# Analýza softwarového projektu

Návrh aplikace pro kryptoměnový mining pool

Michal Ručka

14. 3. 2023

# Obsah

# Popis změn v dokumentu

| Jméno | Datum | Typ úpravy | Verze |
|---|---|---|---|
| Michal Ručka | 13. 3. 2023 | Vytvoření dokumentu, tvorba osnovy a rozpracování zadání | 1.0 |
| Michal Ručka | 14. 3. 2023 | Pokračování ve tvorbě dokumentu | 1.1 |
| Michal Ručka | 14. 3. 2023 | Oprava chyb, rozpracování UC části dokumentu | 1.2 |
| Michal Ručka | 15. 3. 2023 | Dokončení use case části, oprava chyb | 1.3 |
| Michal Ručka | 19. 3. 2023 | Vložení use case diagramu | 1.4 |
| Michal Ručka | 1. 4. 2023 | Oprava use case diagramu | 1.4.1 |
| Michal Ručka | 1. 4. 2023 | Vložení class diagramu | 1.5 |
| Michal Ručka | 19. 4. 2023 | Úprava class diagramu | 1.6 |
| Michal Ručka | 26. 4. 2023 | Přidány sekvenční diagramy | 1.7 |
| Michal Ručka | 29. 4. 2023 | Přidány aktivitní a stavové diagramy | 1.8 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 1 Úvodní informace

## 1.1 Zadání od zákazníka

Vytvořte aplikaci pro kryptoměnový mining pool. Podstatou aplikace je propojit výkonnost těžebních strojů jednotlivých uživatelů.

Aplikace bude zasílat burze informace o hardwarovém vybavení stroje od uživatele. Z těchto dat dále vypočítá, jak velká je jeho těžební výkonnost (dále jen hashrate) a porovná ji s ostatními uživateli. Tyto data budou použity také proto, aby byla vyměřena možná orientační odměna za těžbu.

Pokud bude mít uživatel zapnutou aplikaci, stane se součástí velkého superpočítače (mining poolu), který poběží na stranách uživatelů této aplikace. Tímto konáním vznikne zákazníkovi nárok na část ze zisku, pokud bude úspěšně vytěžen blok kryptoměn, který obsahuje odměnu.

## 1.2 Důvod, okolnosti zavedení řešení

Propojením jednotlivých uživatelů vzniká jeden velký superpočítač (mining pool), který společně na všech spuštěných těžebních strojích těží kryptoměny. Propojením dojde ke zvýšení celkového hashrate mining poolu, tudíž se razantně zvýší šance na vytěžení bloku kryptoměn, který obsahuje odměnu. Mining pool obecně umožňuje při těžbě získat určitý zlomek z odměny také uživatelům, kteří by bez tohoto spojení pravděpodobně žádné odměny nedosáhli. Ovšem je nutné dbát na to, že každý uživatel má jinak výkonný počítač či stroj, tudíž má jiný hashrate. Toto znamená, že nároky na odměny jsou rozdílné pro každého uživatele.

# 2 Systémové požadavky

## 2.1 F – Funkčnost (Functionality)

**Aplikace** musí umět přidávat, upravovat a odstraňovat uživatele.
**Aplikace** musí být schopna získat informace o hardwaru uživatele.
**Aplikace** musí umět vypočítat odhadovaný zisk uživatele na základě jeho hardware vybavení.
**Aplikace** musí být schopna připojit či odpojit zákazníkův stroj k mining poolu.
**Aplikace** musí umět vytvořit mining pool propojením jednotlivých uživatelů.
**Aplikace** musí být schopna navázat a udržet kontakt s aktuálním stavem kryptoměnového blockchainu a spustit na něm těžbu.
**Aplikace** musí umět efektivně přiřazovat úkoly jednotlivým částem mining poolu.
**Aplikace** musí umět přidávat, upravovat a odstraňovat kryptoměnové adresy uživatelů.
**Aplikace** musí poskytnout možnost uschování či výběr kryptoměn.

## 2.2 U – Vhodnost k použití (Usability)

**Aplikace** umožní uživateli výběr částí jeho stroje, které se propojí s mining poolem.
**Aplikace** umožní uživateli nastavit automatické zapnutí či vypnutí těžby dle jeho libovolného nastavení.
**Aplikace** umožní uživateli komunikovat s ostatními uživateli pomocí textových zpráv.
**Aplikace** zobrazí uživateli aktuální statistiky mining poolu.

## 2.3 R – Spolehlivost (Reliability)

**Systém** musí být schopen odolat hackerským útokům jak zvenčí, tak ze stran uživatele.
**Systém** musí vždy umožnit uživateli výběr kryptoměn.
**Systém** zajistí šifrované připojení uživatele k mining poolu.
**Systém** bude pravidelně zálohovat veškerá data aplikace.
**Systém** musí být při těžbě schopen udržet propojení až s 2048 různými uživateli.
**Systém** rezervuje na dobu 3 minut jedno místo pro uživatele, kterému během těžby vypadne internet či se z zní neočekávaně odpojí.
**Systém** musí veškeré úkony spojené s údržbou či dalším vývojem provádět pouze v době mimo hlavní obchodní hodiny amerických burz (tj. v čase mimo 9:30ET až 16:00ET), výhradně tedy o víkendu.

## 2.4 P – Výkon (Performance)

**Doba odezvy** systému na běžně prováděné akce v rozhraní aplikace musí být do 1 sekundy.
**Doba odezvy** systému na žádost o připojení k mining poolu, či odpojení od něj, musí být maximálně do 15 sekund.
**Doba odezvy** systému na žádost o odeslání kryptoměn na externí peněženku musí být do 5 sekund.

## 2.5 S – Schopnost údržby (Supportability)

**Aplikace** je tvořena pro koncové uživatele s operačním systémem linux, ale musí být schopna fungovat také na operačních systémech windows.
**Aplikace** musí obsahovat sadu testů, které budou pravidelně testovat funkčnost všech klíčových funkcí.
**Aplikace** bude mít možnost se na mining pool připojit také v době, kdy bude probíhat údržba. Vyjma tohoto připojení nebudou v dané době žádné další funkce dostupné.

# 3 Charakteristika aktérů a prostředí

## 3.1 Aktéři, uživatelé, role

### 3.1.1 Host

Má možnost nahlédnout bez registrace do aplikace a interagovat s ní. Má také možnost se na dobu maximálně 1h zapojit do procesu samotné těžby a tím si tak otestovat kompatibilitu aplikace se svým počítačem. Má limitované možnosti a nemá nárok na odměnu z úspěšně vytěžených bloků.

### 3.1.2 Těžař amatér

Tento uživatel má pouze jeden stroj. Má možnost být neomezeně součástí mining poolu a podílet se tak na těžbě. Tento uživatel má nárok na odměnu za úspěšně vytěžené bloky. Může si přidat v nastavení adresu své peněženky a provádět výběry kryptoměn z aplikace.

### 3.1.3 Těžař profesionál

Tento uživatel má více než jeden stroj a je mu umožněno si všechny tyto stroje v aplikaci propojit a vytvořit tak mini superpočítač, který se skládá pouze z jeho strojů. Má možnost tyto stroje, jakožto jeden celek, hromadně ovládat přes tuto aplikaci.

### 3.1.4 Správce

Má veškeré pravomoci týkající se těžařů. Může je také ale přidávat, mazat či upravovat. Může udělovat umlčení v textovém chatu. Může udělovat blokování na celou aplikaci, i včetně připojení se k mining poolu. Hlídá spokojenost a bezpečnost uživatelů. Tato role se uděluje pouze zaměstnancům.

### 3.1.5 Vývojář

Má veškeré pravomoci na aplikaci. Má přístup ke zdrojovému kódu a aktivně se podílí na vývoji aplikace. Je zodpovědný za plynulý chod aplikace. Provádí pravidelné testy, plánuje údržby a má pravomoc odstavit systém.

## 3.2 Externí systémy

Aplikace na těžbu kryptoměn je propojená s již existující burzou, ze které čerpá určitá data. Jedním z nich je např. KYC (Know Your Customer) ověření, které slouží jakožto verifikace zákazníka, aby se předešlo případnému praní špinavých peněz. Na této burze dále probíhá případná úschova či prodej získaných kryptoměn. Pro plné využívání této aplikace je potřeba mít účet na této burze.

# 4 Situace definující hranice systému

## 4.1 Ideální případ

Uživatel je zaregistrován na stránkách burzy. Aplikaci má uživatel staženou na svém počítači s Linuxem. Klient je stabilně připojen k internetu. Aktuální počet připojených uživatelů k mining poolu je menší než 2048. Během těžby dojde k úspěšnému vytěžení bloku, který obsahuje odměnu. Dojde k vyplacení odměny uživateli na jeho adresu.

## 4.2 Hraniční případ

### 4.2.1 Nestabilní připojení k internetu

Uživatel je zaregistrován na stánkách burzy. Aplikaci má uživatel staženou na svém počítači Linuxem, či s jiným operačním systémem, než je Linux. Klient má nestabilní či pomalé připojení k internetu, které znatelně ovlivňuje či snižuje maximální výkon jeho stroje. Aplikace provede automaticky restart připojení uživatele k mining poolu. Pokud restart nepomůže, aplikace navrhne uživateli odpojení od mining poolu.

### 4.2.2 Překročení maximálního počtu uživatelů

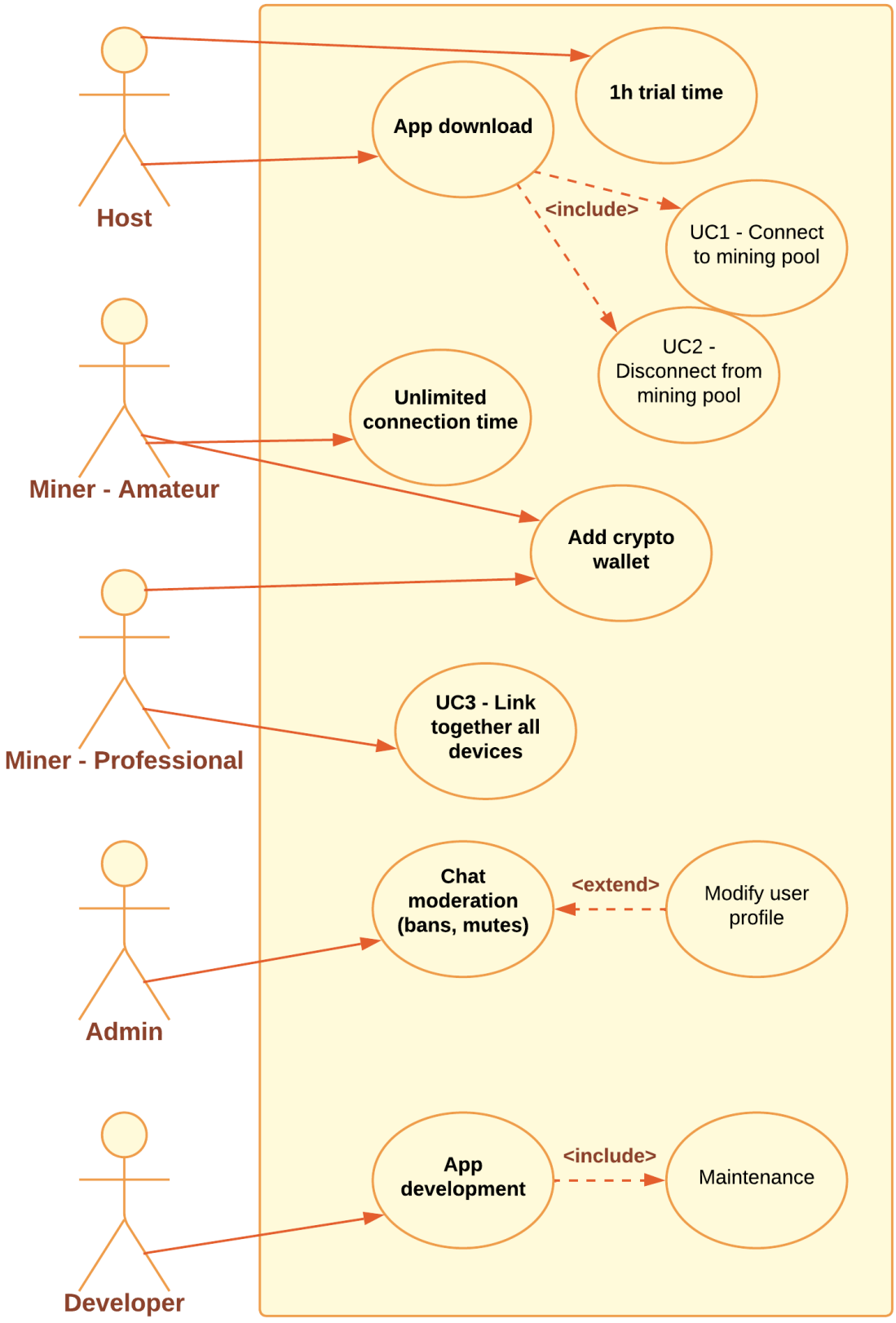
Uživatel je zaregistrován na stánkách burzy. Aplikaci má uživatel staženou na svém počítači. Klient je stabilně připojen k internetu. Aktuální počet připojených uživatelů k mining poolu je roven maximálnímu možnému počtu těžařů (2048). Uživatel, který má zájem se k mining poolu připojit, ale z kapacitních důvodů nemůže, je zařazen do řady. Tato řada představuje klasickou FIFO řadu, ve které se uživatelé řadí jeden za druhého a jakmile se uvolní slot na mining poolu, tak se na něj připojí uživatel, který se jako první připojil do dané řady.

## 4.3 Případ použití za hranou

Podstatou fungování tohoto mining poolu je internetové připojení, ať už uživatele, tak burzy. Aby se uživatel mohl propojit s mining poolem, je zapotřebí mít nejlépe stabilní internetové připojení. Pokud dojde k výpadku internetu, nebude se možné na tento mining pool připojit. Situace se dá vyřešit pouze opětovným připojením k internetu. Aplikace neumožňuje se na tento mining pool připojit bez přístupu k internetu.

# 5 Podrobný náhled na stavbu projektu

## 5.1 Use case diagram



## 5.2 UC1 – Připojení k mining poolu

a) **Název:** Připojení k mining poolu.
b) **Kontext:** Uživatel má zájem o připojení k mining poolu – je připraven těžit.
c) **Level zanoření:** Host, Těžař amatér, Těžař profesionál (1-3)
d) **Aktéři:** Host, těžař amatér, těžař profesionál
e) **Stakeholdeři či jiné osoby:** ---
f) **Vstupní podmínky:** Uživatel musí mít staženou aplikaci, která funguje jako prostředník k připojení na mining pool. Uživatel musí mít přístup k internetu.
g) **Výstupní podmínky:** Uživatel prostřednictvím aplikace naváže spojení s mining poolem a úspěšně se na něj připojí.
h) **Minimální výstup:** Systém při chybě zobrazí hlášku, která uživatele upozorní o neproběhlém propojení s mining poolem. Pokud se bude jednat o jednu z nejčastějších evidovaných chyb, tak hláška bude obsahovat také důvod nepropojení.
i) **Ideální výstup:** Propojení uživatele s mining poolem proběhne úspěšně a bez problémů. Uživateli se zobrazí hláška o úspěšném propojení.
j) **Hlavní scénář:**
    1. Uživatel spustí aplikaci.
    2. Uživatel najede do sekce „Join mining pool“ kde klikne na tlačítko „Join.“
    3. Uživateli se zobrazí tabulka s aktuálními statistikami mining poolu a také se mu zobrazí jeho odhadovaná odměna, kterou si vydělá za 24 hodin těžení.
    4. Uživatel si nastaví, jaké všechny části svého stroje / PC si chce nechat propojit s mining poolem.
    5. Uživatel klikne na tlačítko „Join.“
    6. Aplikace propojí uživatele s mining poolem.
    7. Uživateli se na obrazovce objeví hláška, která mu sdělí, zda propojení proběhlo úspěšně.
k) **Rozšíření:**
    1. Uživatel, který není přihlášen, nemá účet, nebo chce aplikaci pouze otestovat, bude vyzván na přihlášení, vytvoření si účtu, či popřípadě připojení se k mining poolu jakožto host.
    2. Uživatel, který se připojí na mining pool jakožto host, musí počítat se značným omezením funkčnosti aplikace a také s hodinovou zkušební dobou na mining poolu.

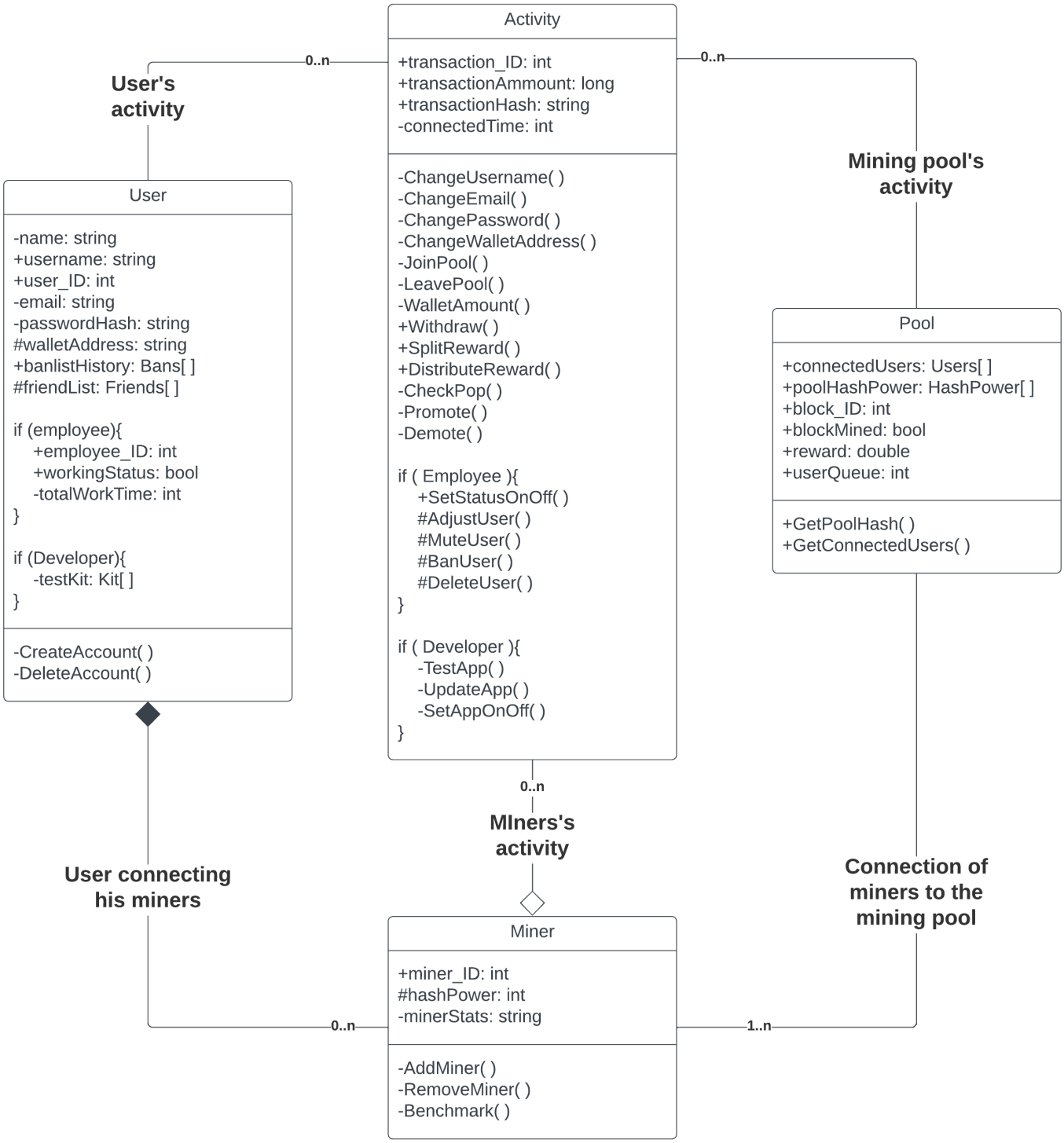
## 5.3 UC2 – Odpojení od mining poolu

a) **Název:** Odpojení od mining poolu.
b) **Kontext:** Uživatel se rozhodl, že chce zrušit propojení s mining poolem.
c) **Level zanoření:** Host, Těžař amatér, Těžař profesionál (1-3)
d) **Aktéři:** Host, těžař amatér, těžař profesionál
e) **Stakeholdeři či jiné osoby:** ---
f) **Vstupní podmínky:** Uživatel musí být nutně propojen s mining poolem a aktivně se podílet na těžbě kryptoměn.
g) **Výstupní podmínky:** Aplikace zpracuje požadavek o odpojení od mining poolu, a uživatele odpojí ihned poté, co dokončí jeho aktuální úkol, který má rozpracovaný.
h) **Minimální výstup:** Systém detekuje, že uživatelův stroj má aktuálně úkol, který nelze přesunout na někoho jiného či jej zrušit. Zobrazí tedy uživateli hlášku, ve které bude orientační časový interval, během kterého dojde k odpojení.
i) **Ideální výstup:** Systém detekuje, že uživatelův stoj nemá aktuálně žádný úkol, či vyčká několik málo sekund, než bude aktuální úkol dokončen a následně jej tedy odpojí.
j) **Hlavní scénář:**
    1. Uživatelův stroj je stabilně připojen k mining poolu a těží.
    2. Uživatel klikne na tlačítko „leave mining pool.“
    3. Aplikace přestane uživateli zasílat nové úkoly a vyčká, než se dokončí aktuální úkoly.
    4. Aplikace zobrazí uživateli odhadovanou dobu, po kterou je nutné nechat stroj ještě v provozu, aby dokončil prováděné operace.
    5. Aplikace zajistí, že v řádu několika sekund nastane situace, kdy bude možno uživatelův stroj bezpečně odpojit.
    6. Aplikace odpojí uživatele od mining poolu.

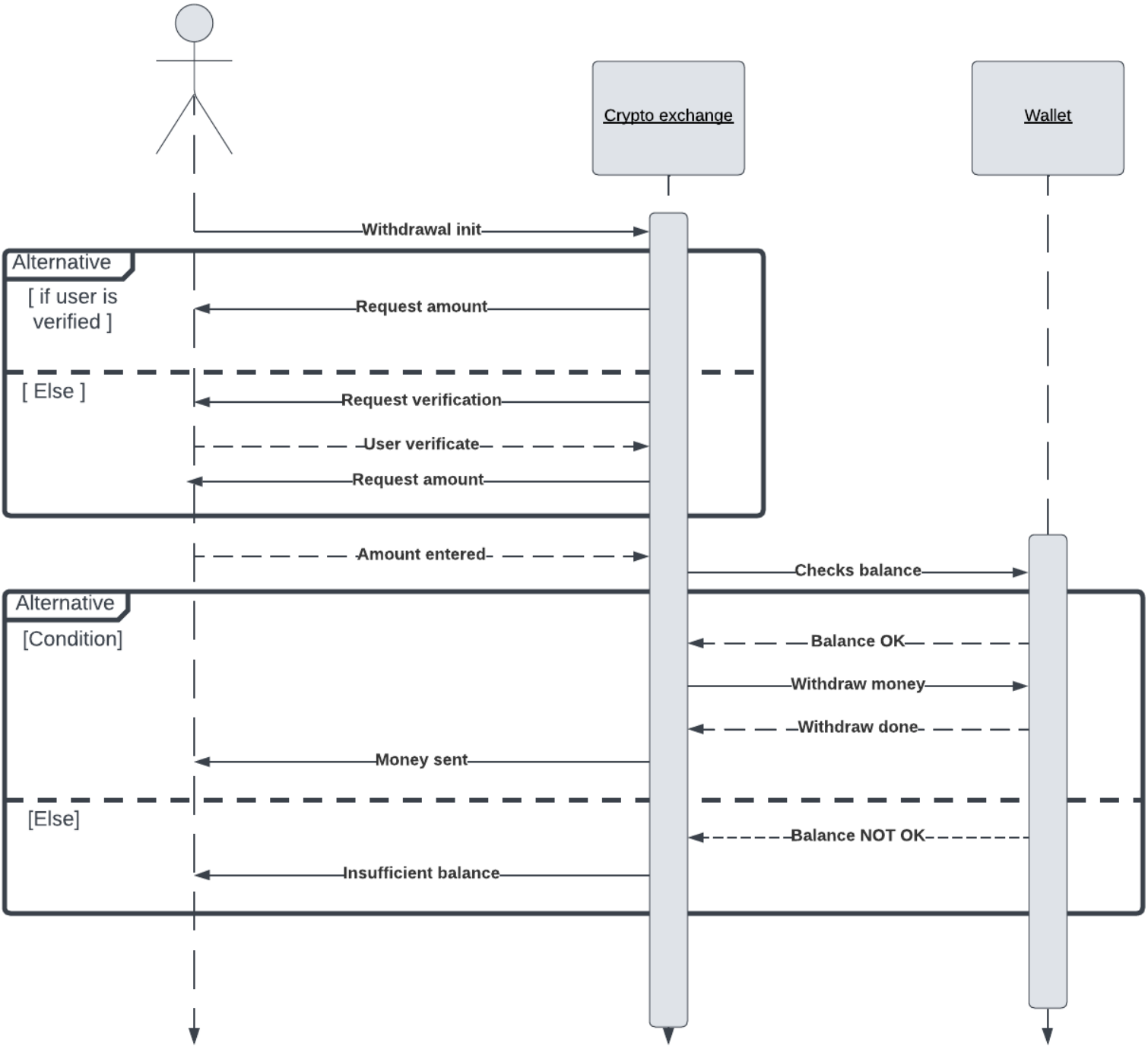
## 5.4 UC3 – Propojení strojů uživatele

a) **Název:** Propojení jednotlivých strojů uživatele
b) **Kontext:** Uživatel si propojí své jednotlivé stroje/PC a vytvoří mini superpočítač
c) **Level zanoření:** Těžař profesionál (3)
d) **Aktéři:** Těžař profesionál
e) **Stakeholdeři či jiné osoby:** ---
f) **Vstupní podmínky:** Uživatel musí být přihlášen na aplikaci a nutně musí mít dva či více strojů, které plánuje propojit.
g) **Výstupní podmínky:** Aplikace přijme požadavek na propojení strojů od jednoho uživatele. Zpracuje ho a provede propojení. Tímto vznikne mini superpočítač a ten se následně může propojit s mining poolem.
h) **Minimální výstup:** Systém detekuje, že v průběhu propojování strojů dojde k chybě a propojení se nezdaří. Zobrazí tedy uživateli chybovou hlášku. Pokud se bude jednat o jednu z evidovaných chyb, tak hláška bude obsahovat také důvod nepropojení.
i) **Ideální výstup:** Systém na základě uživatelova požadavku propojí jeho stroje, které budou následně připraveny k připojení k minning poolu. Pokud během tohoto propojení nenastane žádná chyba a propojení proběhne úspěšně, systém zobrazí uživateli hlášku o úspěšném propojení.
j) **Hlavní scénář:**
    1. Uživatel klikne na tlačítko „Zahájit párování.“
    2. Uživatel zvolí svůj hlavní stroj, který bude sloužit jako prostředník pro ovládání jeho ostatních strojů.
    3. Uživatel bude na tento stroj postupně připojovat své další stroje.
    4. Uživatel po připojení posledního stroje klikne na tlačítko „Ukončit párování.“
    5. Uživateli se na obrazovce objeví hláška, která mu sdělí, zda propojení proběhlo úspěšně.

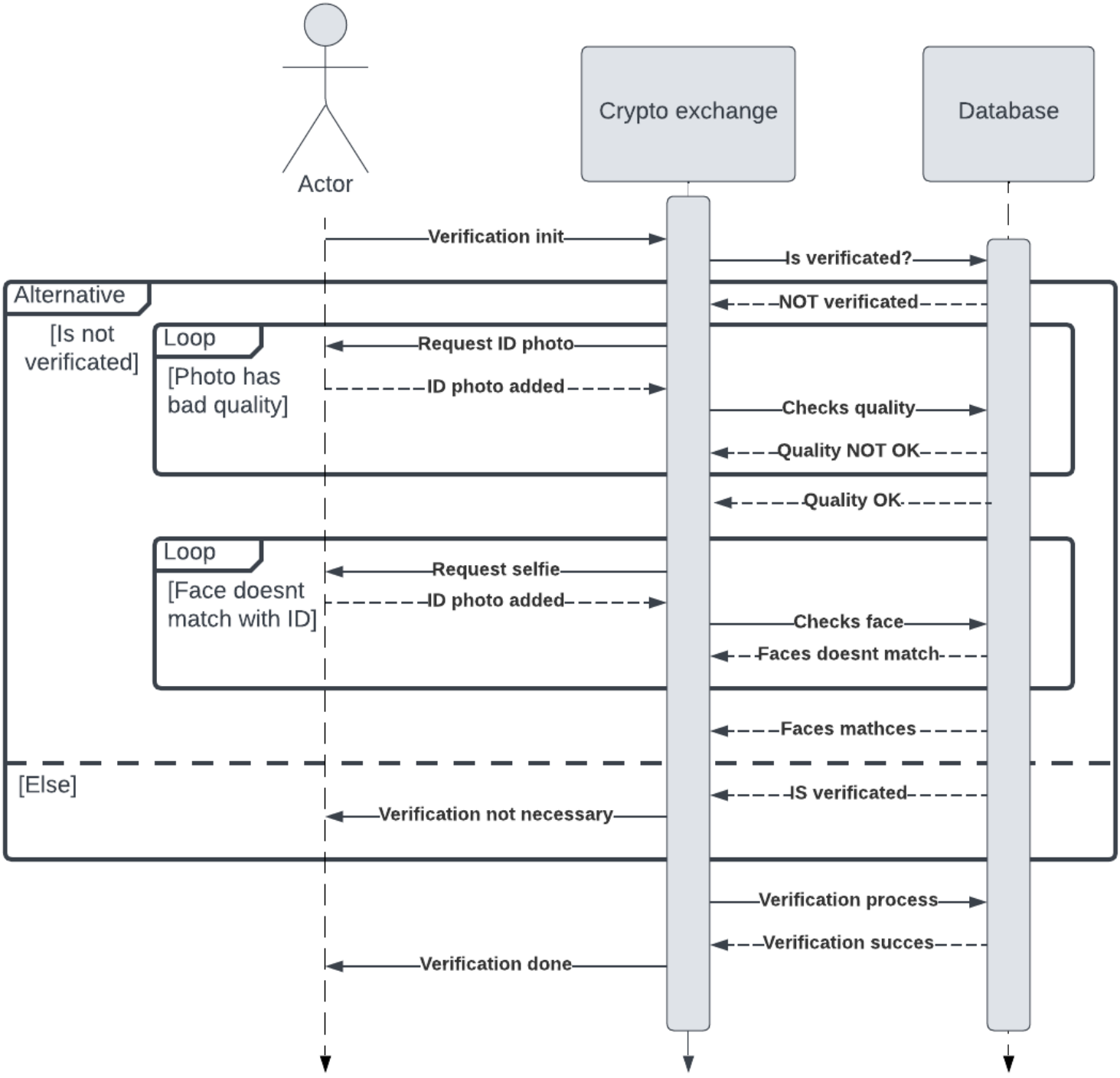
## 5.5 Třídní diagram



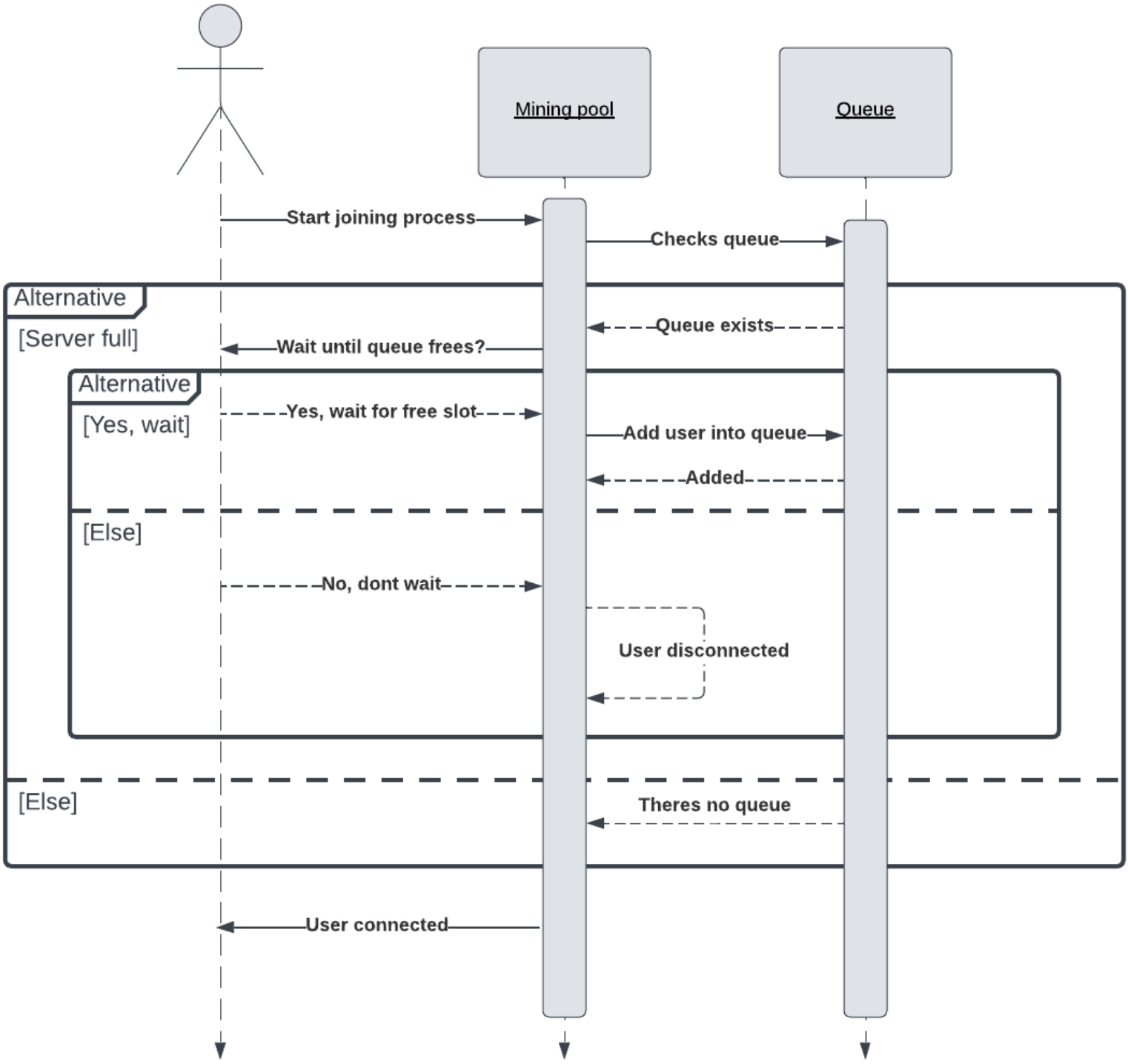
## 5.6 Sekvenční diagram – Výběr prostředků z burzy



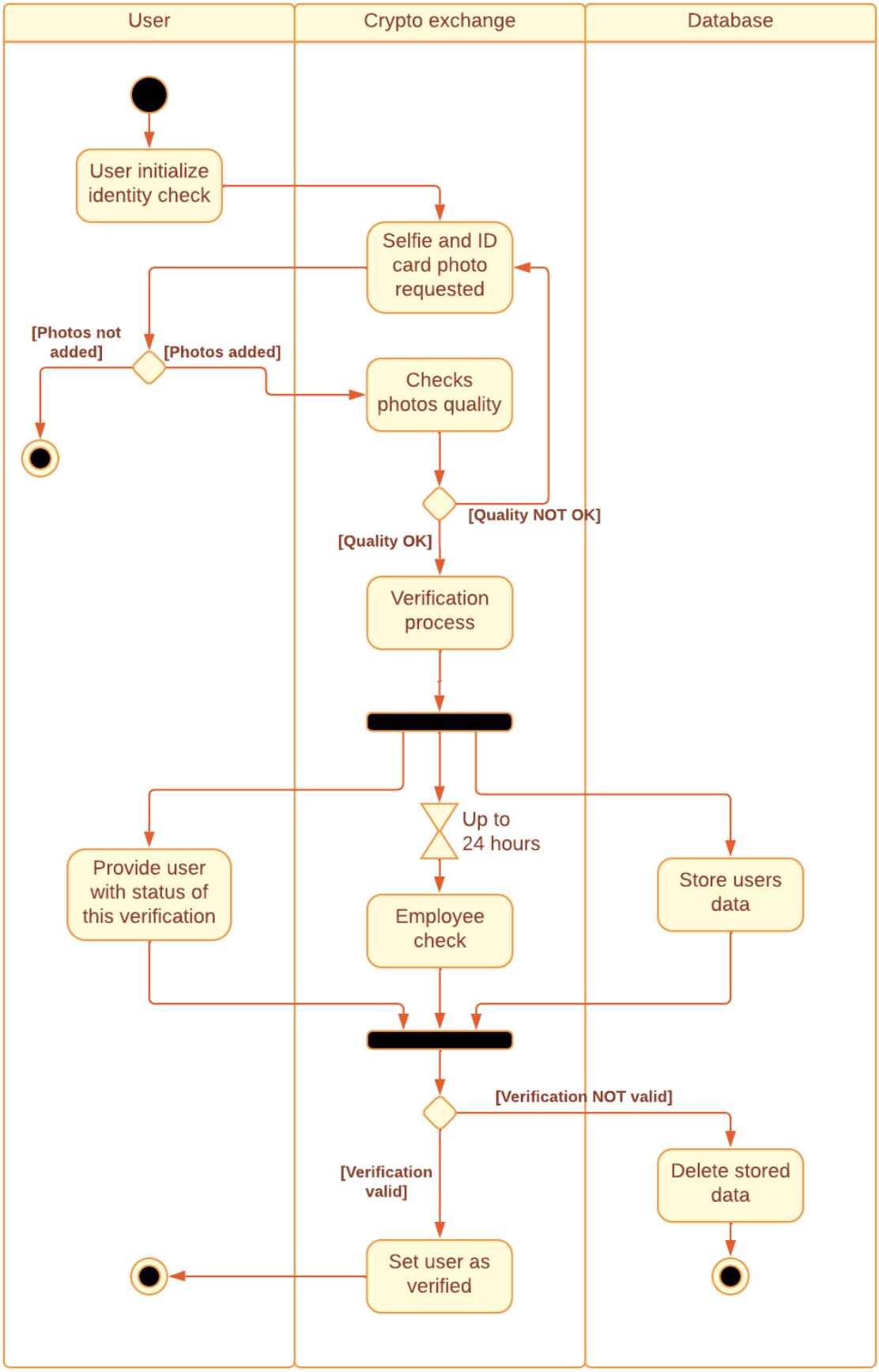
## 5.7 Sekvenční diagram – Verifikace údajů uživatele



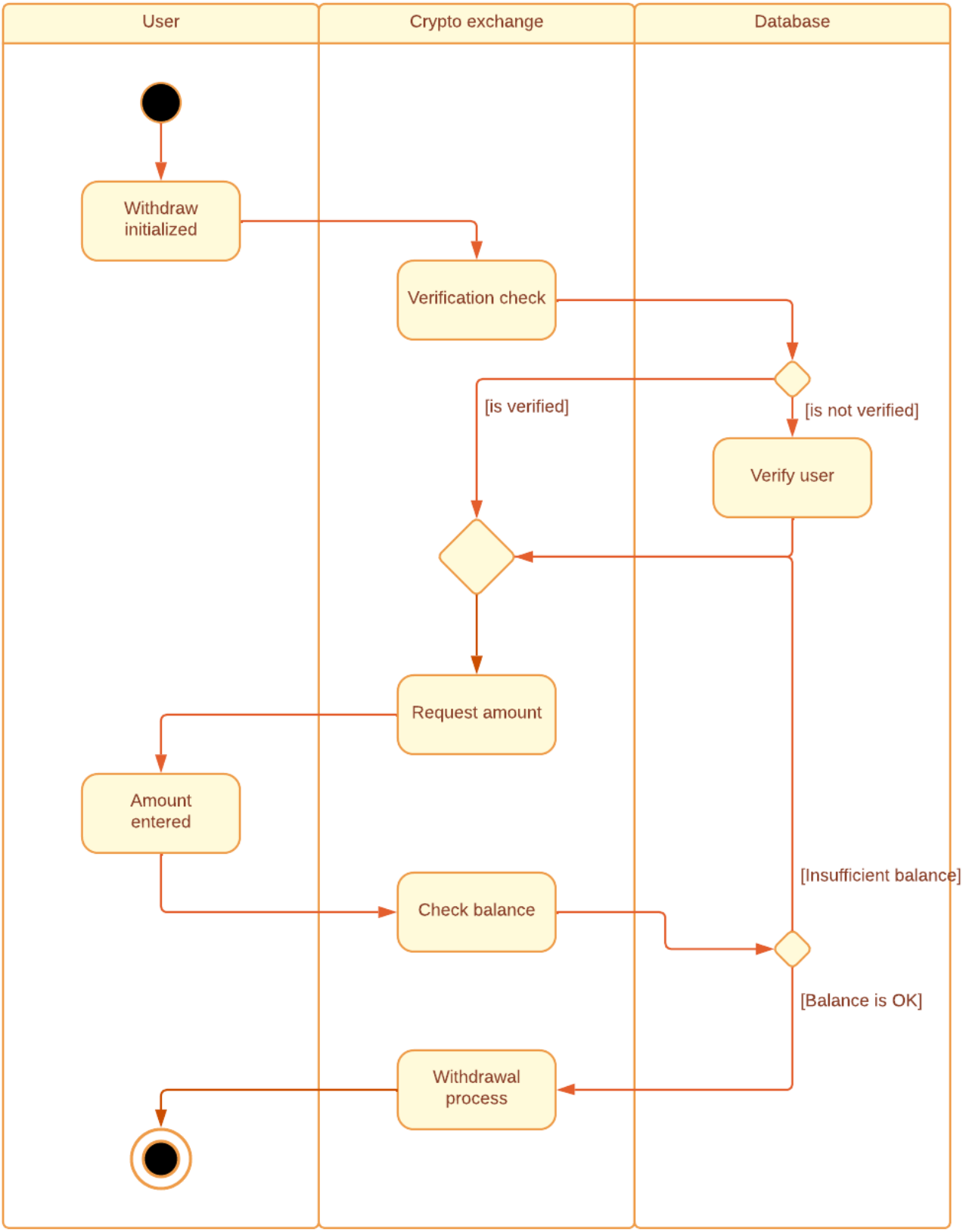
## 5.8 Sekvenční diagram – Připojení se na miningpool



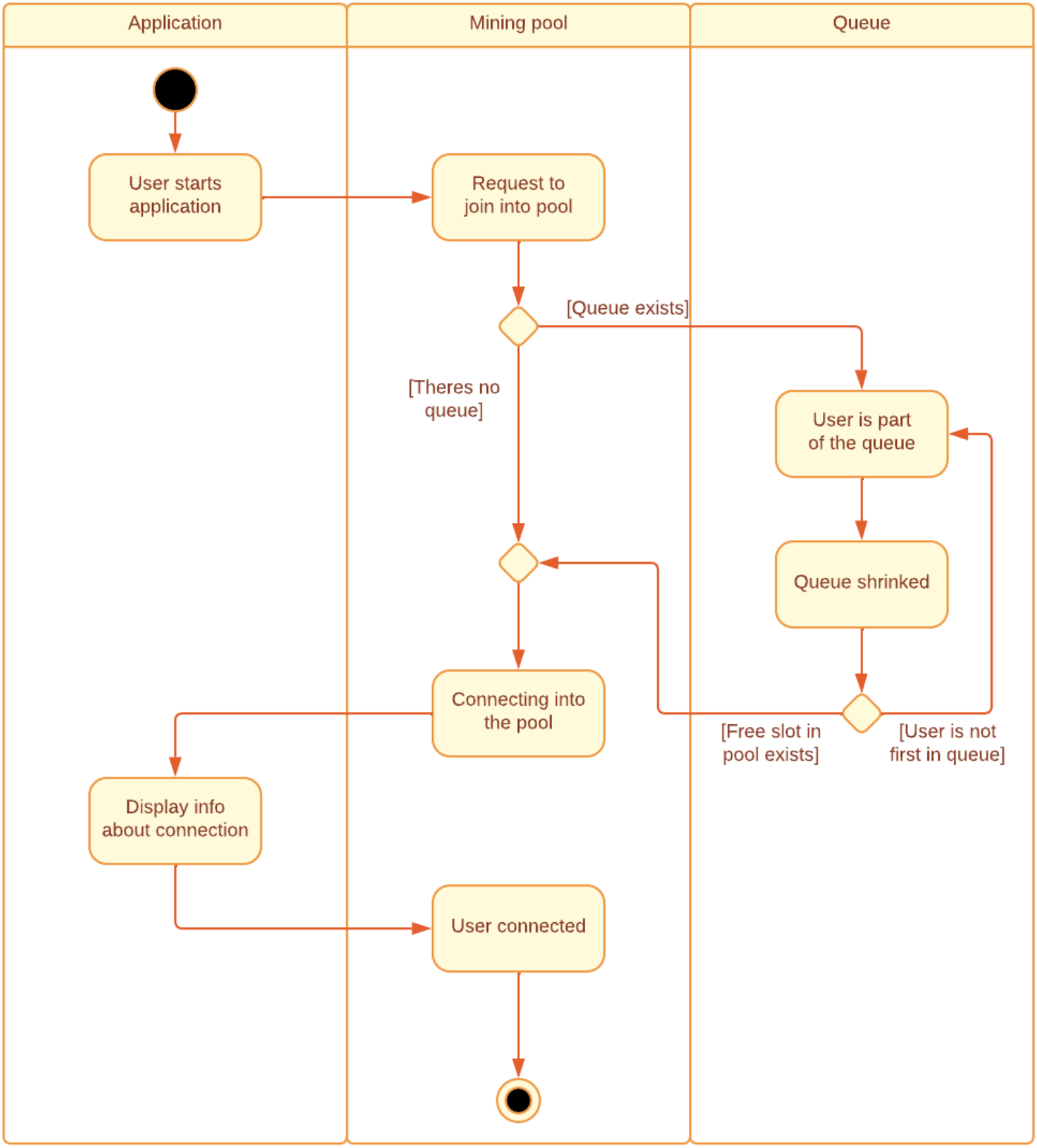
## 5.9 Aktivitní diagram – Verifikace uživatele



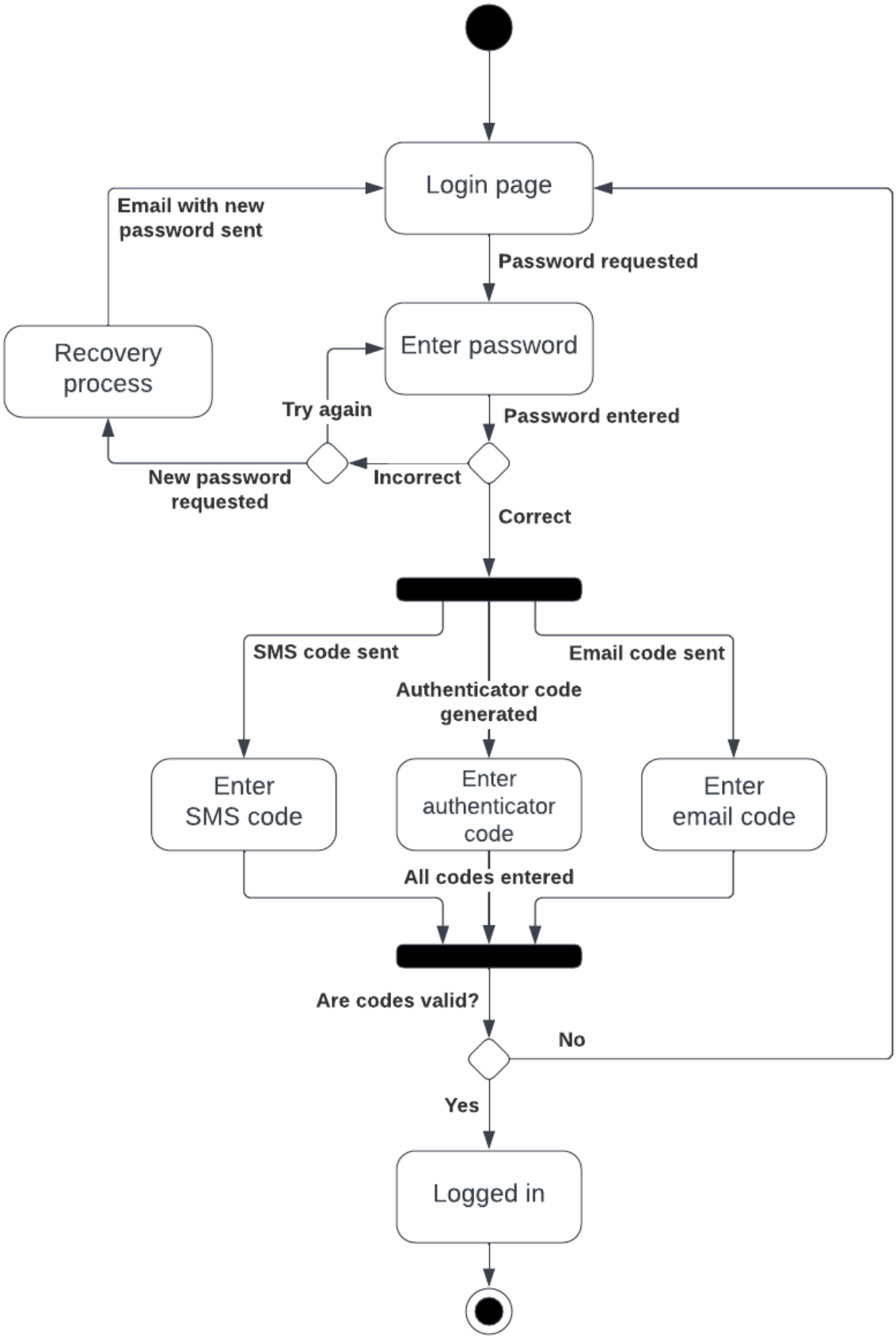
## 5.10 Aktivitní diagram – Výběr prostředků z burzy



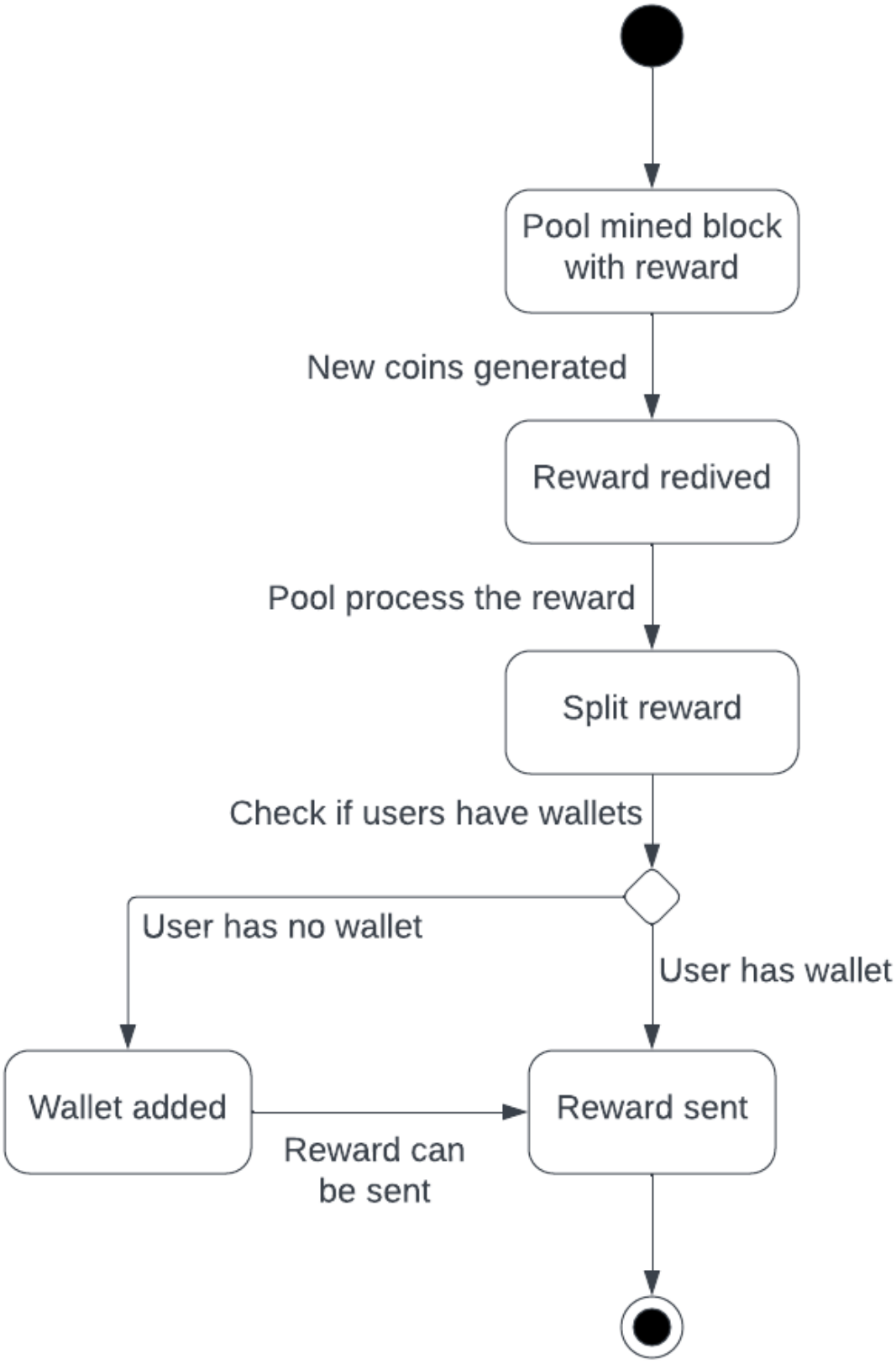
## 5.11 Aktivitní diagram – Připojení k mining poolu



## 5.12 Stavový diagram – Přihlášení uživatele



## 5.13 Stavový diagram – Distribuce odměn za těžbu



## 5.14 Stavový diagram – Update aplikace