Stredná odborná škola Jozefa Murgaša, Hurbanova 6,

Banská Bystrica

Ďuriš Maroš

3.A

Digitálna peňaženka pre kryptomeny

Úvod

V súčasnom digitálnom svete, kde kryptomeny získavajú čoraz väčšiu popularitu, je potrebné poskytnúť používateľom bezpečné a intuitívne nástroje na ich správu. Cieľom môjho projektu je vytvoriť modernú digitálnu peňaženku, ktorá nielen umožní ukladanie a prevody kryptomien, ale poskytne aj pokročilé funkcie pre správu uživateľských účtov. Táto aplikácia je navrhnutá tak, aby kombinovala vysokú úroveň bezpečnosti s jednoduchým ovládaním, čím sa stane vhodným riešením pre začiatočníkov aj pokročilých používateľov kryptomien.

Hlavné ciele projektu

- Poskytovanie cien v reálnom čase – Integrácia s blockchainovými sieťami na získavanie aktuálnych hodnôt kryptomien
- Nákup a predaj kryptomien – Umožnenie používateľom obchodovať priamo v aplikácii za aktuálne ceny
- Bezpečné transakcie – Odosielanie a prijímanie kryptomien s dôrazom na minimalizáciu poplatkov
- História transakcií a správa účtu – Prehľad o všetkých vykonaných operáciách a aktuálnych zostatkoch

Technologický základ projektu

Na dosiahnutie týchto cieľov využívam moderné technológie, ktoré zahŕňajú:

Frontend: Avalonia UI Framework pre responzívne a rýchle užívateľské rozhranie

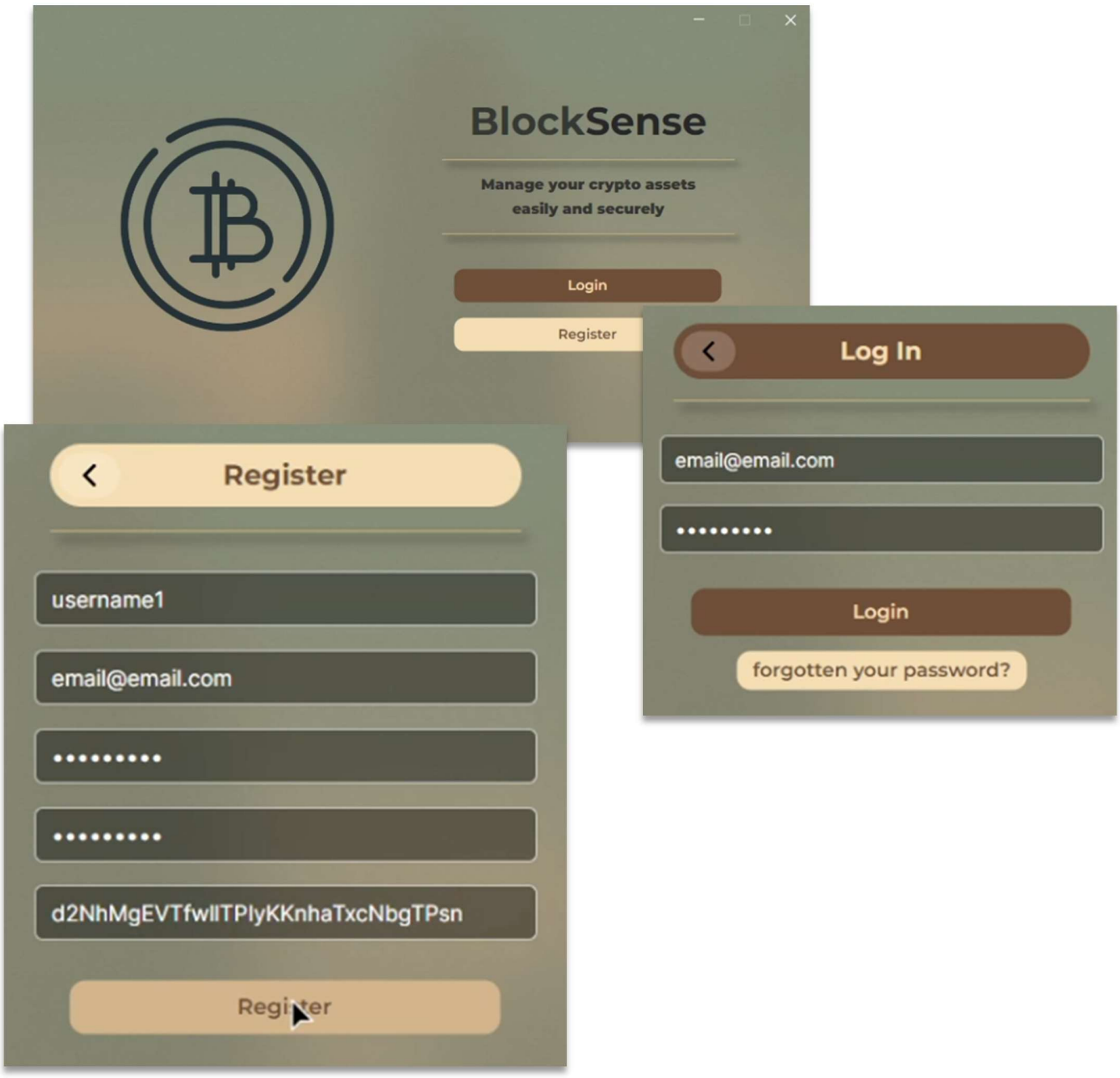
Backend: ASP.NET Core Web API pre serverovú časť

Databáza: MySQL s šifrovaným ukladaním citlivých údajov

Aktuálny stav vývoja

Fáza 1: Úvodný návrh a základné rozhranie

V tejto fáze som vytvoril základnú štruktúru aplikácie, vrátane Návrhu užívateľského rozhrania pre registráciu a prihlásenie. Prepojenia jednotlivých komponentov s obrazovkami prihlasovacieho procesu. Základného dizajnu aplikácie s dôrazom na intuitívnosť a jednoduchosť ovládania



Fáza 2: Bezpečnostné mechanizmy a autentifikácia

V tejto časti som sa zameral na zabezpečenie aplikácie a implementáciu pokročilých autentifikačných metód:

- Databázové prepojenie – Umožňuje ukladanie a správu používateľských účtov
- Hashovanie hesiel – Použitie algoritmu SHA-256 na bezpečné ukladanie hesiel.
- Token-based autentifikácia – Čiastočne implementovaný systém na správu prihlasovacích tokenov
- Generovanie šifrovacích kľúčov – Použitie PKCS5S2 na odvodenie kľúča z hesla a saltu
- Ukladanie tokenov – Pôvodne cez Windows Credential Locker, neskôr upravené na lokálne šifrované úložisko
- Funkcia "Remember Me" – Automatické prihlásenie pomocou refresh tokenov

uid	username	email	type	password	salt
1	username1	email@email.com	user	SwaWc7r9rUGejlpI/3LL6rpHNbbxOxRik2UD9jvIF74=	rBWnYfIDwhO3WaCHZMxrrg==
NULL	NULL	NULL	NULL	NULL	NULL

invitation_code	created_at	updated_at
SeeOkwVTQX5dtPfUWv0aap2lEBya9cnp	2025-01-16 18:43:09	2025-01-16 18:43:09
NULL	NULL	NULL

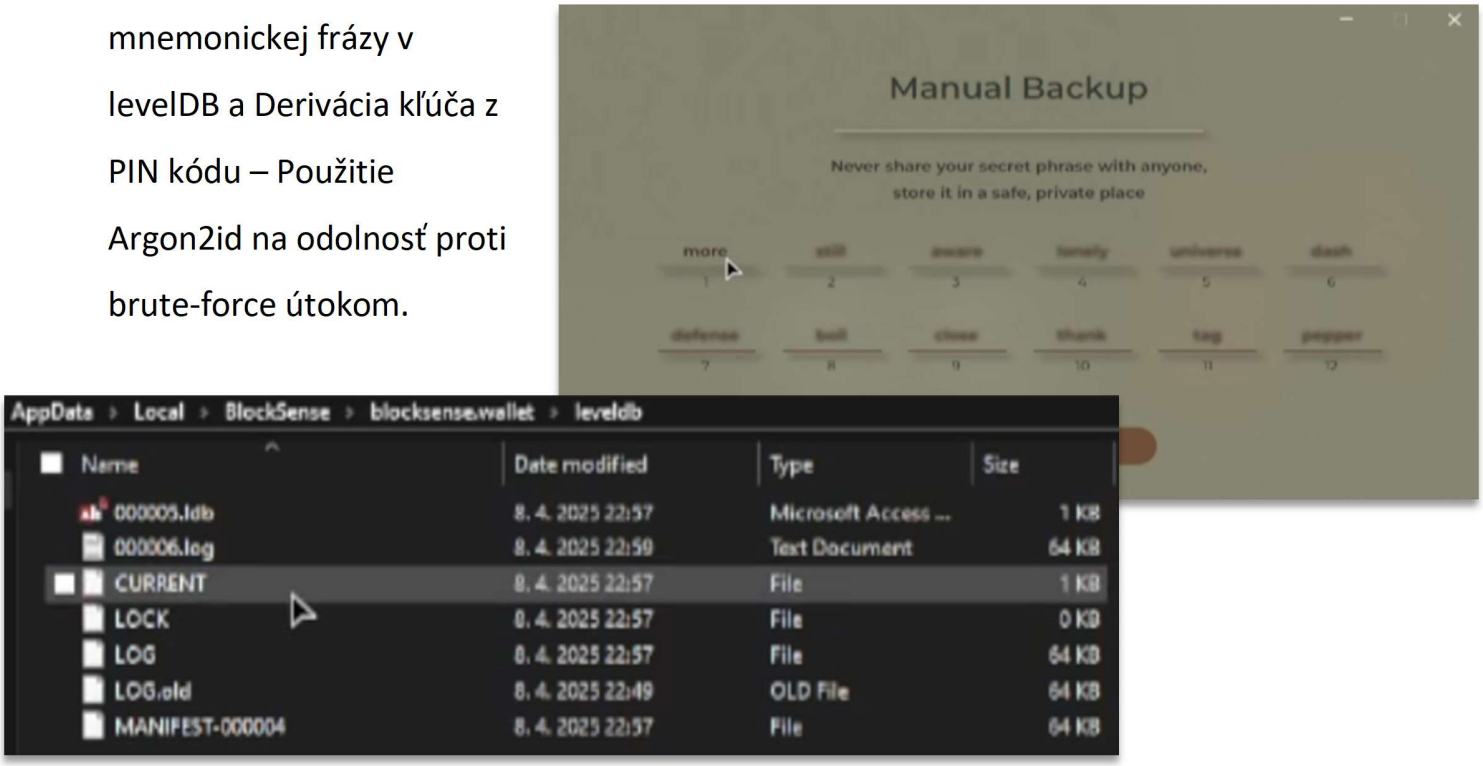
Fáza 3: Rozšírenie bezpečnostných funkcií a správa kľúčov

V najnovšej fáze som implementoval pokročilé bezpečnostné mechanizmy a prípravu na správu kryptomien ako napr. overovanie sily hesla – Pomocou knižnice *zxcvbn-cs* na detekciu slabých hesiel, lokálne šifrovanie tokenov – Namiesto Windows Credential Manager sa teraz používa *Data Protection API* (DPAPI).

Rozšírené overovanie tokenov – Okrem samotného tokenu sa kontroluje aj:

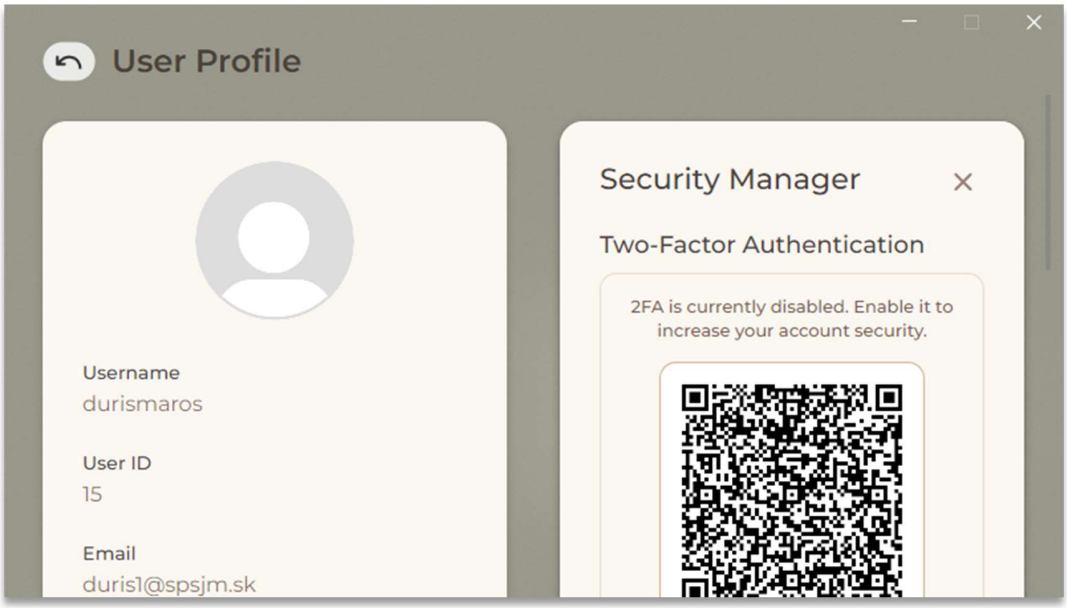
- *HWID* (Hardware ID)
- *MAC adresa*
- *Geografická poloha* (získaná pomocou maxmind-GeoIP2)
- *Dynamická entropia* – Generuje sa náhodná entropia pre zvýšenie bezpečnosti šifrovania

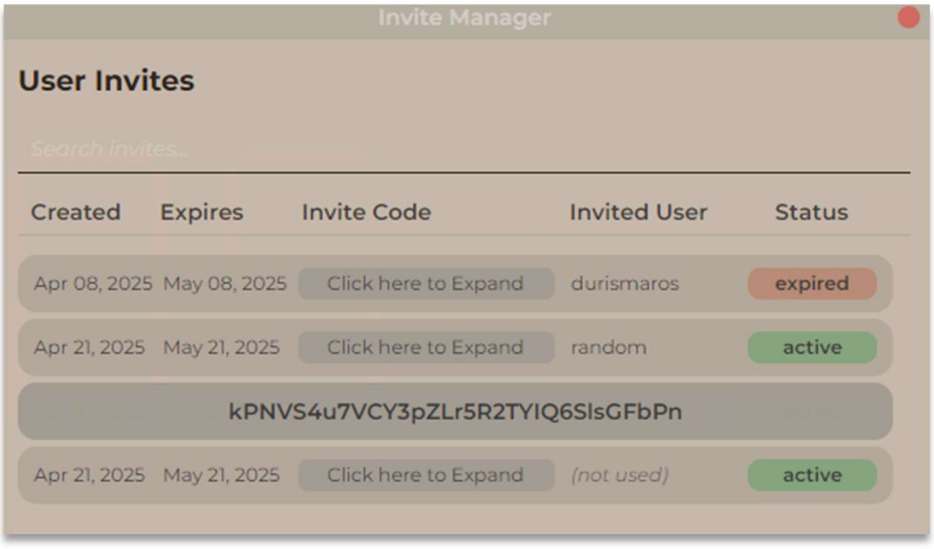
Mnemonická fráza – Generovanie 12-slovnej frázy pre deriváciu verejného a súkromného kľúča, šifrovanie pomocou AES-256 GCM – Bezpečné uloženie mnemonickej frázy v levelDB a Derivácia kľúča z PIN kódu – Použitie Argon2id na odolnosť proti brute-force útokom.



Fáza 4: Vývoj vlastného ASP .NET Core Web API backend servera

V tejto fáze projektu som prešiel od lokálneho vývoja klientskej aplikácie k vytvoreniu plne funkčného backendového systému postaveného na ASP.NET Core Web API. Tento krok bol kľúčový pre budúcu škálovateľnosť aplikácie, lebo umožňuje centralizovanú správu dát, bezpečnú komunikáciu s blockchain sieťami a integráciu s inými aplikačnými rozhraniami a webovými klientmi. Taktiež limituje možnosti klienta a spracúva citlivé informácie na svojej strane, čo je klúčové.





1. Architektúra backendu

Backend je navrhnutý ako RESTful API s nasledujúcou štruktúrou:

ASP.NET Core á.0 – Moderný a výkonný framework pre tvorbu webových API.

Modulárna štruktúra – Jednotlivé funkcionality sú rozdelené do samostatných projektov (napr. AuthService, CryptoService, TransactionService).

Docker podpora – Backend je pripravený na kontainerizáciu, čo umožňuje ľahké nasadenie na cloudové služby ako Azure/AWS.

2. Implementované funkcionality

Token-based autentifikácia pomocou JWT (JSON Web Tokens). Refresh token mechanizmus – Bezpečné obnovovanie platnosti prístupových tokenov.

HTTPS – Šifrovaná komunikácia medzi klientom a serverom, CORS politiky – Obmedzenie prístupu API len na povolené domény.

SQL injection protection – Použitie Entity Framework Core a parametrizovaných dotazov

Rate limiting a IP blocking – Obmedzenie počtu požiadaviek na API.

Záver

Vytvorenie vlastného ASP.NET Core Web API backendu bol zásadný krok k tomu, aby sa digitálna peňaženka stala plne funkčným produktom. Backend poskytuje:

- Bezpečnosť – Moderné šifrovanie a autentifikačné mechanizmy.
- Flexibilitu – Možnosť ľahko pridávať nové funkcionality.

Ďalšou fázou bude integrácia frontendu s API a príprava na produkčné nasadenie.