

دانشگاه صنعتی شریف

پروژهی صرافی ارز دیجیتال: پایگاه داده – فاز اول

استاد: دکتر مهدی آخی

شمارهٔ تیم: ۱۴

محمد جعفریپور ۴-۱۱-۵۷۹۷

محمدامین *حیدری* ۴-۱۱۷-۵۵۳ مانی ابراهیمی ۴-۱۱۷۰۴۹۱

بهار ۳-۱۴

فهرست مطالب

۵																														ڑہ	روڙ	از اول پ	ت فا	كليت	١
۵																																شرح		1.1	
۵																								-						يف	ظا	قسيم و	<u>ڌ</u>	1.4	
Υ																															\mathbf{E}	های R	رام	دیاگ	۲
Υ																																س شرح	•	۲.۱	
Υ																															ۇر د	-ری وضیح ه		۲.۲	
Υ																														Use		۲.۲.			
٧																														alle		۲.۲.۱	,		
Υ																														ion		7.7.1	u		
λ.																														der		7.7.1			
λ.																														ade		۲.۲.۷			
Y																														ook		7.7.9	-		
Y																														ket		7.7.1			
Λ ,																														ker		۲.۲.۶			
9																														enc		7.7.	•		
9																														vor	•	7.7.1			
•																														ent					
9																												•				7.7.1	-		
9																															~	Y.Y.11			
٩	•	•	•	٠	٠	•	•	•	•	٠	•	•	•	•	•	٠	٠	٠	•	•	•	•	(ŗ,	Уľ	oto)]	Hl	sto	orie	es	۲.۲.۱۱			
11																														ەاي	ط	، جبر راب	لات	سوا	٣
11																																شرح	د	٣.١	
11																													ت	والاد	w	اسخ به	ڍ	٣.٢	
11																													١	۔ نوال	w	۳.۲.	١		
11																													۲	ء بوال	w	۳.۲.۱	۲		
۱۱																														ر بوال		٣.٢.١	u		
11																														ر ىوال		٣.٢.٢	c		
۱۲																														ر ىوال		۳.۲.۷	١		
14																														ر ىوال		۳.۲.۶			
14																														ىوال بوال		۳.۲.۱			
۱۲												Ċ																		ىوال ىوال		۳.۲.۶			
14																														بوال بوال		۳.۲.۰			
14																														بوال بوال		۳.۲.۱			
• •	•	•	•	•	•	•	•	•	•	•	•	•	•	•	٠	•	•	•	•	•	•	•	•	•	•			•	1-	بون	w	1 - 1 - 1	-		

فهرست مطالب		۲
-------------	--	---

رام ER	ضمیمه: تصویر دیاگر	۴
NY NY	کلیت فاز دوم پروژه ۵.۱ شرح	۵
ا ول، به نمودارهای منطبق با SQL مودارهای منطبق با SQL مودار برای بیینه سازی	۶.۱ چہار تغیر در ن ۶.۱.۱ رابط ۶.۱.۲ رابط ۶.۱.۳ رابط	۶
۲۵	ساخت پایگاه داده	γ
۲۷	۸.۱.۲ حذف ۸.۱.۳ نرما ۱۲ نرمانها ۸.۲.۱ ایند: ۸.۲.۲ ایند:	٨

کلیت فاز اول پروژه

1.۱ شرح

در این فاز تلاش شده تا یک پایگاه دادهی مرتبط با یک صرافی ارز دیجیتال طراحی شود. این پایگاه داده شامل موجودیتهایی مانند کاربر و کیف پول و تراکنش است. همچنین برای هر موجودیت روابطی با موجودیتهای دیگر نیز تعریف شده است. در ادامه به توضیح هر یک از موجودیتها و روابط آنها با موجودیتهای دیگر پرداختهایم. همچنین در انتها پاسخ به ۱۰ پرسش جبر رابطهای داده شده نیز آمده است. مخزن یا همان repository این پروژه در اینجا قابل مشاهده است.

١.٢ تقسيم وظايف

تیم این پروژه متشکل از سه نفر بود که برای سادگی در سند تقسیم وظایف، برای آنها از اسم کوتاه استفاده کردیم:

شماره دانشجویی	نام کامل	نام کوتاہ
4.114.441	مانی ابراهیمی	Mani
۴-۱۱۷-۵۵۳	محمدامين حيدري	Mamadamin
4-11-2	محمد جعفریپور	Mamal

جدول ١٠١: جدول اعضاى تيم در جدول تقسيم وظايف

جدول تقسیم وظایف نیز از اینجا^۲ قابل مشاهده است.

ا در صورتی که لینک برای شما کار نمیکند، از آدرس https://github.com/maniebra/dbms-exchange-project در صورتی که لینک برای شما کار نمیکند، از آدرس ستفاده نمایید.

^۲در صورتی که این لینک برای شما کار نمیکند، میتوانید از آدرس

 $https://docs.google.com/spreadsheets/d/1x1Guh4HTWLyG9GTomZEtesp5cjIGez9m9Day3bS_kgM/edit?usp=sharing \\ \textbf{.augus}$

${ m ER}$ دیاگرام های

۲.۱ شرح

در این بخش تلاش بر این بود که کلیت پایگاه دادهی مورد نظر را با استفاده از دیاگرامهای ER نمایش دهیم. ابتدا دیاگرام ER اصلی را نمایش دادهایم و سپس به تفکیک بخشهای مختلف آن پرداختهایم.

۲.۲ توضیح هر موجودیت

در ادامه، برای هر موجودیت حاضر در این دیاگرام توضیحی آمده:

User Y.Y.1

موجودیت کاربر یا همان user، که دارای صفات گفته شده از جمله نام و نام خانوادگی و شناسه ملی و شماره تماس و ایمیل و رمز عبور و سایر موارد است. این موجودیت برای کاربران اصلیترین موجودیت بوده چرا که اطلاعات خود هر کاربر را در این موجودیت ذخیره میکنیم. همچنین به یک موجودیت کیف پول متصل است که باعث میشود هر کاربر یک کیف پول داشته باشد.

Wallet Y.Y.Y

موجودیت کیف پول یا همان wallet، که دارای صفات گفته شده از جمله موجودیت کاربر و موجودی و ارز و سایر موارد است. این موجودیت برای ذخیرهی اطلاعات مربوط به کیف پول هر ارز از هر کاربر استفاده میشود. همچنین به یک موجودیت تراکنش متصل است که باعث میشود هر کیف پول دارای تراکنش باشد.

Transactions Y.Y.Y

موجودیت تراکنش یا همان transactions، که دارای صفات گفته شده از جمله موجودیت کیف پول و نوع تراکنش و مبلغ و تاریخ و سایر موارد است. این موجودیت برای ذخیرهی اطلاعات مربوط به تراکنشهای هر کیف پول استفاده میشود. در هر تراکنش مقداری ارز از کیف پول یک کاربر خارج شده و به کیف پول کاربری دیگر میرود. در نظر داشته باشید که هر تبادل، دو تراکنش است.

همچنین صفت fee در تراکنش با داشتن $\mathrm{Market_id}$ و بدست آوردن ارز پایه ی آن مارکت و قیمت لحظه ای آن ارز پایه به ریال محاسبه میشود.

Orders Y.Y.F

موجودیت سفارش ها یا همان Orders، که دارای صفات گفته شده از جمله تاریخ و وضعیت و نوع ارز و حجم و قیمت و سایر موارد است. این موجودیت برای ذخیره اطلاعات مربوط به سفارشات کاربران می باشد و دارای دو نوع خرید و فروش می باشد. همچنین به یک موجودیت تبادل متصل است در اصل ترکیب دو سفارش خرید و فروش می باشد.

Trades Y.Y.3

موجودیت تبادل ها یا همان ${
m Trades}$ ، که دارای صفات گفته شده از جمله تاریخ و حجم و مقدار و سایر موارد است. این موجودیت برای ذخیره اطلاعات مربوط به تبادل ها می باشد که تبادل ها میتواند بین یک کاربر و ادمین سایت و یا دو کاربر باشد که به ترتیب دو موجودیت ${
m OTC}$ و ${
m P2P}$ و تشکیل داده اند. همچنین این موجودیت دارای یک شناسه برای هر تبادل می باشد. صفت ${
m min_fill_remainder}$ به این صورت عمل میکند که حجم باقیماندهی کمینهی دو سفارش خرید و فروش را ذخیره میکند.

OTC

شامل ${
m ID}$ ادمین و مشتری میباشد که بوسیلهی شناسهی ${
m Market}$ به بازار مربوطه متصل شده است.

P2P

شامل دو ${
m ID}$ و ${
m Order ID}$ خریدار و فروشنده یا همان ${
m maker}$ و میباشند که به وسیلهی شناسهی صرافی یا همان ${
m Broker_ID}$ به صرافی مربوطه متصل شدهاند.

OrderBooks Y.Y.9

موجودیت لیست سفارشات یا همان OrderBooks، که دارای صفات گفته شده از جمله شناسه و شناسه ی بازار و و سایر موارد است. این موجودیت برای ذخیره اطلاعات مربوط به لیست های سفارشات هر فروشگاه میباشد، همچنین به یک موجودیت لیست که زیرمجموعهی OrderBooks است متصل شده که شامل دو نوع لیست خرید و فروش می باشد و به موجودیت سفارشات که خود دو نوع خرید و فروش دارد نیز متصل است که در نهایت این دو نوع خرید و فروش با هم سفارشات را بتواند بسازد.

Markets Y.Y.Y

موجودیت فروشگاه ها یا همان Markets، که دارای صفات گفته شده از جمله کارمزد و قیمت لحظه ای بازار و نوع ارز پایه و سایر موارد است. این موجودیت برای ذخیره اطلاعات مربوط به فروشگاه های خرید و فروش ارز دیجیتال برای کاربران می باشد. همچنین به یک موجودیت لیست سفارشات متصل است که شامل دو لیست خرید و فروش هر فروشگاه می باشد.

Brokers Y.Y.A

موجودیت صرافی ها یا همان Brokers، که دارای صفات گفته شده از جمله شناسه و سایر موارد است. این موجودیت برای ذخیره اطلاعت مربوط به صرافی های ارز دیجیتال می باشد. همچنین به موجودیت فروشگاه ها متصل می باشد که برای هر ارز پایه در صرافی یک فروشگاه وجود دارد و به یک یا چند admin متصل است که در ان ادمین های هر صرافی مشخص می شوند.

CryptoCurrency Y.Y.9

موجودیت کریپتو ها یاCryptoCurrency ارز هایی اند که در سایت وجود دارند و توسط افراد مبادله میشوند. این ارز ها ممکن است قیمت ثابت Stable coinباشند و یا قیمت انها هرلحظه عوض شود nonstable Currency.

Network Y.Y.1.

هر ارز شامل چندین شبکه ی مجزا از هم است که تراکنشهای آنها روی بستر متفاوتی انحام میشود.این شبکه ها دارای کارمزد و زمان متفاوتی اند.

Online Payments Y.Y.11

تاریخچهی تمامی واریزیهای هر کاربر، مقدار آن و زمان انحامشده است.

Wallet History Y.Y.1Y

تاریخچهای از تغییرات میزان هر کیف پول است و هر تراکنشی برای دو کیف پول یک Wallet History جدید میسازد.

Crypto Histories Y.Y.17

تاریخچهی تغییرات قیمت یک رمزارز است که زمان آن تغییر و مقدار و قیمت آن در آن زمان (قیمت همان قیمت لحظهای مارکت است) نشان میدهد. با انحام هر تراکنش یک CryptoHistory جدید ایجاد میشود چرا که قیمت لحظهای ارز تغییر میکند.

سوالات جبر رابطهای

```
در این بخش پاسخ به ۱۰ سوال جبر رابطهای ۱ آمده است.
                                                                          ٣.٢ پاسخ به سوالات
                                                                                         ۳.۲.۱ سوال ۱
\Pi_{market\_id,fee}(Transactions)
\bowtie_{Transactions.market\_id=Market.market\_id \land Transactions.date=date} \ (
_{market\_id}\mathcal{F}_{\max(date)}(
                    Market \bowtie_{Market.market\_id=Transactions.market\_id} Transactions)))
                                                                                         ۳.۲.۲ سوال ۲
   \scriptstyle owner\_id \mathcal{F}_{\texttt{Sum}(total\_value \times in\_time\_price)}[Wallets \bowtie_{Market.market\_id=id} Markets]
                                                                                        ۳.۲.۳ سوال ۳
                        _{crypto\_id}\mathcal{F}_{\mathtt{Count}(order\_id)}[\sigma_{fill="false"}(Orders)]
                                                                                        ۳.۲.۴ سوال ۴
A = \rho_{user\_id,total}[_{owner\_id}\mathcal{F}_{Sum(fee)astotalSell}]
                         (Transactions \bowtie_{Transactions.origin\_wallet\_id=wallets.id} Wallet)]
B = \rho_{user\_id,total}[_{owner\_id}\mathcal{F}_{\texttt{Sum}(fee)astotalBuy}]
                            (Transactions \bowtie_{Transactions.dest\_wallet\_id=wallets.id} Wallet)]
                                            user\_id\mathcal{F}_{\mathtt{Sum}(Total)}
                                                                                     Relational Algebra<sup>1</sup>
```

```
۳.۲.۵ سوال ۵
```

 $A =_{user_id, cryptoid} \mathcal{F}_{\texttt{Count}(Transactions.id)}(\\ (Users \times Cryptocurrency) \ltimes_{users.user_id=Transactions.SellerID}$

Transactions)

 $B =_{user_id, cryptoid} \mathcal{F}_{\texttt{Count}(Transactions.id)}($ $(Users \times Cryptocurrency) \times_{users.user_id = Transactions.BuyerID}$

Transactions)

 $user_id, cryptoid \mathcal{F}_{mathttSum(TotalCount)} (\\ \rho_{user_id, cryptoid/TotalCount(A)} \cup \rho_{user_id, cryptoid/TotalCount(B)})$

۳.۲.۶ سوال ۶

 $\mathcal{F}_{\mathtt{Sum}(fee)}[\sigma_{Now-Date} \geq "0000-00-30-00:00:00"}(Transactions)]$

۳.۲.۷ سوال ۷

 $A = \Pi_{cryptoid, in_time_price}(Cryptocurrency)$

 $B =_{cryptoid} \mathcal{F}_{mathttmax(Date)asDate}($

 $\sigma_{Transactions.Date-Now() \leq "0000-00-30-00:00:00"}(Transactions \rtimes Cryptocurrency))$

 $C = \prod_{cryptoid,fee} [Cryptocurrency \bowtie_{Cryptocurrency.idTransactions.cryptoid} ($ $Transactions \bowtie B)]$

 $\Pi_{cryptoid,in_time_price-fee}(A\bowtie)C$

۳.۲.۸ سوال ۸

 $A =_{owner_id} \mathcal{F}_{\texttt{Sum}(Total_value)assum}(Wallets)$

 $B = \Pi_{owner_id, cryptoid, Total_value}(Wallets)$

 $_{cryptoid}\mathcal{F}_{count(owner_id)}[\sigma_{percentage} \geq 0.05(\rho_{cryptoid,owner_id,percentage}]$

 $\Pi_{cryptoid,owner_id,\frac{Total_value}{Sum}(A\bowtie B)}])]$

۳.۲.۹ سوال ۹

 $A = \Pi_{user_id,Date}(\sigma_{Date-Now() \leq "0000-00-30;00:00:00"}(Online_Payments))$

 $B = \rho_{user_id,paymentDate}(A) \bowtie WalletHistories$

 $C =_{cryptoid,user_id,paymentDate} \mathcal{F}_{\texttt{Max}(Date)}(\sigma_{Date < paymentDate}(B))$

 $\rho_{user_id,paymentDate}(A) \times CryptoHistories$

 $E =_{cryptoid,user_id,paymentDate} \mathcal{F}_{\max(Date)}(\sigma_{Date < paymentDate}(D))$

 $X =_{user_id,paymentDate} \mathcal{F}_{\texttt{Sum}(amount \times price)astotalValue}((C \times WalletHistories))$

 $\bowtie_{user_id=user_id \land paymentDate=paymentDate} E \bowtie CryptoHistories)$

 $\bowtie_{user_id=user_id \land paymentDate=paymentDate} Online_Payments$

 $\mathcal{F}_{\texttt{CountUnique(user_id)}}(\sigma_{onlineamount \geq \frac{1}{5}totalValue}(X))$

٣.٢. پاسخ به سوالات

۳.۲.۱۰ سوال ۱۰

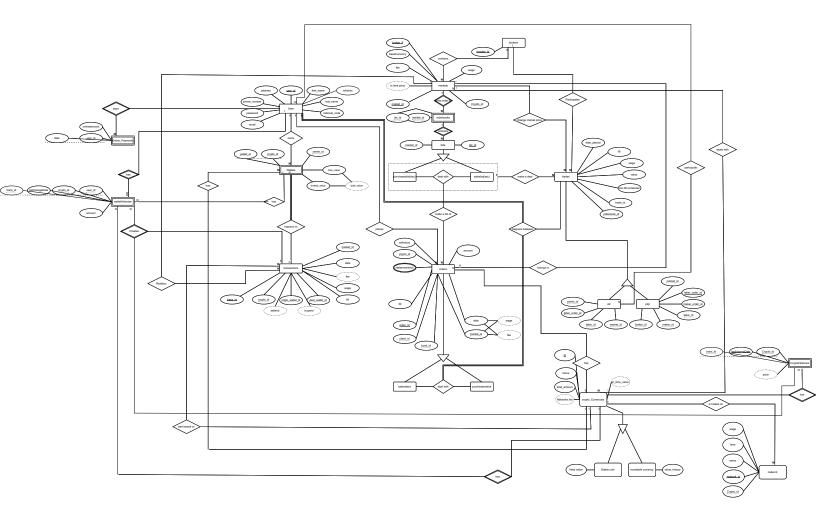
 $A = \rho_{cryptoid,price,totalSell}[cryptoid,price\mathcal{F}_{\texttt{Sum}(\texttt{amount})}((Cryptocurrency \times prices) \\ \bowtie_{Cryptocurrency.id=sellOrders.cryptoid} sellOrders)]$ $B = \rho_{cryptoid,price,totalSell}[cryptoid,price\mathcal{F}_{\texttt{Sum}(\texttt{amount})}((Cryptocurrency \times prices) \\ \bowtie_{Cryptocurrency.id=purchaseOrders.cryptoid} purchaseOrders)]$

 $A \cup B$

${ m ER}$ ضمیمه: تصویر دیاگرام

در انتهای فایل، ضمیمهی تصویر دیاگرام مربوطه آمده است.

در صورتی که در مشاهده ی این تصویر مشکل دارید، فایل PDF را با مرورگرهای Edge یا Ptrome باز نمایید.



کلیت فاز دوم پروژه

۵.۱ شرح

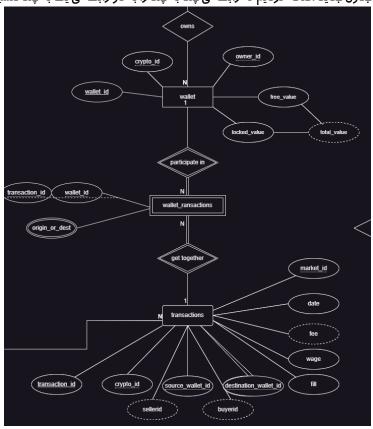
ما در این فاز از پروژه چهار تغیر در نموار فاز قبلی خود ایجاد کردیم که به ترتیب عبارتند از بهینه کردن نمودار برای طراحی دیتابیسَ، ایجاد دیتابیس، نرمال سازی و ایندکس کردن دیتا بیس و در نهایت انحام هشت جستوجو در دیتابیس.

تبدیل نمودارهای فاز اول، به نمودارهای منطبق با SQL

۶.۱ چهار تغیر در نمودار برای بهینه سازی

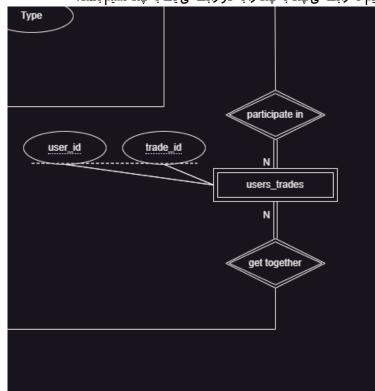
۶.۱.۱ رابطه ی چند به چند بین کیف پول و تراکنشها

از انحایی که در هر تراکنش دو کیف پول استفاده میشد و هر کیف پول در چندین تراکنش شرکت میکرد، یک جدول جدید اضافه کردیم که رابطه ی چند به چند را به دو رابطه ی یک به چند تقسیم کند.



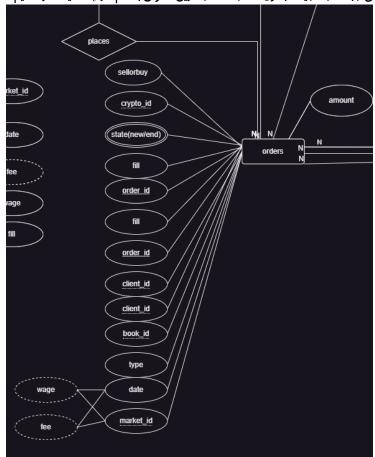
۶.۱.۲ رابطه ی چند به چند بین کاربرها و تبادل ها

از انحایی که هر تبادل از دو کاربر و هر کاربر در چندین تبادل شرکت میکرد، یک جدول جدول جدید اضافه کردیم که رابطه ی چند به چند را به دو رابطه ی یک به چند تسیم بکمد.



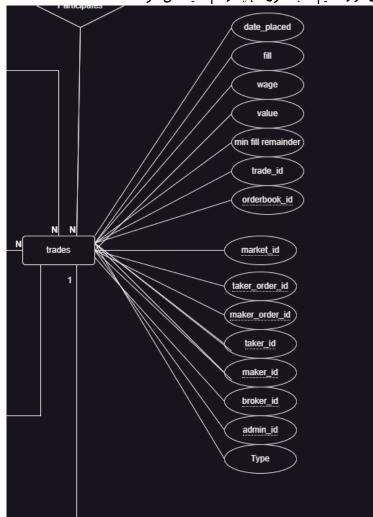
۶.۱.۳ رابطه ی اسپیسیفیکیشن در سفارشات

در فاز قبلی سفارشات به دو دستهی سفارشت خرید و سفارشات فروش تقسیم میشدند که ما در این فاز ای رابطه را در یک جدول سفارشات از طریق ستونی به نام typ و ناده ایم.



۶.۱.۴ رابطه ی جنرالیزیشن در تبادلها

در فاز قبلی تبادلها شامل دو نوع p2p و otc میشدند که ما در این فاز آن دو نوع تبادل را در یک جدول تبادل قرار دادیم که با ستون type از هم تفکیک می شوند.



ساخت پایگاه داده

بر اساس نمودار بخش قبل دو فایل SQL قرار دادیم که در یکی دستورات ایجاد جدولها و دیگری تست کیس برای هر جدول ایجاد شده و در مسیر $\mathrm{Phase}2/\mathrm{SQL}\,\,\mathrm{Files}$ قرار داده شده است.

فصل ۸ بهبود پایگاه داده

۸.۱ نرمالتر سازی

در این بخش ما تمام جداول پایگاه دادهی خود را به فرم نرمال در اوردیم و تغیرات نمودار و دستورات ایجاد پایگاه داده را در دو فایل normalized_sqlform_Integrated.drawio و Normalized Create Tables.sql در مسیر Phase2/Normalize Files در مسیر

حذف crypto id از transactions

transactions(<u>transaction_id</u>, crypto_id, source_wallet_id,

destination_wallet_id, fill, wage, date, market_id)

 $F.D = \{transaction_id \rightarrow all\ attributes, market_id \rightarrow crypto_id\}$

non prime به یک non prime attribute از انحایی که در $market_id \rightarrow crypto_id$ به attribute دیگر اشاره کرده این دیپندنسی را باید در یک جدول دیگر قرار دهیم تا از دومین فرم نرمال به سومین فرم نرمال انتقال پیدا کنیم.

 $transactions(transaction_id, source_wallet_id, destination_wallet_id, fill, wage, date, market_id)$

 $F.D = \{transaction_id \rightarrow all\ attributes\}$

 $R(market_id, crypto_id)$

 $F.D = \{market_id \rightarrow crypto_id\}$

حال دو جدول ما دارای سومین فرم نرمال هستند که همانطور که میبینید جدول ${
m R}$ زیر مجموعه ای از جدول Markets در پایگاه داده اصلی میباشد و نیازی به ساختن جدول اضافه نیست.

sales_lists_id , purchase_list_id از sales_lists_id , purchase_list_id

 $orders(\underline{order_id}, sales_lists_id, purchase_lists_id, is_sell, state, fill, client_id,$

 $date, market_id, amount)$

 $F.D = \{order_id \rightarrow all\ attributes, (market_id, is_sell) \rightarrow (sales_lists_id, purchase_lists_id)\}$

 $non\ prime$ دو $(market_id, is_sell) o (sales_lists_id, purchase_lists_id)$ دو $non\ prime\ attribute$ به دو attribute به دو $non\ prime\ attribute$ به دو $non\ prime\ attribute$ به دو $non\ prime\ attribute$ ما سومین فرم نرمال نباشد و ما باید ان را به یک جدول دیگر انتقال بدهیم.

ما مىتوانيم $(market_id, is_sell) o (sales_lists_id, purchase_lists_id)$ ما مىتوانيم $(market_id, is_sell) o purchase_lists_id)$ و $(market_id, is_sell) o sales_lists_id$ و $(market_id, is_sell) o sales_lists_id$ بشكانيم و با فرض اينكه $(market_id, is_sell)$ به دو مقدار مى باشد، دو جدول براى روابط بالا بسازيم بافرض اينكه $(market_id, is_sell)$

orders(order_id, is_sell, state, fill, client_id, date, market_id, amount)

 $F.D = \{order_id \rightarrow all \ attributes\}$

 $is_sell == TRUE : sale_table(\underbrace{market_id}, sales_lists_id)$ $F.D = \{market_id \rightarrow sales_lists_id\}$

 $is_sell == FALSE : purchase_table(market_id, purchase_lists_id)$

 $F.D = \{market_id \rightarrow purchase_lists_id\}$

همانطور که می دانیم دو جدول جدید ایجاد شده هر دو زیر مجموعهای از جدول Orderbooks میباشند و ما فقط باید دو ستون از جدول سفارشات حذف کنیم.

۸.۱.۳ نرمال کردن حدول ۸.۱.۳

index ۸.۲

برای سه جدول خود index قرار دادیم تا در جستار ها به ما کمک بکند.

۸.۲.۱ ایندکس تاریخ بر روی تبادلها

از انحایی که ما نیاز داریم تا قیمت لحظهای هر بازار را بر اساس اخرین تبادل ثبت شده حساب کنیم. مرتب کردن این حدول بر اساس تاریخ به محاسبهی قیمت بازار بسیار کمک میکند.

CREATE INDEX IF NOT EXISTS date placed idx ON trades(date placed);

INDEX .٨.۲ ها

۸.۲.۲ ایندکس کیف پول بر روی تراکنشها

از انحایی که ما نیازمند محاسبهی موجودی کیف پول هر کاربر هستیم پس بهتر است تراکنش های هر کیف پول را مرتب و درکنار هم در جدول تبادل ها قرار دهیم.

```
CREATE INDEX IF NOT EXISTS walle_id_idx
    ON transactions(source_wallet_id);
```

۸.۲.۳ ایندکس قیمت بر روی سفارشها

از انحایی که تر تبادل کم قیمتترین سفارش فروش مورد استفاده قرار میگیرد بهتر است که بر اساس قیمت سفارشات خود را مرتب کنیم تا در هر لحظه دسترسی سریعی به کم قیمتترین پیشنهاد فروش داشته باشیم.

CREATE INDEX IF NOT EXISTS amount_idx ON orders(amount);