

# **STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST**

**Obor č. 18: Informatika**

## **Demonstrátor: blockchain jako moderní nástroj pro obchod s elektřinou**

**Karolína Podivínská  
Jihomoravský kraj**

**Letovice 2021**

# **STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST**

**Obor č. 18: Informatika**

**Demonstrátor: blockchain jako  
moderní nástroj pro obchod s elektřinou**

**Demonstrator: blockchain as a modern  
tool for electricity commerce**

**Autoři:** Karolína Podivínská

**Škola:** Biskupské gymnázium Brno a mateřská škola,  
Barvičova 85, 602 00 Brno

**Kraj:** Jihomoravský

**Konzultant:** Ing. Radek Fujdiak, Ph.D.

Letovice 2021

## **Prohlášení**

Prohlašuji, že jsem svou práci SOČ vypracovala samostatně a použila jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů.

Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné.

Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Letovicích dne 7. 4. 2021 .....

Karolína Podivínská

## Poděkování

Na tomto místě bych ráda poděkovala všem, kteří mě v psaní mé práce podporovali a tak mi pomáhali. Jmenovité poděkování patří panu Ing. Radku Fujdiakovi, Ph.D, který se stal mým osobním konzultantem. Další velký dík patří Ivaně za pomoc s korekturami.

Tato práce byla vypracována za finanční podpory JMK.

The logo of the Jihomoravský kraj (JMK) is displayed within a black rectangular border. It features the text "jihomoravský kraj" in a blue, sans-serif font. The letter "m" is stylized with a red vertical bar on its left side.

Obrázek 1: Logo JMK (poskytnuto z jcmm)



Obrázek 2: Logo JCMM (poskytnuto z jcmm)

## **Anotace**

Ve své práci SOČ se zabývám technologií blockchain, která nachází využití hlavně v odvětví kryptoměn. Mým úkolem je demonstrovat fungování technologie blockchain pro obchod s elektřinou. K naprogramování svého demonstrátoru používám programovací jazyk Python, dále HTML a CSS. Výstupem je demonstrovaná aplikace, která interpretuje fungování decentralizované sítě založené na blockchainu, společně s popisem jejích výhod a nevýhod a případných návrhů na další realizaci.

## **Klíčová slova**

blockchain; decentralizovaný systém; obchod s elektřinou; python

## **Annotation**

In my SOC work I deal with blockchain technology, which finds use mainly in the cryptocurrency industry. My task is to demonstrate how blockchain technology works within electricity commerce. I use the Python programming language, HTML and CSS to program my demonstrator. The output is a demonstrated application that interprets a decentralized blockchain-based network's operation, together with a description of its advantages and disadvantages and possible proposals for further implementation.

## **Keywords**

blockchain; decentralized system; electricity commerce; python

# OBSAH

Základní pojmy .....	6
Úvod.....	7
1 Technologie blockchain .....	8
1.1 Decentralizace .....	8
1.2 Distribuovaný systém a obchod s elektřinou .....	9
1.2.1 Smlouvy u společností .....	9
1.2.2 Vlastní výroba .....	9
1.2.3 Decentralizovaný obchod s elektřinou dnes .....	11
1.3 Struktura blockchainu .....	12
1.3.1 Blockchainové transakce a jejich bezpečnost .....	13
1.3.2 Blockchainové transakce v porovnání s centralizovanými systémy .....	14
1.3.3 Konsenzus, těžba .....	14
2 Můj blockchain .....	17
2.1 Použité programovací jazyky .....	17
2.2 Aplikace .....	17
2.2.1 Založení účtu, přihlášení .....	17
2.2.2 About this demonstrator .....	19
2.2.3 View Caroline's blockchain .....	19
2.2.4 Submit a transaction .....	20
2.2.5 View pending transactions .....	21
2.2.6 Mining .....	21
2.2.7 View profile .....	23
2.2.8 Sell electricity .....	23
2.2.9 Buy electricity .....	24
2.2.10 Logout .....	25
Závěr, diskuse .....	26
Použitá literatura, zdroje .....	27
Seznam obrázků .....	30
Příloha 1: zdrojový kód – funkce kontrolující bezpečnostní kritéria hesla (screenshot) .....	31
Příloha 2: zdrojový kód – funkce zajišťující aktualizaci blockchainu mezi uzly (screenshot) .....	32

## ZÁKLADNÍ POJMY

<b>blockchain</b>	technologie využívaná v distribuovaných systémech; neustále se zvětšující řetězec vzájemně propojených bloků s neměnným obsahem; veřejná účetní kniha všech transakcí provedených uzly dané sítě
<b>blok</b>	jednotka blockchainu, objekt nesoucí transakce uživatelů a další doplňující informace (časová známka, index, hash...)
<b>těžba</b>	proces připojení nového bloku do blockchainu
<b>těžař</b>	uživatel sítě, který se snaží připojit nový blok do blockchainu a dostat za to danou odměnu
<b>hash</b>	unikátní řetězec znaků (string) přesně stanovené velikosti reprezentující daný objekt (data), který má neomezenou velikost
<b>decentralizovaný systém</b>	systém bez řídicí autority
<b>centralizovaný systém</b>	systém s řídicí autoritou (banka, server)
<b>uzel</b>	uživatel sítě
<b>distribuovaná peer-to-peer síť</b>	síť uzlů bez jakýchkoli centrálních bodů, ve které komunikuje „každý s každým“
<b>konsenzus</b>	smluvený způsob rozhodování v blockchainové síti, který uznávají všechny uzly, sloužící k zabezpečení blockchainu
<b>flash message</b>	krátká informační zpráva zobrazující se po vyvolání nějaké změny v aplikaci, o které by uživatel měl vědět (např. „Uživatel Josef přihlášen“ apod.)
<b>python</b>	jednoduchý a přehledný, objektově orientovaný, vysokoúrovňový programovací jazyk s univerzálním využitím <sup>[46]</sup>
<b>html</b>	hypertextový značkovací jazyk, používaný hlavně pro tvorbu www stránek
<b>css</b>	kaskádové styly, používané pro statické grafické rozhraní www stránek

# ÚVOD

Technologie blockchain je velmi mocným nástrojem v mnoha různých oborech. Jeho hlavní využití však nacházíme všude tam, kde je žádoucí spolehlivost, neměnnost a decentralizované prostředí. Umožňuje totiž vytvořit takový systém, který je dostupný a otevřený pro každého, ale zároveň je bezpečný a data v něm neměnná.

Kromě výhod spojených s decentralizací blockchainová síť poskytuje i další výhody jako je vyšší anonymita, často nižší náklady na provoz sítě nebo transparentnost. Neexistuje zde časové omezení v dostupnosti (pracovní doba), takže transakce mohou probíhat prakticky pořád.

Jako příklad využití uvedu zdravotnictví (uchovávání dat o předpisech léků...), potravinářství (dopravní logistika), volební systém (eliminace problémů při sčítání) či obchod s elektřinou, kterému bych se ve své práci chtěla věnovat (majitelé nemovitostí s vlastními zdroji elektřiny).

Mým cílem je vytvořit aplikaci, která by přehledně ukazovala fungování technologie blockchain. Měla by také umožnit provádění transakcí a demonstrovat tak nákup a prodej elektřiny tímto (zatím) neobvyklým způsobem.



# 1 TECHNOLOGIE BLOCKCHAIN

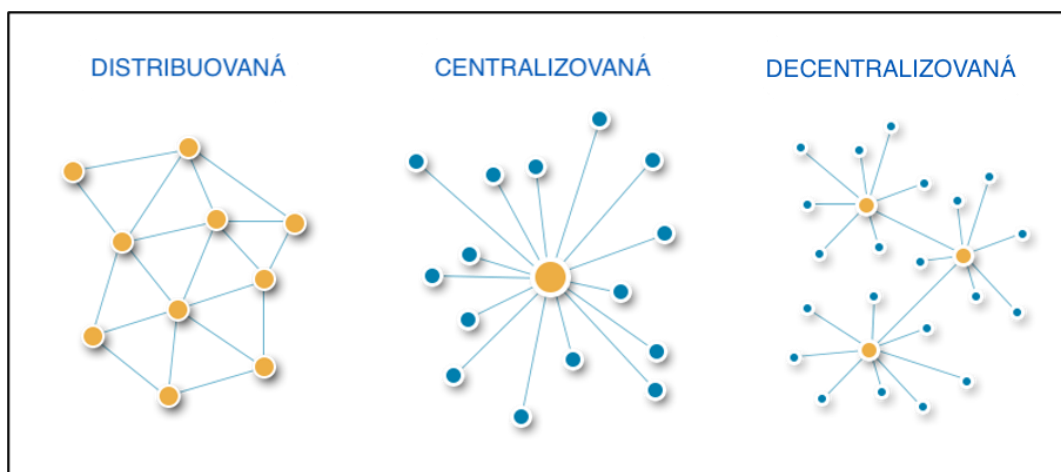
## 1.1 Decentralizace

Ač mnohé firmy mají své privátní blockchainya<sup>[17]</sup>, podstatou blockchainové sítě je decentralizované prostředí – prostředí, ve kterém k provádění operací není potřeba existence centrální autority nebo kontrolního bodu, který by celou síť spravoval<sup>[7]</sup>. Centrální autoritu často představuje banka nebo server, vždy se jedná o třetí stranu zprostředkující určitou formu komunikace mezi dvěma uživateli (uzly) sítě. Pro jasné rozlišení uveďme příklad z praxe:

Adam potřebuje poslat peníze Báře. Typicky otevře internetové bankovníctví a prostřednictvím banky, která ověří, že peníze má, a transakci zaeviduje, jí peníze pošle. Adam i Bára jsou tak dvěma uzly v centralizovaném systému, kde hlavním kontrolním bodem je banka.

Když se však Adam nebude chtít spoléhat na banku, může se pokusit provést transakci decentralizovaně a přijít přímo k Báře a dát jí peníze do ruky. Jakým způsobem si však Adam a Bára zajistí vzájemnou důvěru, pokud se neznají? Problematiku bezpečnosti provádění transakcí v decentralizovaných systémech rozeberu v kapitole 1.3.1.

Nyní už zhruba víme, jak vypadá centralizovaný a decentralizovaný systém. Pro vytvoření blockchainové sítě nám však nestačí klasická decentralizovaná síť uzlů. Jak vidíme na obrázku č. 3, decentralizovaná síť totiž v praxi také má centrální body, jen je jich víc. Můžeme si to představit jako síť firem s vlastními zaměstnanci, kde za každou z nich zodpovídá její ředitel. Jednotliví pracovníci se mohou podílet na vnitřních záležitostech firmy, ale pouze ředitel má pravomoc komunikovat s ostatními firmami jako její zástupce. Pro blockchainovou síť však potřebujeme zajistit, aby mezi sebou mohli na stejné úrovni komunikovat všichni uživatelé sítě. Řešení nabízí tzv. distribuovaná peer-to-peer síť.



Obrázek 3: Distribuovaná, centralizovaná a decentralizovaná síť uzlů (převzato z [https://assets.website-files.com/59d5e4bc47ecf500018f5599/59d796d6c47bd800017e8bef\\_Block%20Chain.png](https://assets.website-files.com/59d5e4bc47ecf500018f5599/59d796d6c47bd800017e8bef_Block%20Chain.png))

## 1.2 Distribuovaný systém a obchod s elektřinou

V dnešní době má zákazník v podstatě tři možnosti, jak získat elektřinu. Buďto podepíše smlouvu s jednou z firem, které elektřinu dodávají (v České republice je jich přes osmdesát<sup>Error! Reference source not found.</sup> a mezi největší patří např. ČEZ, E.ON nebo Bohemia Energy<sup>[29]</sup>) a uplatní tak centralizovaný model, nebo si zajistí vlastní výrobu elektrické energie (nejčastějším řešením jsou solární panely např. na střeše domu). Jakýmsi hybridem mezi těmito možnostmi je řešení spočívající v jejich kombinaci – zákazník si část elektřiny vyrobí a zbytek odkupuje od dodavatele. Každé řešení má samozřejmě své výhody i nevýhody.

### 1.2.1 Smlouvy u společností

Hlavní výhodou odebírání elektřiny od společností je celková jednoduchost – na trhu je jich sice spousta, ale člověk nemusí být zrovna odborník, aby si udělal alespoň základní srovnání a našel vhodného dodavatele, který je důvěryhodný a vyhoví jeho potřebám. Navíc případů, kdy ověřený dodavatel elektrickou energii nemá a nemůže ji zákazníkovi dodat, je minimum. Mnoho firem také nabízí garanci ceny po určité časové období.

Mezi nevýhody patří existence podvodných smluv, které upřednostňují prosperitu firmy na úkor zákazníka. Navíc je mnohdy těžké se z těchto smluv vyvázat. Dále je systém v tomto případě nastaven čistě centralizovaně, takže jsme nuceni spoléhat se na poctivost dané firmy.

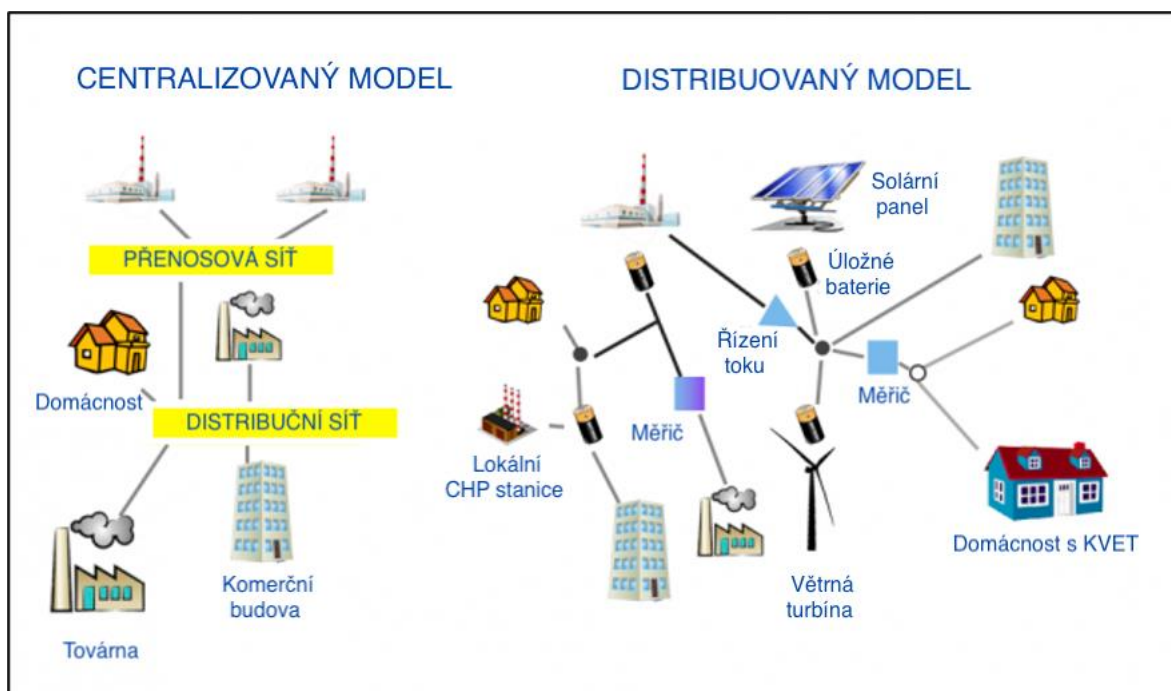
### 1.2.2 Vlastní výroba

Při tomto způsobu získávání elektrické energie má dotyčný jistotu, že ho nikdo nepodvádí. Dalším hlediskem je často diskutovaný dopad na životní prostředí – solární panely jsou mnohem ekologičtější než zpracovávání fosilních paliv.

Na druhou stranu, toto zdánlivě jednoduché řešení však přináší některé nevýhody. Počáteční realizace vlastní výroby vezme hodně času i peněz a člověk musí vědět, do čeho jde, a být připraven na spoustu problémů. Je nutné propočítat ekonomickou výhodnost počátečních investic (náklady na solární panely a montáž, údržbu) a také se připravit na neustálé kolísání zisku (dny, kdy je zataženo apod.). Navíc se může stát, že získaná energie nedostačuje celkové spotřebě. V takovém případě si daný jedinec musí zbylou elektřinu dokoupit od některé ze společností a přejít tak na onen hybridní model. Ten pro něj ve finále může být finančně výhodnější než čistý nákup u firmy, a navíc tak může snížit svoji uhlíkovou stopu, ale problémů s centrální autoritou se tak nezbaví.

A pokud vyrábí elektřiny víc, než potřebuje? Dnešní systém obchodu s elektřinou je nastaven téměř jednosměrně, tedy od dodavatelů elektřiny přes distributory až k zákazníkovi<sup>[30],[31]</sup>. Přitom počet lokálních výrobců, kteří si elektřinu vyrábí sami a mají možnost její přebytek odprodávat dalším zákazníkům, celosvětově roste a zjevně i růst bude<sup>[30],[31],[32],[33]</sup>. Lokální výrobci však většinou mají svázané ruce, velcí obchodníci nejsou zvyklí na odběr elektřiny právě od nich a obchodování je tak zbytečně složité a neefektivní. Další možností je přebytečnou energii skladovat ve formě nabitých baterií, ale to se dnes ukazuje jako neefektivní.

Když se však nad celým problémem zamyslíme, poměrně rychle přijdeme na to, že řešením by mohla být distribuovaná peer-to-peer síť, ve které by mohli na stejné úrovni prodávat svou elektřinu velcí i malí prodejci.



Obrázek 4: Centralizovaný a distribuovaný model obchodu s elektřinou  
(převzato z [https://www.solarunitedneighbors.org/wp-content/uploads/2020/08/centralized-v-decentralized-power-grid\\_0.png](https://www.solarunitedneighbors.org/wp-content/uploads/2020/08/centralized-v-decentralized-power-grid_0.png))

Distribuovaná peer-to-peer síť lokálních prodejců a jejich zákazníků totiž přináší mnoho výhod – snad ve všech případech se jedná o ekologičtější výrobu elektrické energie (solární panely) a jelikož vstup i výstup do/z prodejní sítě je volný, motivuje to k připojení dalších a dalších prodejců. Ti si totiž mohou nastavit vlastní ceny.

U prodeje je klíčová i vzdálenost kupujícího a prodávajícího. Zatímco běžně do domácností elektřina putuje dlouhými dráty a přes další zařízení, v distribuovaném systému klidně můžeme prodávat elektřinu svým sousedům, což značně sníží náklady na její přepravu, a tudíž se značně sníží i celková cena elektřiny, jenž láká nové zákazníky. Kupující se tak domlouvá přímo s prodejcem, má na výběr mnohem víc nabídek, které může porovnávat, a svým nákupem podpořit třeba někoho, koho zná a důvěřuje mu.

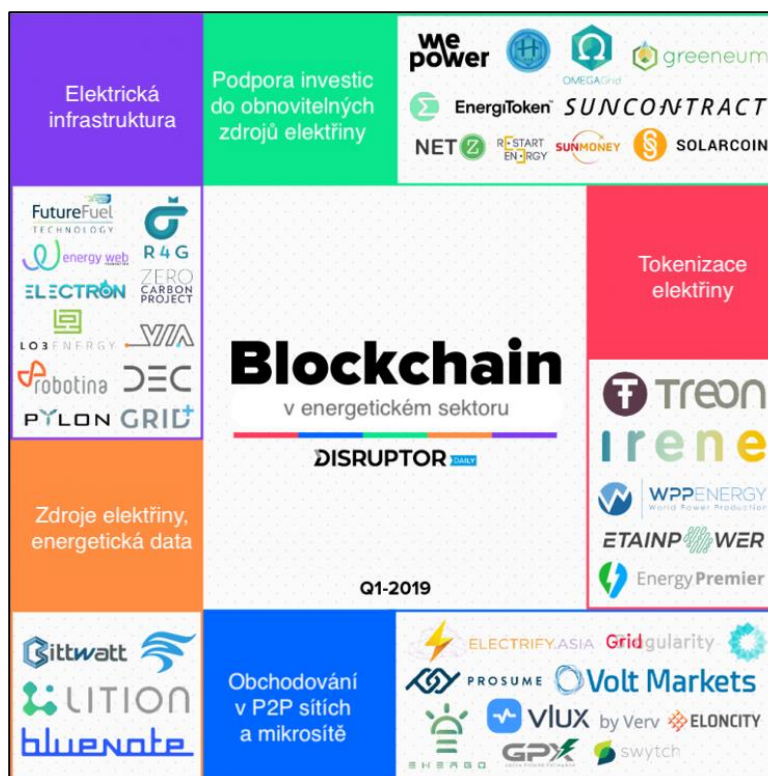
Posledním důležitým aspektem je samotný fyzický transport elektřiny. Přenosová síť může být velmi nerovnoměrně rozložená a většinou má menší počet významnějších vlastníků. Proto se blockchain využívá pro lokální obchodování s elektřinou, kdy část z těchto problémů odpadá.

### 1.2.3 Decentralizovaný obchod s elektřinou dnes

Nutno podotknout, že dnes ještě mnoho lidí blockchainu nebo decentralizovaným systémům nerozumí a představa participovat v distribuované peer-to-peer síti je kvůli tomu může odrazovat. Tento strach může být podpořen ještě tím, že se technologie stále vyvíjí a lidé jim ze začátku jako neodzkoušeným novotám nechtějí věřit. Vyloučit také nelze i budoucí omezení státem apod.

Systém se však přes všechny strasti začíná měnit a jak můžeme vidět na obrázku č. 5, některé firmy již blockchain pro obchodování s elektřinou využívají. Jedním z příkladů je australská technologická firma Power Ledger, která vytvořila platformu umožňující onen sousedský systém prodeje elektřiny z obnovitelných zdrojů. Konkrétně se prodává elektřina získaná pomocí solárních panelů. Firma zorganizovala již více než dvě desítky projektů v osmi zemích celého světa. K vývoji a chodu platformy byl použit Ethereum a POA blockchain. Firma byla založena v roce 2016 a v roce 2018 získala za svoji práci hlavní ocenění v soutěži Extreme Tech Challenge<sup>[32],[37],[38]</sup>.

Za zmínku také stojí Suncontract. Jak již název napovídá, tato firma se specializuje na obchod a podporu získávání elektrické energie z obnovitelných zdrojů. Jejím cílem je tvorba decentralizovaného systému pro udržitelný obchod s elektřinou. Záleží jí na ekologii, podporuje cíle udržitelného rozvoje Organizace spojených národů. Vývoj pokračuje od roku 2016. Pro své uživatele vytvořila aplikaci, kde od roku 2018 mohou s elektřinou jednoduše obchodovat<sup>[32],[39]</sup>.



Obrázek 5: Firmy využívající blockchain v odvětví obchodu s elektřinou  
(převzato z <https://www.disruptordaily.com/wp-content/uploads/2018/11/0-2-768x768.png>)

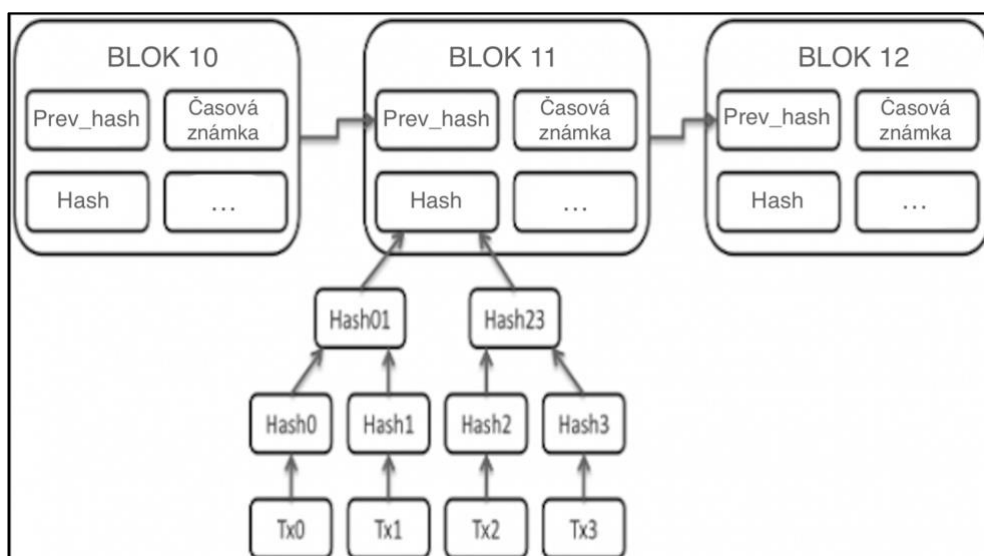
### 1.3 Struktura blockchainu

Jak již název technologie napovídá, blockchain můžeme zjednodušeně chápat jako stále se zvětšující řetězec (*chain*) bloků (*blocks*) s neměnným obsahem.

Tyto bloky mají určité atributy (nesou určité informace), které se sice mohou v různých implementacích lišit, ale některé z nich jsou zásadní pro samotné fungování blockchainu. Příkladem takového důležitého atributu je tzv. hash.

Hash je výstupním řetězcem po volání hashovací funkce, která v podstatě převádí data neomezené velikosti do dat přesně stanovené velikosti, a je prvkem asymetrické kryptografie. Její dvě důležité vlastnosti jsou tyto: zaprvé, neexistuje k ní inverzní funkce (z původních dat uděláme hash, ale z hashe neuděláme původní data), zadruhé, každý hash vychází z unikátních dat, když je tedy jakkoli pozměníme, výsledný hash bude výrazně odlišný od původního. Hash tedy interpretuje daný objekt či data ve zkrácené formě<sup>[21]</sup>.

V každém bloku najdeme dva hashe – první interpretuje aktuální blok a druhý je odkazem na blok předchozí. To umožňuje bloky vzájemně zřetězit. Zvláštním případem je první blok blockchainu – tzv. genesis blok<sup>[20]</sup>. Nemá totiž předka (má nejnižší výšku v blockchainu) a tím pádem nemůže uchovávat ani hash předchozího bloku. Řešením je nahrazení atributu předchozího hashe (na obrázku *Prev\_hash*) řetězcem nul. Mimo to genesis blok často nenese ani žádné transakce.



Obrázek 6: Řetězec bloků – datová struktura blockchainu

(převzato z [https://www.researchgate.net/publication/325053899\\_Assessing\\_Security\\_and\\_Performances\\_of\\_Consensus\\_algorithms\\_for\\_Permissioned\\_Blockchains](https://www.researchgate.net/publication/325053899_Assessing_Security_and_Performances_of_Consensus_algorithms_for_Permissioned_Blockchains))

Pole transakcí je dalším důležitým atributem každého bloku. Blockchain totiž funguje jako otevřená účetní kniha zaznamenávající všechny transakce uživatelů, ve které záznamem však není jedna transakce, nýbrž blok, který transakcí nese hned několik. Když tedy chce nějaký uživatel poslat jinému uživateli peníze či jiné tokeny, jeho transakce se uloží do pole čekajících transakcí, kde čekají do doby, než jsou připojeny do nějakého bloku. Důležitou otázkou je, jak vlastně provádění transakcí na blockchainu funguje.

### 1.3.1 Blockchainové transakce a jejich bezpečnost

Vraťme se k ilustračnímu příkladu z kapitoly 1.1, kdy Adam chce poslat peníze Báře v distribuované blockchainové síti. V zásadě vytvoří transakci, kde Adam bude odesílatelem a Bára příjemcem. Následně informaci o požadavku na provedení transakce rozešle mezi ostatní uživatele sítě, kteří ji ověří. Takto jednoduchou transakce však lze snadno zfalšovat.

Zprvée, transakci chybí autentizace. Když by autentizace nebyla vyžadována, Bára by klidně mohla vytvořit transakci, ve které by byl Adam jako odesílatel a ona jako příjemce bez Adamova souhlasu. Potřebujeme tedy zajistit, aby každý uživatel svoje transakce potvrzoval, autentizoval. K tomu se opět využívá asymetrická kryptografie, tentokrát nikoli pomocí hashů, ale díky tzv. soukromým a veřejným klíčům, které každý z uživatelů vlastní<sup>1</sup>. Pokud chce tedy Adam svou transakci potvrdit, s pomocí svého soukromého klíče vytvoří digitální podpis, kterým ji autentizuje. Digitální podpis totiž Adama jasně identifikuje, zároveň je však odlišný pro každou transakci, aby nezpřístupnil Adamův soukromý klíč. Tím viditelně potvrdí, že svoji transakci myslí opravdu vážně a vytvořil ji on sám<sup>[41]</sup>.

Dalším problémem je tzv. double spending, problém dvojí útraty. Jedná se o situaci, kdy by Adam chtěl stejné peníze, které posílá Báře, poslat i dalšímu uživateli sítě, např. Dominikovi. Jedné polovině sítě by tedy odeslal požadavek na provedení převodu daných peněz Báře a druhé polovině požadavek na provedení převodu stejných peněz Dominikovi. Zde je řešení zdánlivě jednoduché. Jelikož každý uzel v síti má vlastní kopii blockchainu, je schopen dohledat přesnou historii dané mince od jejího vzniku po aktuální stav. Zároveň je každá transakce opatřená vlastní časovou známkou, která určí, která transakce se provede dřív. Pokud tedy chce Adam poslat nejdřív pětikorunu číslo osm set šedesát sedm Báře, uzly nejdříve ověří, jestli danou pětikorunu má. To je zatím pravda, takže se transakce provede. Pokud ale o vteřinu později bude chtít poslat stejnou pětikorunu Dominikovi, uzly již budou vědět, že vlastníkem pětikoruny číslo osm set šedesát sedm není Adam, ale Bára, a transakce bude zamítnuta<sup>[41]</sup>.

Co se však může stát, je tzv. 51 % Attack, situace, kdy by se Adam domluvil s více než polovinou uzlů dané sítě, které by jeho podvodnou transakci označily jako validní. Jelikož by jich byla většina, Adamovi by to prošlo.

I tento typ útoku však má své meze. Adam sice může zapsat podvodnou transakci do aktuálního bloku, který čeká na vytěžení (připojení do blockchainu), pokud by ale chtěl změnit, přidat nebo odstranit nějakou transakci v již připojeném bloku, nejspíš by neuspěl nebo by se mu to minimálně nevyplatilo. Musel by totiž přehashovat a následně validovat všechny bloky dál od toho, ve kterém něco změnil. A validovace bloku v blockchainu není jen tak, o to se stará tzv. *konsenzus* a proces připojení bloku do blockchainu (těžba)<sup>[16]</sup>. Více o těchto mechanismech v kapitole 1.3.3.

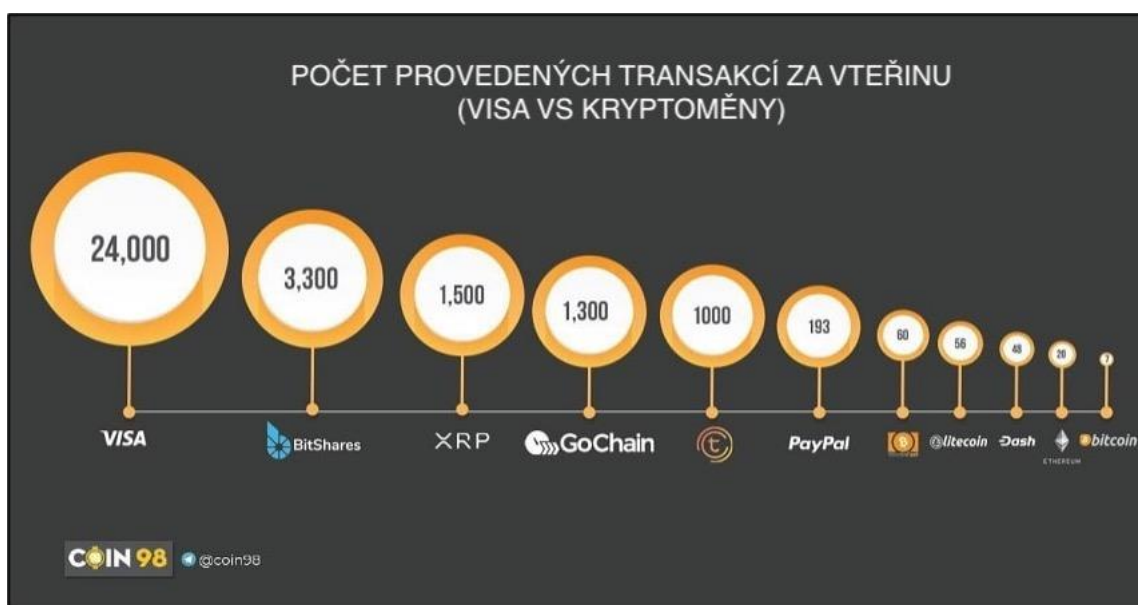
---

<sup>1</sup> Soukromé a veřejné klíče mají i spoustu dalších využití, např. při posílání šifrovaných zpráv, kdy odesílatel svou zprávu zašifruje veřejným klíčem příjemce. Pro ostatní uzly je tak zpráva viditelná jen jako změř znaků, příjemce ji může jako jediný pomocí svého privátního klíče rozšifrovat.



### 1.3.2 Blockchainové transakce v porovnání s centralizovanými systémy

Při porovnávání jednotlivých systémů umožňujících provádět transakce je důležitým faktorem, kolik transakcí je schopen systém provést za sekundu. Zde jsou decentralizované systémy v nevýhodě. Pro porovnání, bitcoinový blockchain je schopen provést zhruba 7 transakcí za sekundu, zatímco VISA jich za stejnou dobu zvládá provést zhruba 24 000<sup>[34],[35][36]</sup>. Na druhou stranu, reálné převedení z účtu na účet u normální banky může trvat dny, blockchain nezná žádnou pracovní dobu a není problém transakci bezpečně převést kdykoli za krátký čas (u bitcoinový blockchain za deset minut). Pokud navíc vezmeme v potaz i další výhody decentralizovaných systémů a fakt, že i blockchain se jako technologie stále vyvíjí a vylepšuje, nejspíš nám nízký počet prováděných transakcí za sekundu nebude tolik vadit.



Obrázek 7: Počet transakcí provedených za sekundu – vede VISA (převzato z <https://blog.tezro.com/wp-content/uploads/2020/11/Compare-The-Transaction-Speed.jpeg>)

Další otázkou je soukromí. Výhodou blockchainu je to, že nemusíme věřit žádné centrální autoritě. Nesmíme však zapomínat, že všechny transakce zapsané do blockchainu jsou veřejně dohledatelné, protože každý z uzlů má vlastní kopii blockchainu. Jistě bychom nechtěli, aby si o nás kdekdo mohl přečíst citlivé informace jako kontaktní údaje nebo naši soukromou adresu, zároveň však potřebujeme jako prodejce vědět, na jakou adresu a komu máme svou elektřinu poslat.

Systémy založené na blockchainu se tak různými metodami snaží dosáhnout alespoň částečné anonymity, např. bitcoinová síť k tomuto účelu používá technologii CoinJoin<sup>[3],[6]</sup>.

### 1.3.3 Konsenzus, těžba

Okolo hradu se nachází několik menších nepřátelských vojsk s různými generály v čele. Aby nepřátelé dobyli hrad, potřebují se vzájemně domlouvat na strategii. Zároveň se však jednotliví generálové navzájem podezřívají ze zrádovství a nemohou si tak dovolit posílat citlivé zprávy jen tak mezi sebou, protože po cestě by zrádce mohl zprávu snadno změnit. Potřebují tedy nějaký mechanismus, který by zamezil podvádění nebo by od toho potenciální zrádce odrazoval.

Tomuto konceptu se říká tzv. problém byzantských generálů<sup>[8]</sup> a s blockchainovou sítí toho má hodně společného. Jako generály si můžeme představit jednotlivé uzly sítě, které se na sebe potřebují vzájemně spoléhat. Předávání důvěrné zprávy poté interpretuje samotné připojení nového bloku do blockchainu. Pokud by byl proces validace a následného připojení bloku jednoduchý, pak by dostatečně silný útočník mohl veškerá data libovolně modifikovat, a validovat celý blockchain zpětně téměř bez práce. I zde potřebujeme zajistit nějakou vzájemnou dohodu mezi uzly, tedy onen *konsenzus*, který by síť chránil před útočníky.

Část bezpečnostních opatření, která jsou součástí konsenzu, byla popsána již v kapitole 1.3.1. Ve stejné kapitole jsem také uvedla, že pro útočníka při 51 % Attacku je téměř nemožné měnit data v již připojených blocích nebo se mu to minimálně nevyplatí. Připojení (těžba) nového bloku totiž od těžařů vyžaduje důkaz, že k vytěžení vynaložili dostatek úsilí. Nejčastěji se jedná o výpočetní výkon (proof of work, PoW) nebo podíl, vratná záloha ve společném kapitálu (proof of stake, PoS). Tyto dva případy si pro lepší interpretaci vysvětlíme zpět na problému byzantských generálů.

Nejprve mechanismus PoS. Aby generálové přežili zradám, domluví se, že vytvoří společný nedotknutelný peněžní fond, do kterého každý generál musí viditelně vložit velkou finanční zálohu. To je sice samo o sobě před podváděním neochrání, ale potencionální zrádci budou viditelně odhaleni, což povede k budoucí nedůvěře (vklad byl proveden veřejně) a následně budou finančně strádat (nebude jim ani vrácena záloha).

Nejběžnějším příkladem využití PoS je síť kryptoměny Ethereum, která od prosince 2020 přechází od původního PoW mechanismu. Každý uzel, který chce připojit nový blok v síti s mechanismem PoS se tedy musí stát ověřovatelem a na začátku vložit do sítě svých 32 ETH (k datu 4.4.2021 je hodnota 1 ETH 2 066,09 USD, 32 ETH tedy má hodnotu zhruba 66 100 USD). Pro vytvoření každého nového bloku je náhodně vybrán jeden uzel. Samozřejmě platí, že čím víc ETH daný uzel vložil a čím déle je ověřovatelem, tím větší je pravděpodobnost, že pro tento úkol bude vybrán. Následně je blok ověřován i ostatními uzly. Když je blok přidán, prvotní uzel dostane odměnu za vytvoření i ověření bloku, další uzly jsou odměněny pouze za ověření. V opačném případě, kdy prvotní uzel podvádí, mu nebude záloha vrácena<sup>[8],[9],[10]</sup>.



Obrázek 8: PoW vs PoS v blockchainových systémech (převzato z [https://innovation.network/wp-content/uploads/2020/09/Proof\\_of\\_Work\\_vs\\_Proof\\_of\\_Stake5.jpg](https://innovation.network/wp-content/uploads/2020/09/Proof_of_Work_vs_Proof_of_Stake5.jpg))

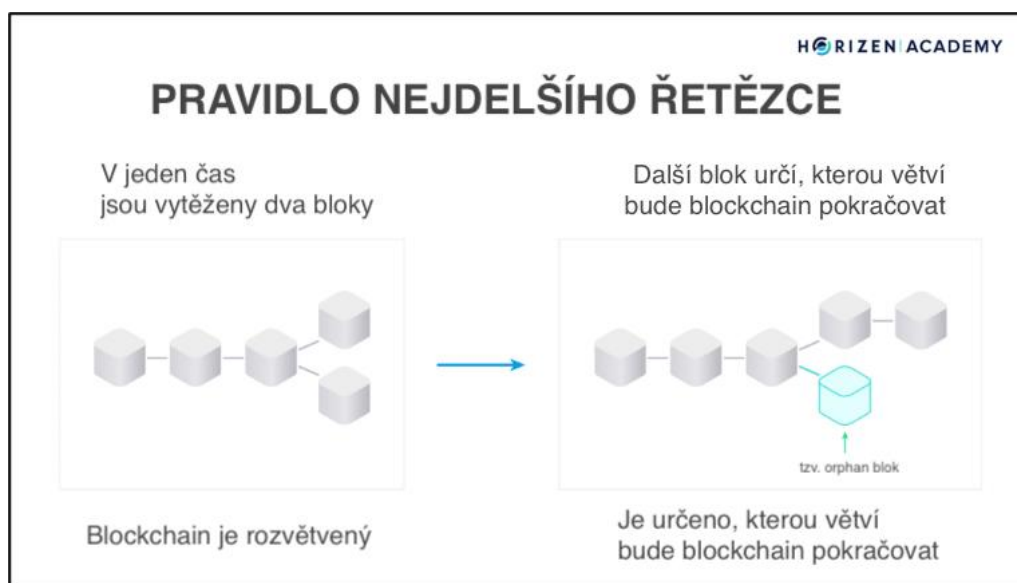


PoW funguje na principu extrémně náročných matematických hádanek. Aby mohl některý generál ostatním poslat zprávu, musí k ní připojit řešení daného matematického problému. To od něj však vyžaduje investici do matematiků, kteří mu pomohou hádanku vyřešit. Pokud tedy jiný generál obdrží zprávu se správným řešením hádanky, ví, že pisateli zprávy zjevně stálo za to investovat do vlastních matematiků, kteří vypočítali výsledek.

Tento mechanismus je využíván v bitcoinové síti. Jednotliví těžaři mezi sebou soutěží o to, kdo najde řešení matematické hádanky<sup>2</sup> a připojí tak blok jako první. Ten, kdo takto blok vytěží, dostane odměnu. Tato odměna se obvykle skládá z fixní částky nastavené sítí a transakčních poplatků.

Pokud by tedy útočník chtěl měnit nějaká data v bloku, který již úspěšně prošel procesem připojení, změnil by i hash daného bloku a musel by daný blok (a případně všechny následující bloky) přehashovat a zpětně validovat, což by se mu prostě nevyplatilo. Navíc, pokud se podíváme např. na bitcoinový blockchain a jeho PoW, zjistíme, že výpočetním výkonem, který by byl schopen zpětně validovat blockchain do větší hloubky, žádný těžař nikdy nemůže disponovat. Logicky, čím hlouběji blok v blockchainu je, tím náročnější je v něm něco změnit.

Zajímavá situace nastává v případě, kdy dva těžaři vytěží blok ve stejnou chvíli. Zde samozřejmě lze postupovat vícero způsoby, pro příklad uvedu tzv. pravidlo nejdelšího řetězce, kdy se počká na vytěžení následujícího bloku, který se připojí na jeden z nich. Blockchain dále bude pokračovat touto „delší“ větví a druhý nevyužitý blok (tzv. *orphan* blok) v blockchainu nebude dále participovat.



Obrázek 9: Pravidlo nejdelšího řetězce

(převzato z [https://academy.horizen.io/assets/post\\_files/technology/advanced/2.5-consensus-mechanisms/longest\\_chain\\_M.jpg](https://academy.horizen.io/assets/post_files/technology/advanced/2.5-consensus-mechanisms/longest_chain_M.jpg))

---

<sup>2</sup> V bitcoinovém blockchainu je PoW založen na hledání hashe daného bloku s určitým předpisem. Jak jsem vysvětlovala dříve v této kapitole, hash je však pro data jednoho bloku vždy stejný, proto je potřeba do každého bloku přidat nějaký kousek dat, který neovlivní „důležité“ informace v něm (transakce a časovou známku), zároveň ale umožní obsah bloku modifikovat. K tomu slouží atribut *nonce*. Při každém pokusu o nalezení vhodného hashe se za *nonce* dosadí jiné číslo, což hash změní. Když hash odpovídá předpisu, blok je připojen.

## 2 MŮJ BLOCKCHAIN

### 2.1 Použité programovací jazyky

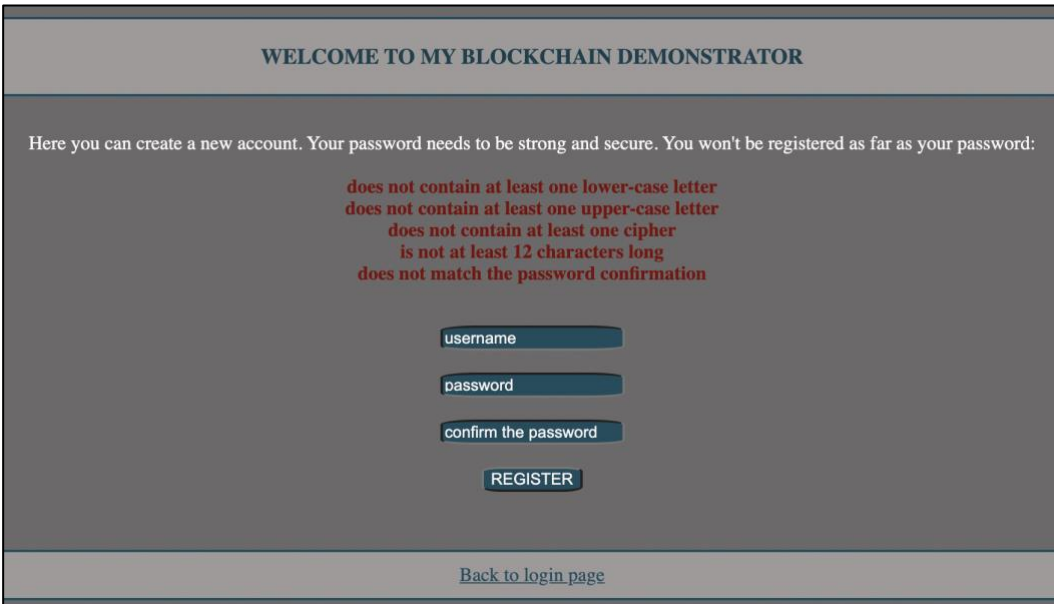
K vytvoření své aplikace jsem se rozhodla využít programovací jazyk Python – především pro jeho jednoduchost, rozšířenost a až nucenou přehlednost. Významnou roli ve výběru také hrál fakt, že před psaním práce jsem s Pythonem měla již nějaké zkušenosti.

Pro tvorbu základního grafického rozhraní jsem připojila pár HTML souborů a jeden soubor s kaskádovými styly.

### 2.2 Aplikace

#### 2.2.1 Založení účtu, přihlášení

Pro využívání demonstrátoru je nutné se bezplatně zaregistrovat do uživatelské databáze (Flask-*SQLAlchemy*<sup>3</sup>).



Obrázek 10: Screenshot z aplikace – založení účtu

Při registraci si uživatel zvolí jméno, kterým se bude do aplikace přihlašovat. Musí být jedinečné, maximální délka je dvacet znaků. Dále si zvolí heslo, které musí splňovat následující bezpečnostní kritéria (funkce *my\_secure\_pasw(pasw)*, viz Příloha 1):

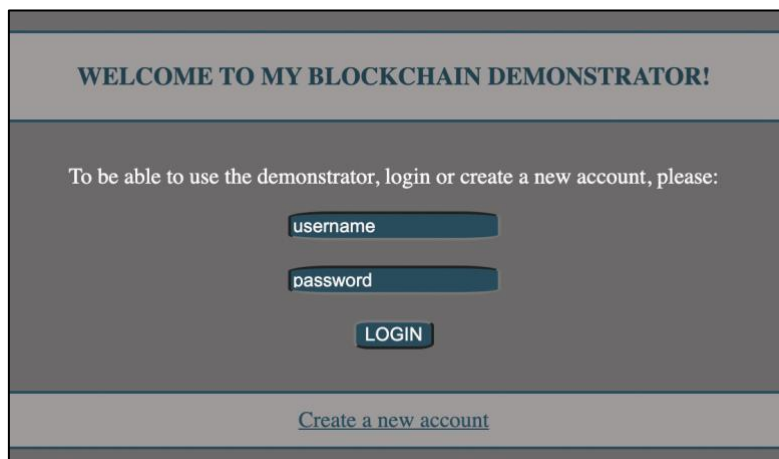
- Heslo obsahuje alespoň jedno malé písmeno (latinka).
- Heslo obsahuje alespoň jedno velké písmeno (latinka).
- Heslo obsahuje alespoň jednu číslici (arabskou).
- Heslo je alespoň 12 znaků dlouhé.

---

<sup>3</sup> [https://passlib.readthedocs.io/en/stable/lib/passlib.hash.pbkdf2\\_digest.html#passlib.hash.pbkdf2\\_sha256](https://passlib.readthedocs.io/en/stable/lib/passlib.hash.pbkdf2_digest.html#passlib.hash.pbkdf2_sha256)

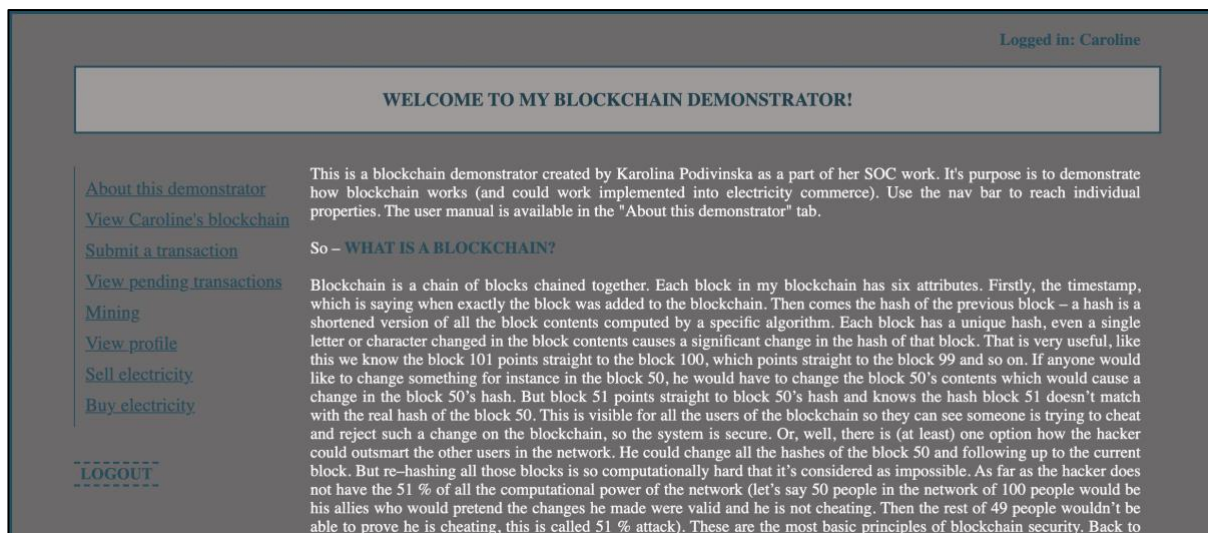
Následně je uživatel zaregistrován a jeho jméno společně s heslem v zašifrované formě (tj. výstup funkce `pbkdf2_sha256.hash()`<sup>4</sup>, kdy vstupem je heslo v běžné formě) uložena v uživatelské databázi. To umožňuje uchovávat v databázi pouze zašifrovanou podobu, nikoliv hesla samotná. Zároveň je však možné snadno rozpoznat, zda bylo heslo na vstupu zadáno správně. Systém neumožňuje obnovovat uživatelské účty.

Pro přihlášení uživatel zadá jméno a heslo, které je prostřednictvím funkce `pbkdf2_sha245.verify()`<sup>5</sup> porovnáno s jeho zašifrovanou formou uloženou v databázi.



Obrázek 11: Screenshot z aplikace – přihlašovací formulář

Pokud zadá data správně, je přesměrován na domovskou stránku, kde má k dispozici rozcestník dalších stránek aplikace a také text popisující základy technologie blockchain. Veškeré texty v aplikaci i zdrojový kód jsou napsány v anglickém jazyce. Pokud uživatel zadá data špatně, aplikace mu pomocí *flash message* sdělí, co zadal špatně, a vyzve ho k opětovnému pokusu.



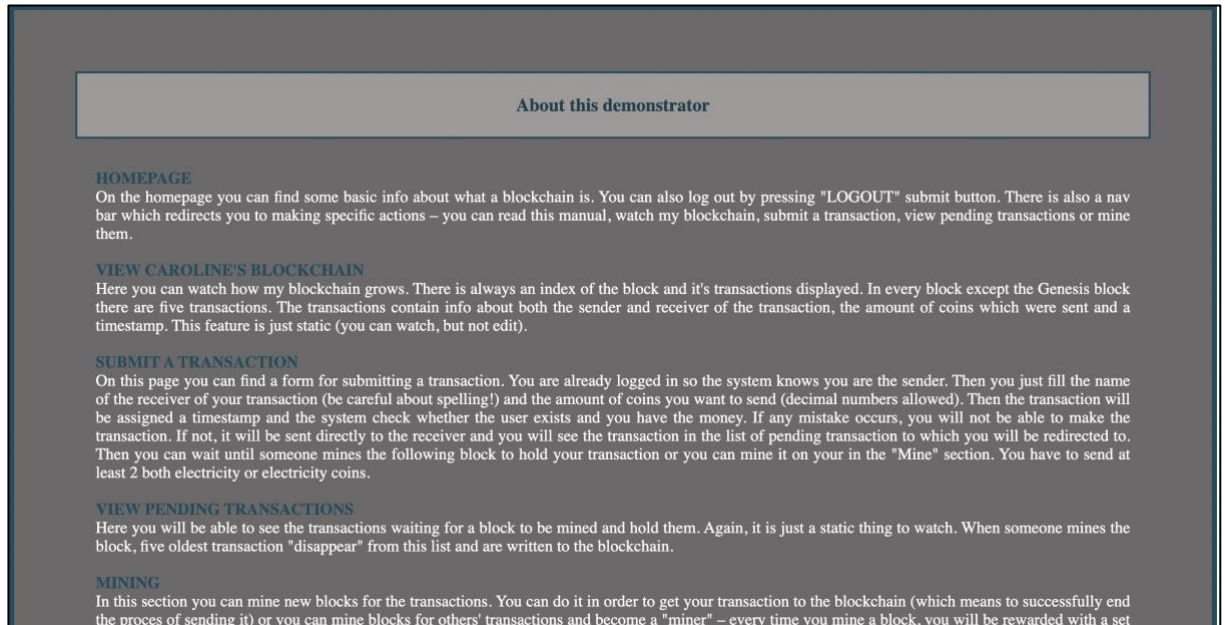
Obrázek 12: Screenshot z aplikace – domovská stránka

<sup>4</sup> [https://passlib.readthedocs.io/en/stable/lib/passlib.hash.pbkdf2\\_digest.html](https://passlib.readthedocs.io/en/stable/lib/passlib.hash.pbkdf2_digest.html)

<sup>5</sup> <https://passlib.readthedocs.io/en/stable/lib/passlib.ifc.html#passlib.ifc.PasswordHash.verify>

## 2.2.2 About this demonstrator

Statická stránka *About this demonstrator* má za úkol uživateli poskytnout základní manuál pro používání aplikace. Obsahuje seznam stránek a krátký popis toho, k čemu každá z nich slouží.



Obrázek 13: Screenshot z aplikace – základní manuál pro uživatele

## 2.2.3 View Caroline's blockchain

Stránka *View Caroline's blockchain* zobrazuje jednotlivé bloky blockchainu. U každého bloku se zobrazuje jeho pět atributů. Prvním z nich *index*, tedy výška bloku v blockchainu, následuje *hash* daného bloku a *pre\_hash*, tedy hash předchozího bloku (u genesis bloku 0), *timestamp* udávající čas, kdy byl blok připojen do blockchainu. Skrytým atributem je *counter*, který je používán při těžbě. Nejdůležitějším atributem je samozřejmě *trans*, seznam transakcí zapsaných v bloku.

Každá transakce má rovněž svůj index a časovou známku, dále informace o jejím odesílateli, příjemci a množství odeslaných tokenů. Skrytým atributem je *signature*, její digitální podpis (1.3.1).

Tato stránka musí fungovat dynamicky (na rozdíl od statických stránek semusí aktualizovat na všech počítačích, které aplikaci využívají, protože její obsah se mění), jinak by každý uzel měl vlastní blockchain. To zajišťuje funkce *get\_chain()*, která vrací jako návratovou hodnotu stávající blockchain každého uzlu (počítače) v síti. Ty se mezi sebou ve funkci *blockchain()* vzájemně porovnávají, aktualizují a sjednotí – jako platný je označen nejdelší platný blockchain (viz Příloha 2).



Obrázek 14: Screenshot z aplikace – výpis blockchainu

## 2.2.4 Submit a transaction

*Submit a transaction* slouží k zadání jednoduché transakce. Každá transakce mého blockchainu má svého odesílatele (přihlášený uživatel), příjemce (*receiver*) a množství tokenů, které jsou odesílány (*amount of coins*, může být i desetinné číslo). Uživatel rovněž musí specifikovat, jestli posílá tokeny elektřiny nebo peněžní tokeny. K tomu slouží rozbalovací nabídka vedle odesílacího tlačítka *SEND*. Transakce je rovněž opatřena časovou známkou a vlastním hashem.

Pokud se uživatel pokusí poslat tokeny sám sobě, neexistujícímu uživateli nebo bude chtít odeslat množství tokenů, které nevlastní, aplikace ho na to prostřednictvím *flash message* upozorní a transakce nebude provedena.

Submit a transaction

This is an easy form for submitting a new transaction. Type the receiver of your transaction and then the amount of money you want to send (decimal numbers allowed)

**Be carefull, this action is irreversible. Reciever's address is case sensitive.**

receiver

amount of coins

Money ▼ SEND

[Back to homepage](#)

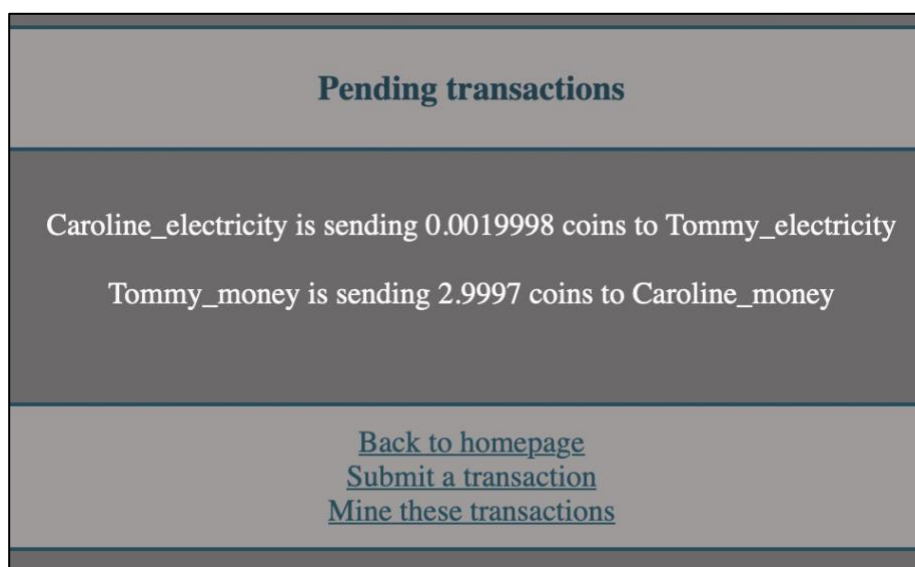
Obrázek 15: Screenshot z aplikace – formulář pro zadání jednoduché transakce

## 2.2.5 View pending transactions

Poté, co uživatel zadal požadavek na provedení transakce, transakce se přidá do pole neověřených transakcí blockchainu, kde bude čekat na připojení do bloku. Na stránce *View pending transactions* se právě tyto transakce zobrazují<sup>6</sup>.

Jestliže daná transakce byla provedena s peněžními tokeny, za uživatelská jména příjemce i odesílatele se přidá přípona *\_money*, aby bylo jasné, o jaký druh tokenů se jedná. Pokud jsou odesílány tokeny elektřiny, přípona má tvar *\_electricity*.

Speciálním případem jsou transakce odesílatele *Reward For The Miner*. U něj totiž žádná přípona není, jelikož se jedná o transakci připisující odměnu pro těžaře, která je vyplácena vždy v tokenech elektřiny (nejedná se o právoplatného uživatele, ale jen zástupné jméno – žádný skutečný uživatel toto jméno používat nesmí, aby se zamezilo zmatkům a chybám při záměně uživatelských transakcí za ty určené těžařům od systému a naopak).



Obrázek 16: Screenshot z aplikace – vypisování čekajících transakcí

Aby bylo možné zobrazovat tyto čekající transakce a těžit nové bloky všemi uzly, *View pending transactions* se stejně jako celý blockchain (2.2.3) musí aktualizovat.

## 2.2.6 Mining

Stránka *Mining* je určená pro těžbu. Vypadá velmi podobně jako *View pending transactions*, ze které sem lze přímo přejít – také vypisuje transakce čekající na připojení do bloku. Rozdílem je, že pomocí tlačítka *MINE* může uživatel dané transakce připojit do nového bloku a vytěžit ho.

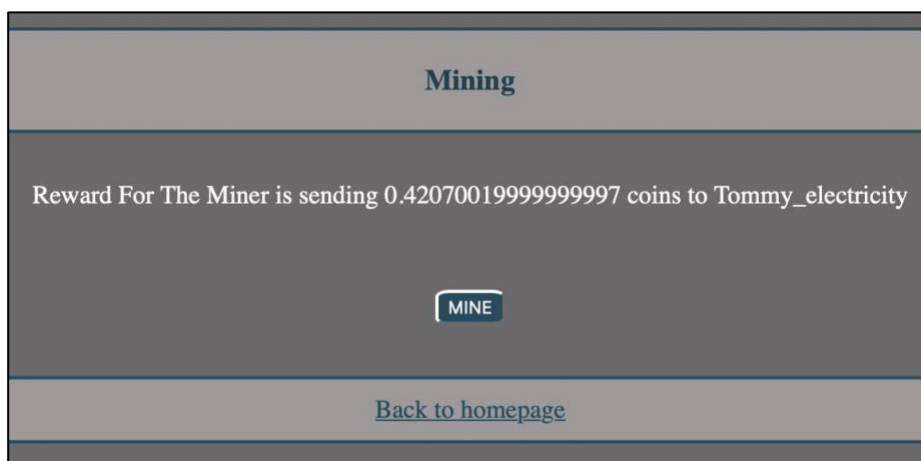
Můj blockchain je nastavený tak, že v každém bloku je uloženo přesně pět transakcí. Pokud tedy uživatel chce těžit blok s méně než pěti transakcemi, je upozorněn, že transakcí není dostatek, a nebude mu umožněno akci provést. Jestliže chce těžit blok, když je v systému

---

<sup>6</sup> Účelově se nezobrazuje celá odesílaná částka, jedná se o podklad k budoucímu řešení vyplácení transakčních poplatků těžařům

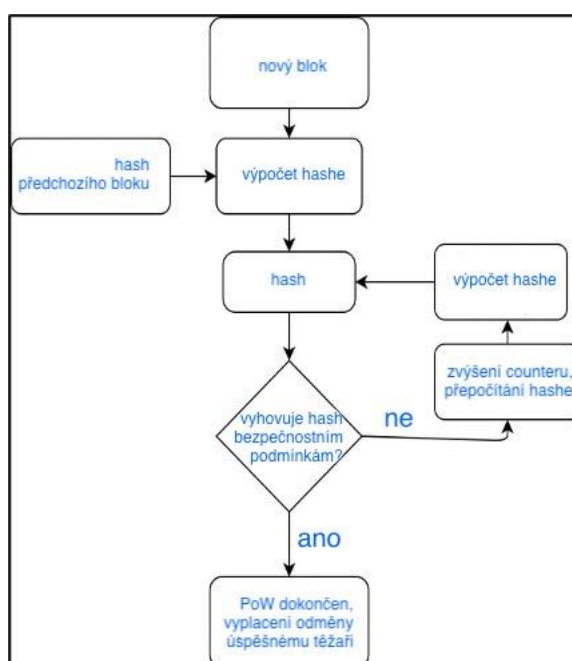


více čekajících transakcí, prostě vytěží blok, do kterého se uloží prvních pět. Tyto transakce jsou tak napevno uloženy v blockchainu a smazány z pole čekajících transakcí.



Obrázek 17: Screenshot z aplikace – stránka Minig po čerstvém vytěžení bloku

Ve svém blockchainu jsem jako algoritmus pro těžbu zvolila PoW, tedy důkaz prací – především pro jeho jednoduchost. Když má být vytěžen nový blok, jeho atribut *counter* je na hodnotě nula. Těžař s pomocí výpočetní síly jeho stroje vypočítá hash nad obsahem daného bloku. Pokud tento hash neodpovídá nastaveným kritériím (počet nul, které musí být na prvních x znacích hashe), *counter* bloku je zvýšen o jedna a těžař opakuje výpočet. Pokud uspěje a je první, kdo najde uspokojivý hash a vytěží tak daný blok, vytvoří se nová transakce připisující mu odměnu.



Obrázek 18: PoW algoritmus

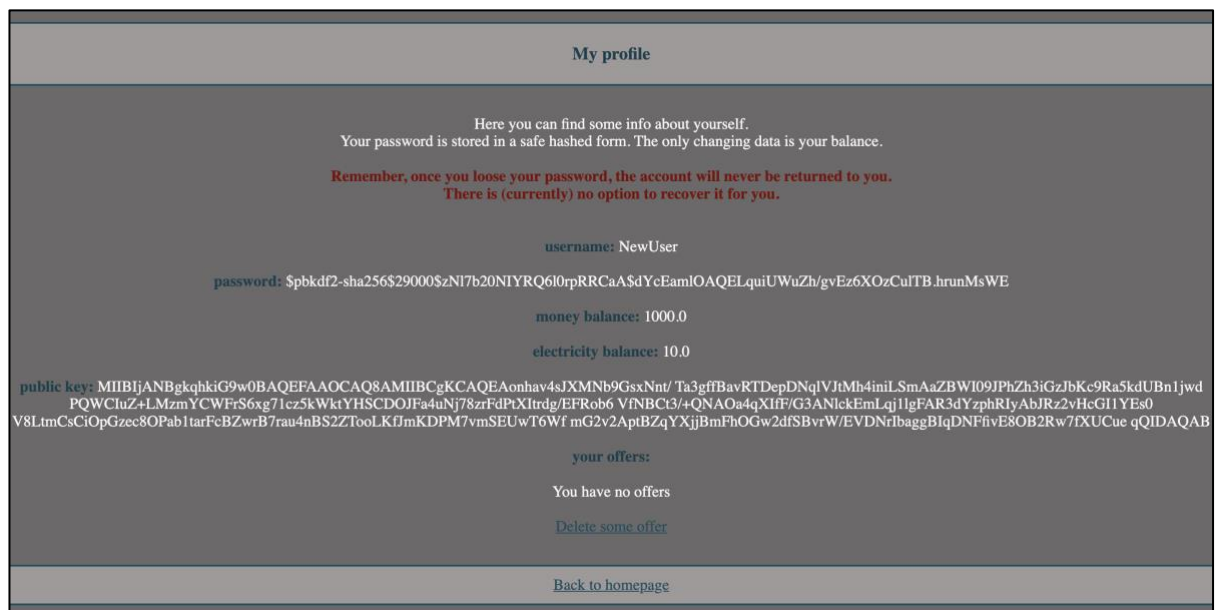
(převzato z [https://www.researchgate.net/publication/331040157\\_A\\_Survey\\_on\\_Bitcoin\\_Cryptocurrency\\_and\\_its\\_Mining](https://www.researchgate.net/publication/331040157_A_Survey_on_Bitcoin_Cryptocurrency_and_its_Mining))

## 2.2.7 View profile

Na stránce *View profile* uživatel vidí své jméno, heslo v zašifrované formě, zůstatek peněžních tokenů a tokenů elektřiny, svůj veřejný klíč a seznam nabídek na prodej elektrických tokenů, které vytvořil. Zde má také možnost tyto nabídky stornovat.

Po založení účtu každý uživatel má na svém kontě 1 000 peněžních tokenů a 10 tokenů elektřiny, se kterými může obchodovat nebo provádět běžné transakce. Jsou mu též přiděleny klíče, kterými následně podepisuje své transakce (viz kapitola 1.3.1).

Každý uživatel se tak může stát kupujícím, prodávajícím, těžařem i účastníkem běžných transakcí a vidí data veřejně uložená v blockchainu. Jako uzel decentralizované sítě blockchain rovněž aktualizuje a pomáhá odhalit případné chyby.



Obrázek 19: Screenshot z aplikace – profil nového uživatele

## 2.2.8 Sell electricity

*Sell electricity* slouží k vytváření nabídek k prodeji vlastní elektrické energie. Prodejce zvolí, kolik tokenů elektřiny chce prodávat (*sell electricity*) za jakou částku (*receive money*). Obě částky lze zvolit jako desetinná čísla. Systém zkontroluje, zda prodávající dané tokeny elektřiny má a následně vytvoří objekt typu *Offer*, který ještě obsahuje atribut *retailer* identifikující prodávajícího (jméno přihlášeného uživatele, který nabídku vytvořil).

Každá nabídka dostane svůj index, číslo, podle kterého je možné nabídky na stránce *View profile* stornovat (daný uživatel pochopitelně může stornovat pouze své nabídky) a na stránce *Buy electricity* je naopak využívat.



Tokeny elektřiny, které prodejce nabízí, se dočasně umístí do pole *trading\_storage* a celá nabídka do pole *trading\_data* na blockchainu, aby se zamezilo případu, kdy si uživatel chce koupit tokeny elektřiny od prodejce, který už je v danou dobu nemá.

The screenshot shows a web form titled "Sell electricity". Below the title is a grey box containing the text: "This is an easy form for submitting an offer. Type the amount of electricity you want to sell (decimal numbers allowed) and then the amount of money you want to receive from the buyer." Below this text are two input fields: "sell electricity" and "receive money". Below these fields is a "SEND" button. At the bottom of the form is a link "Back to homepage".

Obrázek 20: Screenshot z aplikace – formulář pro založení nabídky

Po validním založení nabídky je uživatel přesměrován na stránku *Buy electricity*, kde se může ujistit, že jeho nabídka byla v pořádku zařazena do seznamu nabídek.

## 2.2.9 Buy electricity

Stránka *Buy electricity* slouží k využívání nabídek, tedy k nakupování tokenů elektřiny za peněžní tokeny od ostatních uživatelů.

The screenshot shows a web page titled "Buy electricity". Below the title is a grey box containing the text: "Here is the list of offers. If you want to make a purchase, remember the name of the offer and click BUY." Below this text is a list of offers:

- 0. Tommy offers to sell 2 electricity coins for 20 money coins
- 1. Caroline offers to sell 3 electricity coins for 40 money coins

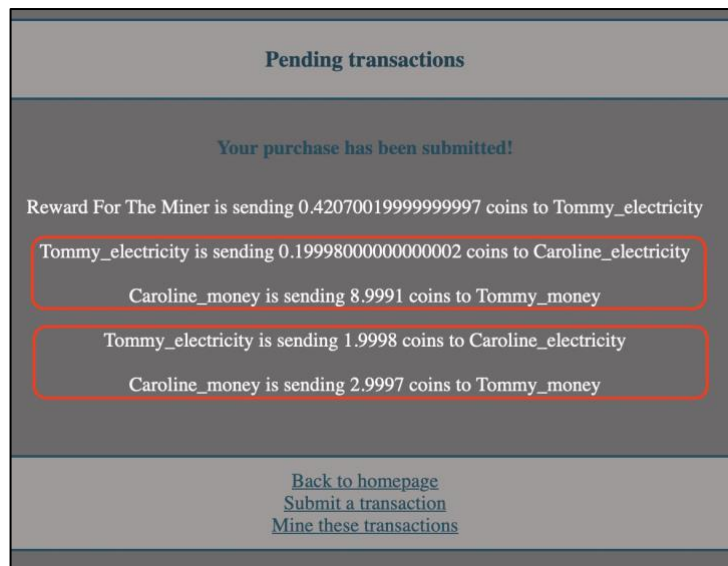
Below the list is a "BUY" button. At the bottom of the page is a link "Back to homepage".

Obrázek 21: Screenshot z aplikace – výpis nabídek

Jak již bylo řečeno v kapitole 2.2.8, každá nabídka je opatřena číslem, které udává její index v poli nabídek na blockchainu. Pokud chce uživatel některou nabídku využít, zapamatuje si její číslo a po stisknutí tlačítka *BUY* ho zadá. Systém zkontroluje, zda kupující zadal číslo existující objednávky a zda má na nákup dostatek peněžních tokenů. Pokud tomu tak je, jsou ve stejný čas vytvořeny dvě transakce – jedna v peněžních tokenech od kupujícího prodejci, druhá v tokenech elektřiny od prodejce (resp. z pole *trading\_data*) kupujícím. Nabídka poté již poté

není pro ostatní zájemce dostupná. Pokud kupující udělal při zadávání chybu, znovu je upozorněn prostřednictvím *flash message* a není mu umožněno nákup dokončit.

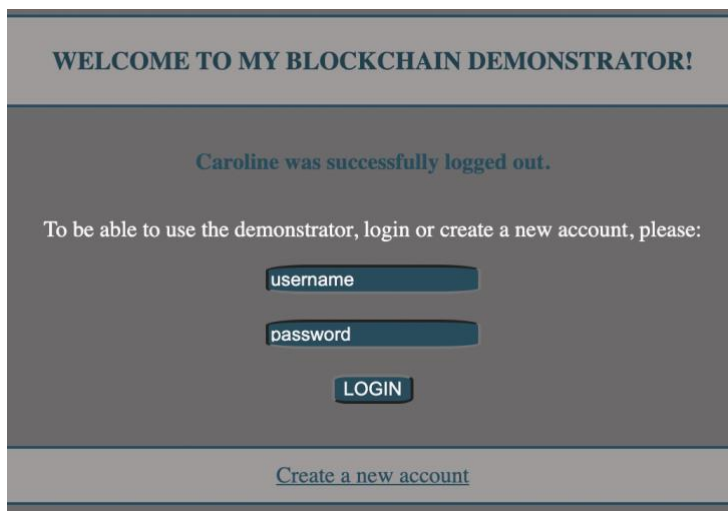
I *Buy electricity* se mezi uživateli musí aktualizovat podobně jako u *View Caroline's blockchain* nebo *View pending transactions* (2.2.3).



Obrázek 22: Screenshot z aplikace – situace po dvojitém nákupu prostřednictvím nabídky

## 2.2.10 Logout

Po stisknutí tlačítka *LOGOUT* na domovské stránce je uživatel odhlášen z aplikace a přesměrován na přihlašovací stránku pro možnost opětovného přihlášení.



Obrázek 23: Screenshot z aplikace – úspěšné odhlášení z aplikace

## ZÁVĚR, DISKUSE

V úvodu práce jsem si za cíl stanovila vytvořit funkční, interaktivní aplikaci popisující a ilustrující koncepty technologie blockchain. To se mi podařilo, naprogramovala jsem aplikaci Caroline's Blockchain Demonstrator (bez webhostingu), zdrojové kódy jsou dostupné pod odkazem [https://github.com/Caroline2/blockchain\\_demonstrator](https://github.com/Caroline2/blockchain_demonstrator).

Aplikace je funkční a splňuje účel, ke kterému byla naprogramovaná, tedy k demonstraci jednoduchého obchodování s elektřinou v prostředí založeném na blockchainu. Umožňuje interakci s uživatelem prostřednictvím základního grafického rozhraní, kde jsou k dispozici i základní informace o technologii blockchain a funkcionalitách aplikace. Uživatelům je umožněno uskutečňovat přímé transakce, vystavovat nabídky na prodej tokenů elektřiny nebo tyto tokeny kupovat, těžit nové bloky a samozřejmě zobrazovat samotný blockchain.

Za její hlavní přínos považuji to, že je volně dostupná a umožňuje tak komukoli vyzkoušet přehledně si vyzkoušet, jak funguje systém založený na blockchainu – ať už v onom kontextu obchodu s elektřinou nebo třeba v kontextu úplně jiném, kdy má aplikace bude sloužit jen jako inspirace či prvotní zdrojový kód. Aplikace totiž poskytuje spoustu prostoru pro vylepšení nebo případnou modifikaci, ať už je to již zmíněné převedení aplikace do webového prostředí, implementace odlišného konsenzu, grafická úprava, vyšší zabezpečení nebo třeba přidání dalších funkcionalit apod. V budoucích měsících či letech zvažuji její další vývoj.

Mým druhým cílem bylo předložit koncept a výhody užití technologie blockchain v odvětví obchodu s elektřinou. Tento cíl jsem rovněž splnila, popsala jsem, jak se tato technologie v odvětví obchodu s elektřinou již uplatňuje a v čem tkví její výhody.

## POUŽITÁ LITERATURA, ZDROJE

- [1] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1.
- [2] DRESCHER, Daniel. *Blockchain basics: A non-technical introduction in 25 steps* [online]. Berkeley, California: Apress, [2017] [cit. 2019-10-29]. ISBN 978-1-4842-2603-2.
- [3] BASHIR, Imran. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained* [online]. 2. Birmingham: Packt Publishing, 2018 [cit. 2021-02-21]. ISBN 978-1788839044. Dostupné z: <https://1lib.cz/book/4998840/bf08d0?regionChanged=&redirect=180740510>
- [4] SZEWCZYKOVÁ, Julie. *Vybrané aspekty bitcoinu a jeho implikace pohledem práva a ekonomie* [online]. Praha, 2018 [cit. 2019-10-07]. Dostupné z: <https://dspace.cuni.cz/handle/20.500.11956/104859>. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Doc. Ing. Helena Chytilová, M.A., Ph.D.
- [5] ROMANENKO, Pavel. 20 Blockchain Use Cases for 2018 You Should Know: Lessons learned from the Blockchain Circle's workshop. In: *IT Slovník* [online]. 2018, 11. 12. [cit. 2021-02-20]. Dostupné z: <https://hackernoon.com/20-blockchain-use-cases-for-2018-you-should-know-f7d2919c191d>
- [6] CoinJoin. In: *Open Bitcoin Privacy Project Wiki: notes on bitcoin privacy technology* [online]. [cit. 2021-02-23]. Dostupné z: <http://wiki.openbitcoinprivacyproject.org/topics/coinjoin>
- [7] FENCL, Ivan. Blockchain a virtuální měny: I. část. In: *Právo pro podnikatele: Advokátní kancelář* [online]. 2019, 22. 7. [cit. 2021-02-20]. Dostupné z: <https://pravopropodnikatele.cz/blockchain-a-virtualni-meny-i-cast/>
- [8] HAYS, Demelza. Consensus Mechanism. In: *Crypto Research Report* [online]. 2018, 17. 6. [cit. 2021-02-20]. Dostupné z: <https://cryptoresearch.report/crypto-research/consensus-mechanisms/>
- [9] ANURAG. 8 Famous Blockchain Consensus Mechanisms and their Benefits. In: *NewGenApps: Enabling Smarter Communication with AI* [online]. 2018, 19. 4. [cit. 2021-02-20]. Dostupné z: <https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits/>
- [10] WON, Daniel. Ethereum Proof of Stake Date: Date + What You Need to Know. In: *Exodus Crypto Blog* [online]. 2020, 24. 2. [cit. 2021-02-22]. Dostupné z: <https://www.exodus.com/blog/ethereum-proof-of-stake-date/>
- [11] Favicon. In: *Favicon Icons: Free Download, PNG and SVG* [online]. [cit. 2021-02-20]. Dostupné z: <https://icons8.com/icons/set/favicon>
- [12] KUMAR, Bijay. Python Get An IP address. In: *Python Tutorials: Learn Python Free* [online]. 2020, 20. 10. [cit. 2021-02-20]. Dostupné z: <https://pythonguides.com/python-get-an-ip-address/>

- [13] TECRACOIN. What is Genesis Block and why Genesis Block is needed? In: *Tetra Coin: Science, not Fiction* [online]. 2019, 18. 9. [cit. 2021-02-20]. Dostupné z: <https://tecracoin.medium.com/what-is-genesis-block-and-why-genesis-block-is-needed-1b37d4b75e43>
- [14] Bitcoin Glossary. In: *Blockchain: Support Center* [online]. 2013– [cit. 2021-02-20]. Dostupné z: <https://support.blockchain.com/hc/en-us/articles/213276463-Bitcoin-Glossary>
- [15] Blockchain. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001– [cit. 2021-02-20]. Dostupné z: <https://en.wikipedia.org/wiki/Blockchain>
- [16] FRANKENFIELD, Jake. 51% Attack [online]. In: *Investopedia: Sharper Insight, better investing* [online]6. 5. 2019 [cit. 2019-12-22]. Dostupné z: <https://www.investopedia.com/terms/1/51-attack.asp>
- [17] CONWAY, Luke. Blockchain Explained. In: *Investopedia: Sharper Insight, better investing* [online]. 2020, 17. 12. [cit. 2021-03-24]. Dostupné z: <https://www.investopedia.com/terms/b/blockchain.asp>
- [18] BITCOINOVEJ KANÁL. #5 - Co je Bitcoin? A jak funguje blockchain? In: *YouTube* [online]. 2019, 12. 3. [cit. 2021-02-10]. Dostupné z: <https://www.youtube.com/watch?v=KSKY1P9qLk4>
- [19] SIMPLY EXPLAINED. How does a blockchain work: Simply Explained. In: *YouTube* [online]. 2017, 13. 11. [cit. 2021-02-10]. Dostupné z: [https://www.youtube.com/watch?v=SSo\\_EIwHSd4](https://www.youtube.com/watch?v=SSo_EIwHSd4)
- [20] SKALEX. Bitcoin Glossary: What is a Genesis Block? In: *YouTube* [online]. 2019, 27. 2. [cit. 2021-02-10]. Dostupné z: <https://www.youtube.com/watch?v=WAI0cPA0EBk>
- [21] 3BLUE1BROWN. But how does bitcoin actually work? In: *YouTube* [online]. 2017, 7. 7. [cit. 2021-02-10]. Dostupné z: <https://www.youtube.com/watch?v=bBC-nXj3Ng4>
- [22] LENKA, Chinmoy. Python program to check the validity of a Password. In: *GeeksforGeeks* [online]. 2020, 29. 12. [cit. 2021-02-10]. Dostupné z: <https://www.geeksforgeeks.org/python-program-check-validity-password/>
- [23] SATWIKKANSAL. Python\_blockchain\_app. In: *GitHub* [online]. 2020, 25. 2. [cit. 2021-02-10]. Dostupné z: [https://github.com/satwikkansal/python\\_blockchain\\_app/tree/ibm\\_blockchain\\_post](https://github.com/satwikkansal/python_blockchain_app/tree/ibm_blockchain_post)
- [24] DVF. Blockchain. In: *GitHub* [online]. 2018, 16. 2. [cit. 2021-02-10]. Dostupné z: <https://github.com/dvf/blockchain/blob/master/blockchain.py>
- [25] PALLETS. Flask. In: *GitHub* [online]. 2020, 3. 4. [cit. 2021-02-10]. Dostupné z: <https://github.com/pallets/flask>
- [26] GOLAMI, Somayyeh. Implementing-Smart-Blockchain. In: *GitHub* [online]. 2020, 16. 4. [cit. 2021-02-10]. Dostupné z: <https://github.com/SomayyehGholami/Implementing-Smart-Blockchain>
- [27] DOUBEK, Michal. Má dnes ještě smysl změnit dodavatele elektřiny?: Pavel Morávek (ENEKA). In: *YouTube* [online]. 2020, 28. 9. [cit. 2021-04-02]. Dostupné z: <https://www.youtube.com/watch?v=7q1hv0TZxac>
- [28] Dodavatelé elektřiny: Abecední seznam společností. In: *Elektrina.cz* [online]. 2014– [cit. 2021-04-02]. Dostupné z: <https://www.elektrina.cz/dodavatele-elektriny/>

- [29] ŠÁLAMOVÁ, Michaela. Dodavatelé elektřiny. In: *Ušetřeno.cz* [online]. 2020, 20. 1. [cit. 2021-04-02]. Dostupné z: <https://www.usetreno.cz/dodavatele-elektriny/>
- [30] SHIPWORTH, David. Peer-to-peer energy trading using blockchains. In: *YouTube* [online]. 2017, 27. 6. [cit. 2021-04-02]. Dostupné z: <https://www.youtube.com/watch?v=AcufQeaOK1U&t=2541s>
- [31] EW-DOS: The Energy Web Decentralized Operating System: An Open-Source Technology Stack to Accelerate the Energy Transition. PART 1: Vision & Purpose. In: *Energy Web* [online]. 2020 [cit. 2021-04-02]. Dostupné z: <https://energyweb.org/wp-content/uploads/2019/12/EnergyWeb-EWDOS-PART1-VisionPurpose-202006-vFinal.pdf>
- [32] What is Peer-to-Peer Energy Trading? In: *Infinite Energy* [online]. 2020, 1. 3. [cit. 2021-04-02]. Dostupné z: <https://www.infiniteenergy.com.au/peer-to-peer-energy-trading/>
- [33] TUSHAR, Wayes, Tapan K. SAHA, Chau YUEN, David SMITH a H. Vincent POOR. Peer-to-Peer Trading in Electricity Networks: An Overview. In: *Arxiv* [online]. 2020, 19. 1. [cit. 2021-04-02]. Dostupné z: <https://arxiv.org/pdf/2001.06882.pdf>
- [34] Cryptocurrency Transaction Speeds in 2020. In: *Tezro* [online]. 2020, 3. 11. [cit. 2021-04-02]. Dostupné z: <https://blog.tezro.com/cryptocurrency-transaction-speeds/>
- [35] Crypto vs Visa: transactions' speed compared. In: *PaySpace Magazine* [online]. 2020, 20. 1. [cit. 2021-04-02]. Dostupné z: <https://payspacemagazine.com/cryptocurrency/crypto-vs-visa-transactions-speed-compared/>
- [36] RIETH, Yulia. Payment Systems: Visa vs. Bitcoin. In: *DeCenter* [online]. 2018, 6. 6. [cit. 2021-04-02]. Dostupné z: <https://decenter.org/en/payment-systems-visa-vs-bitcoin>
- [37] IRVINE, Will. And The Extreme Tech Challenge 2018 winner is...: Extreme Tech Challenge (XTC) announces 2018 winner of its fourth annual competition. In: *Slingshot sponsorship* [online]. 2018, 25. 10. [cit. 2021-04-02]. Dostupné z: <https://www.slingshotsponsorship.com/and-the-extreme-tech-challenge-2018-winner-is/>
- [38] We're Power Ledger. In: *Power Ledger* [online]. [cit. 2021-04-02]. Dostupné z: <https://www.powerledger.io/company/about>
- [39] A blockchain innovation with the goal of a green energy future. In: *Suncontract* [online]. [cit. 2021-04-02]. Dostupné z: <https://suncontract.org/about-suncontract-blockchain-project/>
- [40] Šablona práce. In: *SOČ: středoškolská odborná činnost* [online]. 2020 [cit. 2021-04-02]. Dostupné z: <https://www.soc.cz/sablona-soc/sablona-prace/>
- [41] Šablona SOČ. In: *SOČ: středoškolská odborná činnost* [online]. [cit. 2021-04-02]. Dostupné z: [http://www.soc.cz/dokumenty/sablona\\_SOC.docx](http://www.soc.cz/dokumenty/sablona_SOC.docx)
- [42] HUBÍK, Jan. Bitcoin meetup: Jak funguje blockchain? In: *YouTube* [online]. 2018, 23. 7. [cit. 2021-04-02]. Dostupné z: <https://www.youtube.com/watch?v=nvTodoUyiWU>
- [43] NATHAN-149. CustomCryocurrency: gymcoin. In: *GitHub* [online]. 2019, 6. 6. [cit. 2021-04-03]. Dostupné z: <https://github.com/nathan-149/CustomCryocurrency/tree/master/gymcoin>
- [44] WACKEROW, Paul. Proof Of Stake: POS. In: *Ethereum* [online]. 2020, 23. 12. [cit. 2021-04-05]. Dostupné z: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>
- [45] What Is Proof Of Stake? In: *Shrimpy* [online]. 2020, 27. 1. [cit. 2021-04-05]. Dostupné z: <https://blog.shrimpy.io/blog/what-is-proof-of-stake>
- [46] What is Python?: Executive summary. In: *Python* [online]. 2001– [cit. 2021-04-05]. Dostupné z: <https://www.python.org/doc/essays/blurb/>

## SEZNAM OBRÁZKŮ

Obrázek 1: Logo JMK .....	3
Obrázek 2: Logo JCMM .....	3
Obrázek 3: Distribuovaná, centralizovaná a decentralizovaná síť uzlů.....	8
Obrázek 4: Centralizovaný a decentralizovaný systém obchodu s elektřinou.....	10
Obrázek 5: Firmy využívající blockchain v odvětví obchodu s elektřinou .....	11
Obrázek 6: Řetězec bloků – datová struktura blockchainu.....	12
Obrázek 7: Počet transakcí provedených za sekundu – vede VISA .....	14
Obrázek 8: PoW vs PoS v blockchainových systémech.....	15
Obrázek 9: Pravidlo nejdelšího řetězce .....	16
Obrázek 10: Screenshot z aplikace – založení účtu .....	17
Obrázek 11: Screenshot z aplikace – přihlašovací formulář.....	18
Obrázek 12: Screenshot z aplikace – domovská stránka .....	18
Obrázek 13: Screenshot z aplikace – základní manuál pro uživatele .....	19
Obrázek 14: Screenshot z aplikace – výpis blockchainu .....	20
Obrázek 15: Screenshot z aplikace – formulář pro zadání jednoduché transakce .....	20
Obrázek 16: Screenshot z aplikace – vypisování čekajících transakcí .....	21
Obrázek 17: Screenshot z aplikace – stránka Minig po čerstvém vytěžení bloku.....	22
Obrázek 18: PoW algoritmus.....	22
Obrázek 19: Screenshot z aplikace – profil nového uživatele .....	23
Obrázek 20: Screenshot z aplikace – formulář pro založení nabídky.....	24
Obrázek 21: Screenshot z aplikace – výpis nabídek.....	24
Obrázek 22: Screenshot z aplikace – situace po dvojitém nákupu prostřednictvím nabídky ..	25
Obrázek 23: Screenshot – úspěšné odhlášení z aplikace .....	25



## PŘÍLOHA 1: ZDROJOVÝ KÓD – FUNKCE KONTROLUJÍCÍ BEZPEČNOSTNÍ KRITÉRIA HESLA (SCREENSHOT)

```
def my_secure_psw(pasw):  
    if not re.search("[a-z]", pasw):  
        flash("Your password has to contain at least one \\  
        | lower-case letter!")  
        return False  
    elif not re.search("[A-Z]", pasw):  
        flash("Your password has to contain at least one \\  
        | upper-case letter!")  
        return False  
    elif not re.search("[0-9]", pasw):  
        flash("Your password has to contain at least one cipher!")  
        return False  
    elif len(pasw) < 12:  
        flash("Your password has to be at least 12 chars long!")  
        return False  
    else:  
        return True
```



## PŘÍLOHA 2: ZDROJOVÝ KÓD – FUNKCE ZAJIŠŤUJÍCÍ AKTUALIZACI BLOCKCHAINU MEZI UZLY (SCREENSHOT)

```
@app.route("/carolines_blockchain")
def blockchain():
    consensus()
    new_chain = None
    max_length = len(b.chain)
    for node in b.peers:
        response = requests.get(f"http://{node}/chainome")

        if response.status_code == 200:
            length = response.json()['length']
            chain = response.json()['chain']

            if length > max_length and b.check_chain_validity():
                max_length = length
                new_chain = chain

    if new_chain:
        b.chain = b.chain_json_decode(new_chain)
        b.unconfirmed = []
        print("New chain")
    return render_template("chain.html", b = b)

@app.route("/chainome")
def get_chain():
    response = {
        'chain': b.chain_json_encode(),
        'length': len(b.chain)
    }
    return jsonify(response), 200
```