use of shared & joint wallets. This kind of system makes it prone to security risks, privacy concerns, tax implications, etc. Also, there will be loss of control, which can lead to unintended transactions. This problem is eradicated by introducing "Wallets" as a dependent entity of the "User".