



دانشگاه صنعتی شریف

## پروژهی صرافی ارز دیجیتال: پایگاه داده - فاز اول

استاد: دکتر مهدی آخی

شماره تیم: ۱۴

محمد جعفری پور  
۴۰۱۱۰۵۷۹۷

محمد امین حیدری  
۴۰۱۱۷۰۵۵۳

مانی ابراهیمی  
۴۰۱۱۷۰۴۹۱

بهار ۱۴۰۳



## فهرست مطالب

۵	۱	کلیت فاز اول پروژه
۵	۱.۱	شرح
۵	۱.۲	تقسیم وظایف
۷	۲	دیاگرام های ER
۷	۲.۱	شرح
۷	۲.۲	توضیح هر موجودیت
۷	۲.۲.۱	User
۷	۲.۲.۲	Wallet
۷	۲.۲.۳	Transactions
۸	۲.۲.۴	Orders
۸	۲.۲.۵	Trades
۸	۲.۲.۶	OrderBooks
۸	۲.۲.۷	Markets
۸	۲.۲.۸	Brokers
۹	۲.۲.۹	CryptoCurrency
۹	۲.۲.۱۰	Network
۹	۲.۲.۱۱	Online Payments
۹	۲.۲.۱۲	Wallet History
۹	۲.۲.۱۳	Crypto Histories
۱۱	۳	سوالات جبر رابطه ای
۱۱	۳.۱	شرح
۱۱	۳.۲	پاسخ به سوالات
۱۱	۳.۲.۱	سوال ۱
۱۱	۳.۲.۲	سوال ۲
۱۱	۳.۲.۳	سوال ۳
۱۱	۳.۲.۴	سوال ۴
۱۲	۳.۲.۵	سوال ۵
۱۲	۳.۲.۶	سوال ۶
۱۲	۳.۲.۷	سوال ۷
۱۲	۳.۲.۸	سوال ۸
۱۲	۳.۲.۹	سوال ۹
۱۳	۳.۲.۱۰	سوال ۱۰

۱۵	۴	ضمیمه: تصویر دیاگرام ER
۱۷	۵	کلیت فاز دوم پروژه
۱۷	۵.۱	شرح
۱۹	۶	تبدیل نمودارهای فاز اول، به نمودارهای منطبق با SQL
۱۹	۶.۱	چهار تغییر در نمودار برای بهینه سازی
۲۰	۶.۱.۱	رابطه ی چند به چند بین کیف پول و تراکنش ها
۲۱	۶.۱.۲	رابطه ی چند به چند بین کاربرها و تبادل ها
۲۲	۶.۱.۳	رابطه ی اسپسیفیکیشن در سفارشات
۲۳	۶.۱.۴	رابطه ی جنرالیزیشن در تبادل ها
۲۵	۷	ساخت پایگاه داده
۲۷	۸	بهبود پایگاه داده
۲۷	۸.۱	نرمال تر سازی
۲۷	۸.۱.۱	حذف crypto_id از transactions
۲۸	۸.۱.۲	حذف list_id ها از orders
۲۸	۸.۱.۳	حذف maker_id, taker_id از trades
۲۸	۸.۲	index ها
۲۸	۸.۲.۱	ایندکس تاریخ بر روی تبادل ها
۲۸	۸.۲.۲	ایندکس کیف پول بر روی تراکنش ها
۲۸	۸.۲.۳	ایندکس قیمت بر روی سفارش ها

## فصل ۱

# کلیت فاز اول پروژه

### ۱.۱ 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<sup>۱</sup> قابل مشاهده است.

### ۱.۲ تقسیم وظایف

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

نام کوتاه	نام کامل	شماره دانشجویی
Mani	مانی ابراهیمی	۴۰۱۱۷۰۴۹۱
Mamadamin	محمدامین حیدری	۴۰۱۱۷۰۵۵۳
Mamal	محمد جعفری‌پور	۴۰۱۱۰۵۷۹۷

جدول ۱.۱: جدول اعضای تیم در جدول تقسیم وظایف

جدول تقسیم وظایف نیز از اینجا<sup>۲</sup> قابل مشاهده است.

---

<sup>۱</sup>در صورتی که لینک برای شما کار نمی‌کند، از آدرس <https://github.com/maniebra/dbms-exchange-project> استفاده نمایید.

<sup>۲</sup>در صورتی که این لینک برای شما کار نمی‌کند، می‌توانید از آدرس [https://docs.google.com/spreadsheets/d/1x1Guh4HTWLyG9GTomZEsp5cjIGez9m9Day3bS\\_kgM/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1x1Guh4HTWLyG9GTomZEsp5cjIGez9m9Day3bS_kgM/edit?usp=sharing) استفاده نمایید.



## فصل ۲

# دیاگرام های ER

### 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 ۲.۲.۱

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 ۲.۲.۲

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

#### Transactions ۲.۲.۳

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 ارزش 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 Market\_id و بدست آوردن ارزش پایه‌ی آن مارکت و قیمت لحظه‌ای آن ارزش پایه به ریال محاسبه می‌شود.

## Orders ۲.۲.۴

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 ۲.۲.۵

موجودیت تبادل ها یا همان 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 OTC و P2P را تشکیل داده اند. همچنین این موجودیت دارای یک شناسه برای هر تبادل می باشد. صفت min\_fill\_remainder به این صورت عمل می کند که حجم باقی مانده ی کمینه ی دو سفارش خرید و فروش را ذخیره می کند.

## OTC

شامل ID ادمین و مشتری می باشد که بوسیله ی شناسه ی Market به بازار مربوطه متصل شده است.

## P2P

شامل دو ID و OrderID خریدار و فروشنده یا همان maker و taker می باشند که به وسیله ی شناسه ی صرافی یا همان Broker\_ID به صرافی مربوطه متصل شده اند.

## OrderBooks ۲.۲.۶

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 زیرمجموعه ی 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 ۲.۲.۷

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 ۲.۲.۸

موجودیت صرافی ها یا همان Brokers، که دارای صفات گفته شده از جمله شناسه و سایر موارد است. این موجودیت برای ذخیره اطلاعات 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.



### ۲.۲.۹ CryptoCurrency

موجودیت کریپتو ها یا CryptoCurrency ارز هایی اند که در سایت وجود دارند و توسط افراد مبادله میشوند. این ارز ها ممکن است قیمت ثابت Stable coin باشند و یا قیمت آنها هر لحظه عوض شود nonstable Currency.

### ۲.۲.۱۰ Network

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

### ۲.۲.۱۱ Online Payments

تاریخچه ی تمامی واریزی های هر کاربر، مقدار آن و زمان انجام شده است.

### ۲.۲.۱۲ Wallet History

تاریخچه ای از تغییرات میزان هر کیف پول است و هر تراکنشی برای دو کیف پول یک Wallet History جدید می سازد.

### ۲.۲.۱۳ Crypto Histories

تاریخچه ی تغییرات قیمت یک رمزارز است که زمان آن تغییر و مقدار و قیمت آن در آن زمان (قیمت همان قیمت لحظه ای مارکت است) نشان می دهد. با انجام هر تراکنش یک CryptoHistory جدید ایجاد می شود چرا که قیمت لحظه ای ارز تغییر می کند.



## فصل ۳

# سوالات جبر رابطه‌ای

### ۳.۱ شرح

در این بخش پاسخ به ۱۰ سوال جبر رابطه‌ای<sup>۱</sup> آمده است.

### ۳.۲ پاسخ به سوالات

#### ۳.۲.۱ سوال ۱

$$\Pi_{\text{market\_id}, \text{fee}}(\text{Transactions} \bowtie_{\text{Transactions.market\_id}=\text{Market.market\_id} \wedge \text{Transactions.date}=\text{date}} (\text{market\_id} \mathcal{F}_{\max(\text{date})} (Market \bowtie_{\text{Market.market\_id}=\text{Transactions.market\_id}} \text{Transactions})))$$

#### ۳.۲.۲ سوال ۲

$$\text{owner\_id} \mathcal{F}_{\text{Sum}(\text{total\_value} \times \text{in\_time\_price})} [Wallets \bowtie_{\text{Market.market\_id}=id} Markets]$$

#### ۳.۲.۳ سوال ۳

$$\text{crypto\_id} \mathcal{F}_{\text{Count}(\text{order\_id})} [\sigma_{\text{fill}=\text{"false"}} (Orders)]$$

#### ۳.۲.۴ سوال ۴

$$A = \rho_{\text{user\_id}, \text{total}} [\text{owner\_id} \mathcal{F}_{\text{Sum}(\text{fee})} \text{as totalSell} (\text{Transactions} \bowtie_{\text{Transactions.origin\_wallet\_id}=\text{wallets.id}} \text{Wallet})]$$

$$B = \rho_{\text{user\_id}, \text{total}} [\text{owner\_id} \mathcal{F}_{\text{Sum}(\text{fee})} \text{as totalBuy} (\text{Transactions} \bowtie_{\text{Transactions.dest\_wallet\_id}=\text{wallets.id}} \text{Wallet})]$$

$$\text{user\_id} \mathcal{F}_{\text{Sum}(\text{Total})}$$

---

Relational Algebra<sup>۱</sup>

## سوال ۳.۲.۵

$$A =_{user\_id, cryptoid} \mathcal{F}_{\text{Count}(Transactions.id)}(Users \times Cryptocurrency) \bowtie_{users.user\_id=Transactions.SellerID} Transactions$$

$$B =_{user\_id, cryptoid} \mathcal{F}_{\text{Count}(Transactions.id)}(Users \times Cryptocurrency) \bowtie_{users.user\_id=Transactions.BuyerID} Transactions$$

$$_{user\_id, cryptoid} \mathcal{F}_{\text{mathtt{Sum}(TotalCount)}}(\rho_{user\_id, cryptoid/TotalCount(A)} \cup \rho_{user\_id, cryptoid/TotalCount(B)})$$

## سوال ۳.۲.۶

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

## سوال ۳.۲.۷

$$\begin{aligned} A &= \Pi_{cryptoid, in\_time\_price}(Cryptocurrency) \\ B &=_{cryptoid} \mathcal{F}_{\text{mathtt{max}(Date)asDate}}(\sigma_{Transactions.Date-Now() \leq "0000-00-30-00:00:00"}(Transactions \times Cryptocurrency)) \\ C &= \Pi_{cryptoid, fee}[Cryptocurrency \bowtie_{Cryptocurrency.id=Transactions.cryptoid} (Transactions \bowtie B)] \\ &\Pi_{cryptoid, in\_time\_price-fee}(A \bowtie C) \end{aligned}$$

## سوال ۳.۲.۸

$$\begin{aligned} A &=_{owner\_id} \mathcal{F}_{\text{Sum}(Total\_value)assum}(Wallets) \\ B &= \Pi_{owner\_id, cryptoid, Total\_value}(Wallets) \\ &_{cryptoid} \mathcal{F}_{\text{count}(owner\_id)}[\sigma_{percentage \geq 0.05}(\rho_{cryptoid, owner\_id, percentage}[ \\ &\Pi_{cryptoid, owner\_id, \frac{Total\_value}{Sum}}(A \bowtie B)])] \end{aligned}$$

## سوال ۳.۲.۹

$$\begin{aligned} A &= \Pi_{user\_id, Date}(\sigma_{Date-Now() \leq "0000-00-30;00:00:00"}(Online\_Payments)) \\ B &= \rho_{user\_id, paymentDate}(A) \bowtie WalletHistories \\ C &=_{cryptoid, user\_id, paymentDate} \mathcal{F}_{\text{Max}(Date)}(\sigma_{Date < paymentDate}(B)) \\ &\rho_{user\_id, paymentDate}(A) \times CryptoHistories \\ E &=_{cryptoid, user\_id, paymentDate} \mathcal{F}_{\text{max}(Date)}(\sigma_{Date < paymentDate}(D)) \\ X &=_{user\_id, paymentDate} \mathcal{F}_{\text{Sum}(amount \times price)astotalValue}((C \times WalletHistories) \\ &\bowtie_{user\_id=user\_id \wedge paymentDate=paymentDate} E \bowtie CryptoHistories) \\ &\bowtie_{user\_id=user\_id \wedge paymentDate=paymentDate} Online\_Payments \end{aligned}$$

$$\mathcal{F}_{\text{CountUnique}(user\_id)}(\sigma_{onlineamount \geq \frac{1}{5} totalValue}(X))$$

۳.۲.۱۰ سوال ۱۰

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

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

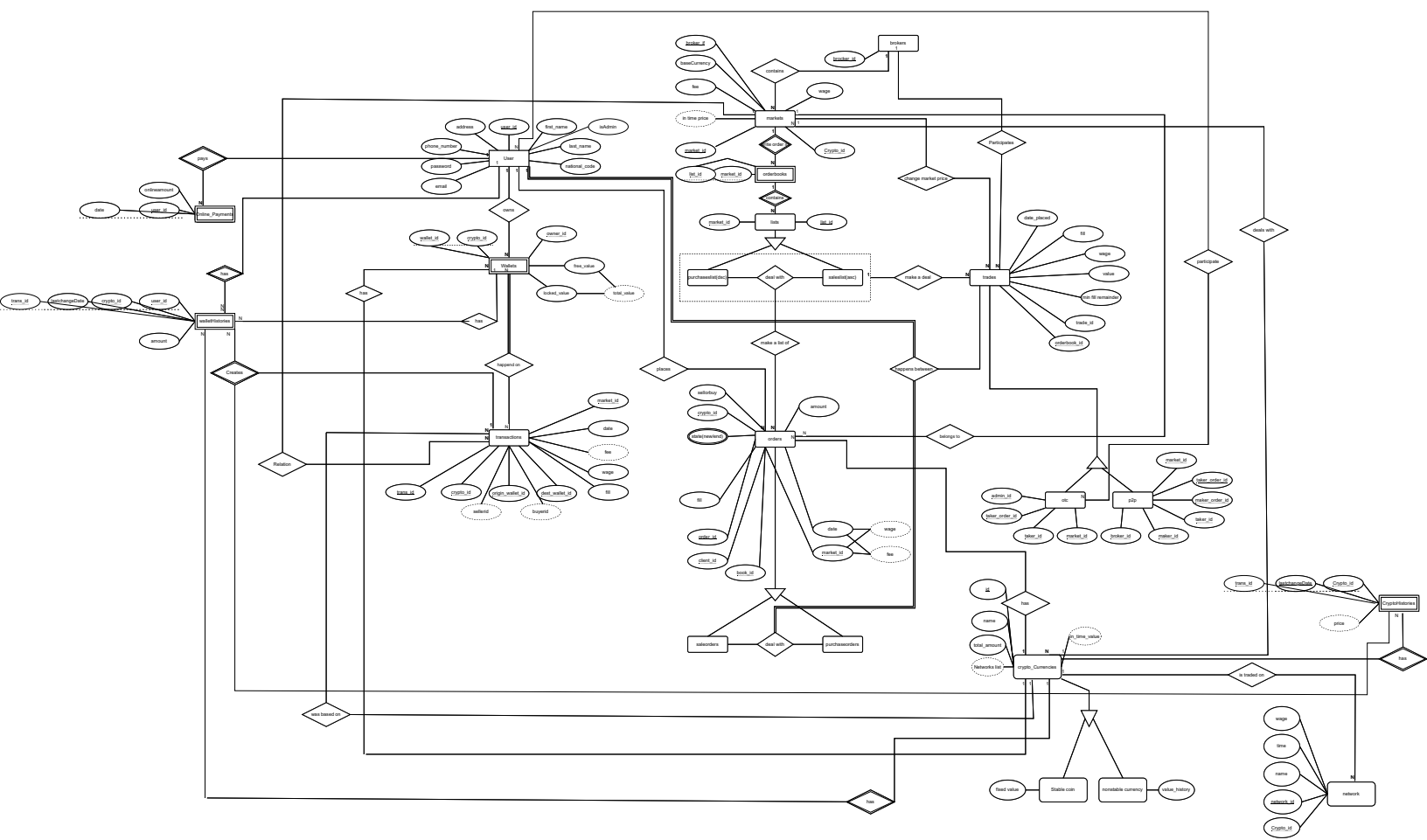
$$A \cup B$$



## فصل ۴

# ضمیمه: تصویر دیاگرام ER

در انتهای فایل، ضمیمه‌ی تصویر دیاگرام مربوطه آمده است.  
در صورتی که در مشاهده‌ی این تصویر مشکل دارید، فایل PDF را با مرورگرهای Chrome یا Edge باز نمایید.





## فصل ۵

# کلیت فاز دوم پروژه

### ۵.۱ شرح

ما در این فاز از پروژه چهار تغییر در نمودار فاز قبلی خود ایجاد کردیم که به ترتیب عبارتند از بهینه کردن نمودار برای طراحی دیتابیس، ایجاد دیتابیس، نرمال سازی و ایندکس کردن دیتا بیس و در نهایت انجام هشت جستجو در دیتابیس.



## فصل ۶

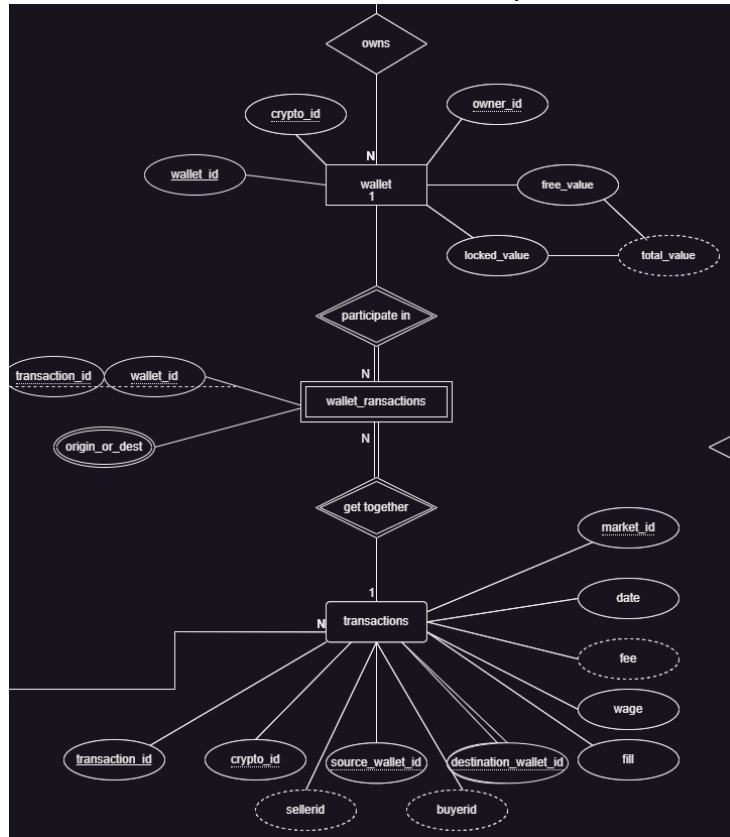
# تبدیل نمودارهای فاز اول، به نمودارهای منطبق با SQL

### ۶.۱ چهار تغییر در نمودار برای بهینه سازی

در این بخش نمودار خود را تغییر دادیم تا مناسب درست کردن SQL باشد.

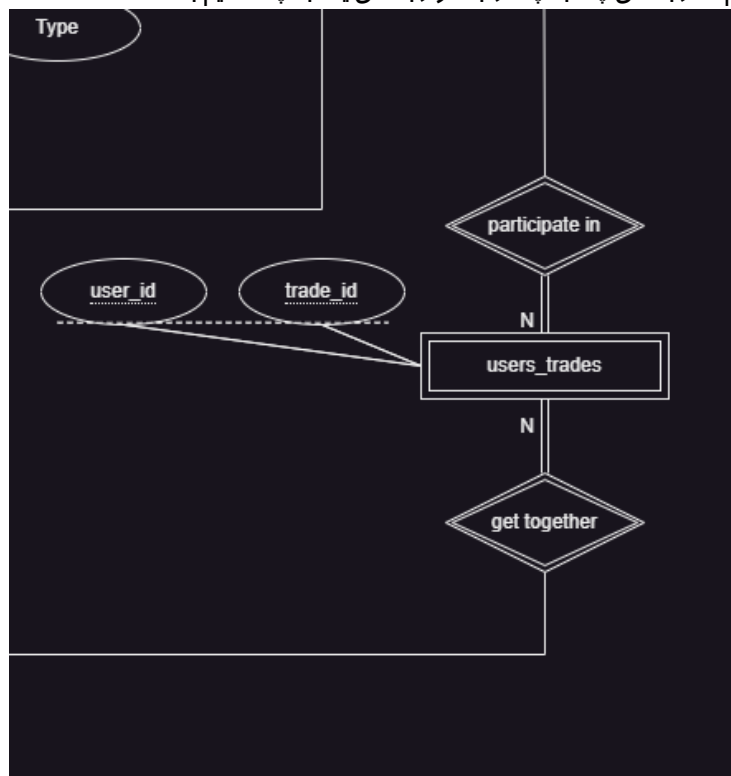
### ۶.۱.۱ رابطه ی چند به چند بین کیف پول و تراکنش ها

از آنجایی 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.



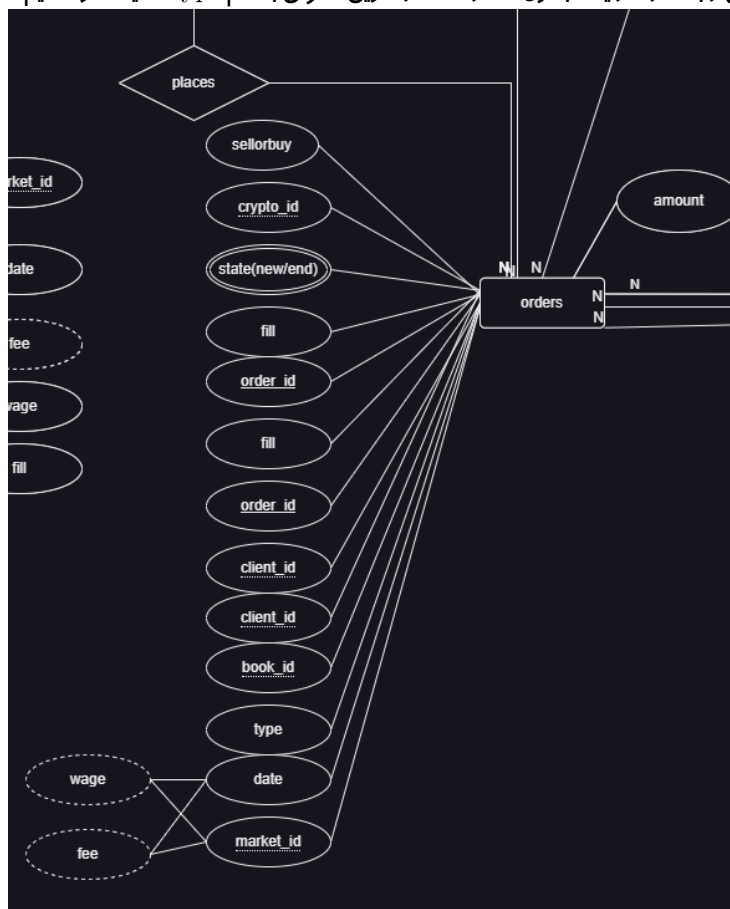
### ۶.۱.۲ رابطه ی چند به چند بین کاربرها و تبادلاتها

از آنجایی که هر تبادل از دو کاربر و هر کاربر در چندین تبادل شرکت میکند، یک جدول جدید اضافه کردیم که رابطه ی چند به چند را به دو رابطه ی یک به چند تقسیم بکند.



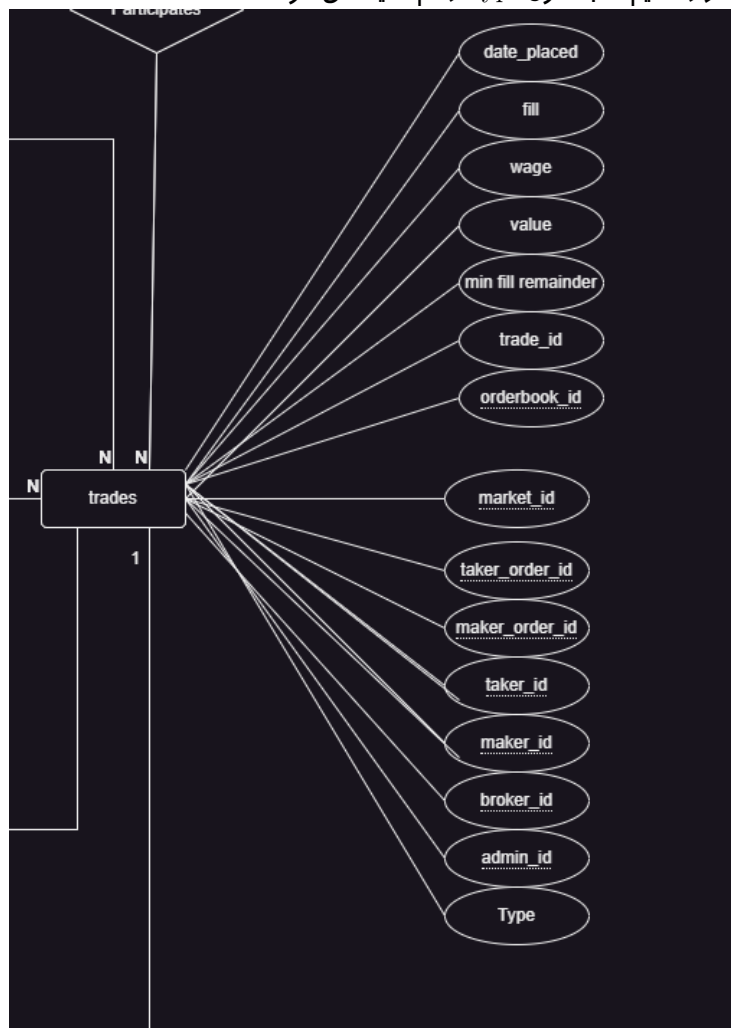
## ۶.۱.۳ رابطه‌ی اسپسیفیکیشن در سفارشات

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 type تفکیک کرده ایم.



#### ۶.۱.۴ رابطه ی جنرالیزیشن در تبادل ها

در فاز قبلی تبادل ها شامل دو نوع p2p و otc می شدند 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.







## فصل ۷

# ساخت پایگاه داده

بر اساس نمودار بخش قبل دو فایل SQL قرار دادیم که در یکی دستورات ایجاد جدول ها و دیگری تست کیس برای هر جدول ایجاد شده و در مسیر Phase2/SQL 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 آوردیم و تغییرات نمودار و دستورات ایجاد پایگاه داده را در دو فایل `normalized_sqlform_Integrated.drawio` و `Normalized` `Create Tables.sql` در مسیر `Phase2/Normalize Files` قرار دادیم.

#### ۸.۱.۱ حذف `crypto_id` از `transactions`

$transactions(transaction\_id, crypto\_id, source\_wallet\_id,$   
 $destination\_wallet\_id, fill, wage, date, market\_id)$

$$F.D = \{transaction\_id \rightarrow all\ attributes, market\_id \rightarrow crypto\_id\}$$

از آنجایی که در  $market\_id \rightarrow crypto\_id$  یک `non prime attribute` به یک `non prime` از attribute دیگر اشاره کرده این دپندنسی 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 `R` زیر مجموعه ای از جدول `Markets` در پایگاه داده اصلی میباشد و نیازی به ساختن جدول اضافه نیست.

**۸.۱.۲ حذف list\_id ها از orders****۸.۱.۳ حذف maker\_id, taker\_id از trades****۸.۲ index ها**

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

**۸.۲.۱ ایندکس تاریخ بر روی تبادل ها**

از انتحایی که ما نیاز داریم تا قیمت لحظه ای هر بازار را بر اساس آخرین تبادل ثبت شده حساب کنیم. مرتب کردن این جدول بر اساس تاریخ به محاسبه ی قیمت بازار بسیار کمک می کند.

```
CREATE INDEX IF NOT EXISTS date_placed_idx ON trades(date_placed);
```

**۸.۲.۲ ایندکس کیف پول بر روی تراکنش ها**

از انتحایی که ما نیازمند محاسبه ی 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 سفارش ها**

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

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