Jihočeská univerzita v Českých Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky

Teze diplomové práce

Aplikace technologie blockchain a chytrých kontraktů v oblasti IoT

Vypracoval: Bc. Petr Knotek

Vedoucí práce: doc. Ing. Ladislav Beránek, CSc., MBA

České Budějovice

2023

Klíčová slova: aplikace, blockchain, chytré smlouvy, internet věcí
JEL Classification: O14, Q55
Anotace: Tato práce se zaměřuje na použití technologie blockchain a chytrých kontraktů v kontextu internetu věcí (IoT). Cílem práce bylo zmapovat různé technologie blockchain a chytrých kontraktů, vybrat ty nejvhodnější a vytvořit z nich aplikaci, která funguje s IoT zařízeními. Teoretická část práce poskytuje ucelený přehled technologie blockchain, chytrých kontraktů a Internet of Things. Práce se zaobírá zkoumáním jednotlivých technologii jako jsou blockchainové platformy podporující chytré kontrakty nebo aplikace chytrých kontraktů pro předávání dat skrze IoT sít. Analýza různých platforem blockchainu umožnila vybrat tu nejvhodnější pro vývoj naší aplikace, což bylo Ethereum. Našim programovacím jazykem pro chytré kontrakty se stalo solidity kvůli své kompatibilitě s etherem. Praktická část práce začíná stručným popisem rozhodnutí o záměru, na co bude aplikace zaměřena a jaká technologie bude vybrána pro tvorbu naší aplikace. V rámci tohoto popisu se zaměříme na to, jaké nástroje budou potřeba pro náš vývoj a fungování samotné aplikace a v neposlední řadě řešení architektury samotné aplikace. V druhé polovině praktické části se věnujeme samotnému programování jednotlivých částí naší aplikace jako je chytrý kontrakt či jeho testovací soubor skrze frameworky. A v poslední řadě samotná webová aplikace napsaná v HTML, CSS, JS, která všechny tyto části spojuje dohromady. Navrhnutá aplikace by měla zastoupit centralizovaný volební systém, který se v minulosti setkal s mnoho podvody a neshledává se s nejlepší kritikou. Naše aplikace umožnuje decentralizované volby, které jsou zaštítěné právě technologiemi blockchain a chytrých kontraktů, které nám dávají důvěru ve svoji neměnnost a IoT sít jí dává možnost zvětšit svůj maximální dosah co se týče využití. Testování aplikace prokázalo její funkčnost a bezpečnost a propojitelnost se zařízením internetu věcí. Aplikace splnila všechna svá očekávání, i když je zde určitě místo pro zlepšení.

Úvod a přehled literatury

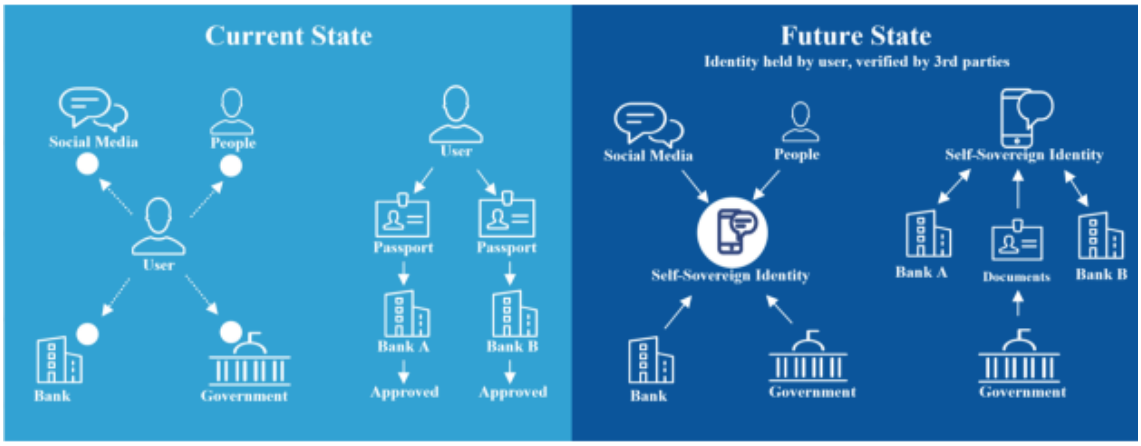
Vzhledem k rychlé a obrovské revoluci, s níž se moderní svět v těchto dnech setkává, se očekává, že Blockchain, Internet of Thing, big data a další technologická vylepšení budou hrát v lidských životech významnou roli. Velký efekt nastane, když se všechny tyto technologie integrují dohromady, a vytvoří se tak funkční celek, ale to je zatím otázka budoucnosti.
Blockchainy v poslední době přitahují zájem zainteresovaných stran v širokém spektru průmyslových odvětví: od financí a zdravotnictví, až po veřejné služby, nemovitosti, a vládní sektor. Důvodem tohoto prudkého nárůstu zájmu o tuto technologii je díky blockchain aplikacím, které dříve mohly fungovat pouze prostřednictvím důvěryhodného zprostředkovatele, nyní mohou fungovat decentralizovaně, bez potřeby centrální autority, a dosáhnout stejné funkčnosti se stejnou mírou jistoty. To dříve jednoduše nebylo možné. Říkáme, že blockchain umožňuje sítě bez důvěry, protože strany mohou provádět transakce, i když si navzájem nedůvěřují. Absence důvěryhodného zprostředkovatele znamená rychlejší usmíření mezi transakčními stranami. Hojné využívání kryptografie, která je klíčovou vlastností blockchainových sítí, přináší autoritativnost za všechny interakce v síti. Chytrých smlouvách – automatizované skripty, které se nacházejí v blockchainu – integrují tyto koncepty a umožňují řádné, distribuované a automatizované pracovní postupy. Díky tomu by měly být blockchainy lákavé pro oblast IoT. Přechod na decentralizovanou síť samozřejmě nemusí mít vždy smysl. Navíc, i když je takový přechod žádoucí, požadavky aplikace mohou být takové, že blockchainová síť je nemůže splnit. Blockchainy a chytré smlouvy přinášejí řadu výhod, ale je s nimi spojeno i mnoho nevýhod.

Když se podíváme zpátky do doby kdy se poprvé začaly objevovat nynější technologie tak se ocitneme v roce 1997, kdy Nick Szabo vytvořil termín "chytré smlouvy", a také dále vysvětlil jeho významové charakteristiky a aplikace (Szabo, 1997). V roce 2008 anonym "Satoshi Nakamoto" publikoval článek pod názvem "Bitcoin: A Peer-to-Peer Electronic Cash System", ve kterém podrobně popsal digitální měnu známou jako bitcoin, která byla vytvořena na základě blockchainu (Nakamoto, 2008). Blockchain zatím vstoupil do mnoha odvětví, jako jsou finance, řízení dodavatelského řetězce atd. Většina implementací blockchainu tvrdí, že zvyšuje efektivitu, snižuje náklady a podporuje transparentnější interakce mezi sociálními subjekty. Studie šla nad rámec současných běžných aplikací a integrovala technologii blockchain do strategického plánování podniku, aby byla považována za konkurenční výhodu pro různé firmy. Došli k závěru, že" technologie blockchain je propojena s dalšími zdroji, a že konkurenceschopnost zdrojů se odráží prostřednictvím procesu výběru technologie (Bjørnstad, Harkestad, & Krogh, 2017). Vzhledem k tomu, že Blockchain se poprvé objevil v digitální měně Bitcoin, dochází k mírné záměně obou pojmů. Na základní úrovni můžeme jednoduše definovat "Blockchain" jako nástroj a Bitcoin nebo Ethereum jako jednu z aplikací Blockchainu.

Jelikož práce podrobně probere všechny tři hlavní technologie, tak se nyní zaměříme na možné fungování v určitých případech a odvětvích.

Jedním z nejslibnějších případů využití blockchainu a chytrých smluv v internetu věcí je správa digitální identity. V tomto scénáři může blockchain poskytnout neměnný záznam identity jednotlivce, který lze bezpečně sdílet mezi různými zařízeními a platformami. Chytré smlouvy lze použít k vynucení zásad řízení přístupu a usnadnění výměny ověřených informací mezi stranami. Tento přístup může pomoci zabránit krádeži identity, omezit podvody a zvýšit soukromí a bezpečnost (Deloitte & Alliance, 2016).

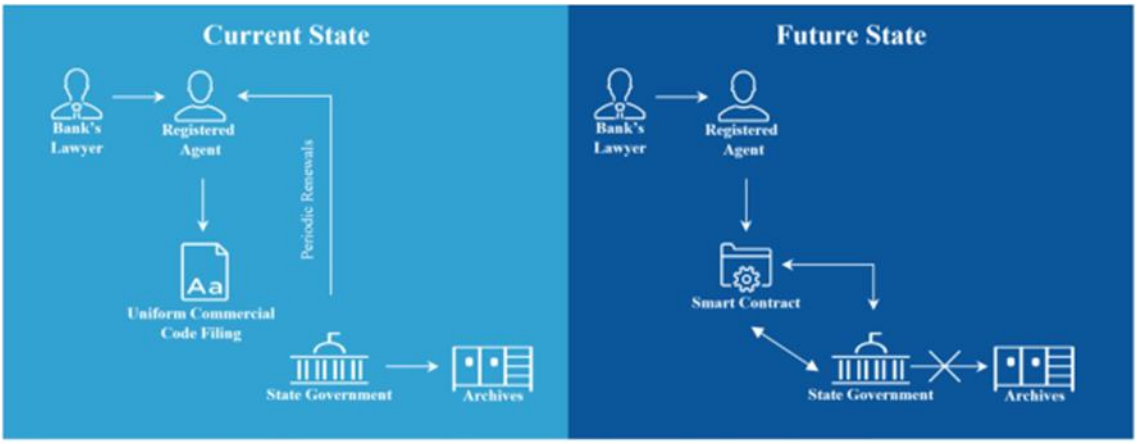
Obrázek 1: Schéma řešení digitální identity



***Zdroj**: (Deloitte & Alliance, 2016)*

Držení záznamů je důležité v různých odvětvích, včetně financí, práva a zdravotnictví. Blockchain nám nabízí možnost uchovávat a spravovat širokou škálu digitálních zá-znamů v decentralizovaném systému odolném proti manipulaci, ke kterému mají pří-stup pouze oprávněné strany. Chytré smlouvy mohou dále automatizovat proces ověřo-vání a aktualizace těchto záznamů, čímž se sníží potřeba zprostředkovatelů a zefektiv-ní pracovní postupy. Podobně lze chytré smlouvy využít k automatizaci dodržování právních předpisů a nařízení, jako je například Jednotný obchodní zákoník ve Spoje-ných státech, což snižuje právní náklady a zvyšuje provozní efektivitu. (Deloitte & Alliance, 2016)

***Obrázek 2**: Schéma uchovávání záznamů*



***Zdroj**: (Deloitte & Alliance, 2016)*

Volební systém s využitím blockchainu a chytrých smluv má potenciál vytvořit bezpečné a transparentní hlasovací prostředí, které ztíží manipulaci s výsledky voleb ze strany padělatelů. Záznamy o hlasování mohou být uloženy v decentralizovaném systému odolném proti manipulaci, k němuž mají oprávněné strany bezpečný přístup, což zajistí, že každý hlas bude přesně započítán a nebude možné jej po odevzdání změnit.

Chytré smlouvy mohou také automatizovat různé úkoly související s volebním procesem, jako je registrace voličů, distribuce hlasovacích lístků a sčítání hlasů, což může pomoci omezit chyby a zpoždění, a zajistit, aby volby proběhly spravedlivě a efektivně. Kromě toho mohou blockchain a chytré smlouvy pomoci řešit klíčové problémy současného volebního systému,

jako jsou podvody s voliči, potlačování volebních práv a nízká volební účast. (Chia-Hao Lee, 2022)

Technologie blockchain může například lidem usnadnit hlasování na dálku nebo hlasování pomocí mobilních zařízení, což by mohlo zvýšit volební účast. Celkově má využití blockchainu a chytrých smluv ve volebním systému potenciál způsobit revoluci ve způsobu, jakým jsou volby prováděny, a učinit je bezpečnějšími, transparentnějšími a přístupnějšími pro všechny. A proto jsem si zvolil toto téma volební procesu jako cíl pro svou praktickou část, která se tímto problémem bude zabývat.

Cíl práce

Cílem této práce je poskytnout podrobný popis fungování blockchainů a chytrých smluv, identifikovat výhody a nevýhody, které jejich zavedení do systému přináší, a upozornit na způsoby, kterými lze využít blockchain a IoT společně. V druhé části se práce zaměří na tvorbu samotné aplikace s využitím blockchain technologie v kombinaci s chytrými kontrakty v prostředí IoT.

Metodika

Pro tento projekt jsme zvolili jako blockchain technologie Ethereum, která nám poslouží jako ideální nástroj pro naše účely. Jako programovací jazyk pro naší chytrou smlouvu jsme zvolili solidity, jelikož má velkou kompatibilitu s etherem, ale je také nástroj pro vytváření kódu na strojové úrovni a jeho kompilaci v rámci Ethereum Virtual Machine (EVM). Pro zpracování naší webové aplikace využijeme JavaScript a kombinací HTML a CSS pro vizualizaci webové aplikace. A pro IoT řešení se vydáme vytvořením samostatné sítě, kterou připojíme k technologii blockchain a vyzkoušíme interakce skrze zařízení Google Nest druhé generace, což by mělo zastoupit IoT zařízení v našem případě.

První nástroj, který potřebujeme, je Node Package Manager neboli NPM. NPM je správce balíčků v jazyce JavaScript. Primární využití JS se samozřejmě zaměřuje na vývoj mobilních aplikací a přidávání interakcí na webové stránky. Možnost průběžného testování a nasazování je nesmírná výhoda. Místo toho, aby vývojáři vyžadovali kompletní aktualizaci aplikace, mohou provádět malé změny, které zlepšují uživatelský komfort, přidávají funkce a zvyšují bezpečnost dat.

Další nástroj je Truffle Framework, který nám umožňuje vytvářet decentralizované aplikace na blockchainu Ethereum. Poskytuje sadu nástrojů, které nám umožňují psát chytré kontakty pomocí programovacího jazyka Solidity. Umožňuje nám také testovat naše chytré kontrakty a nasazovat je na blockchain. Poskytuje nám také místo pro vývoj naší aplikace na straně klienta.

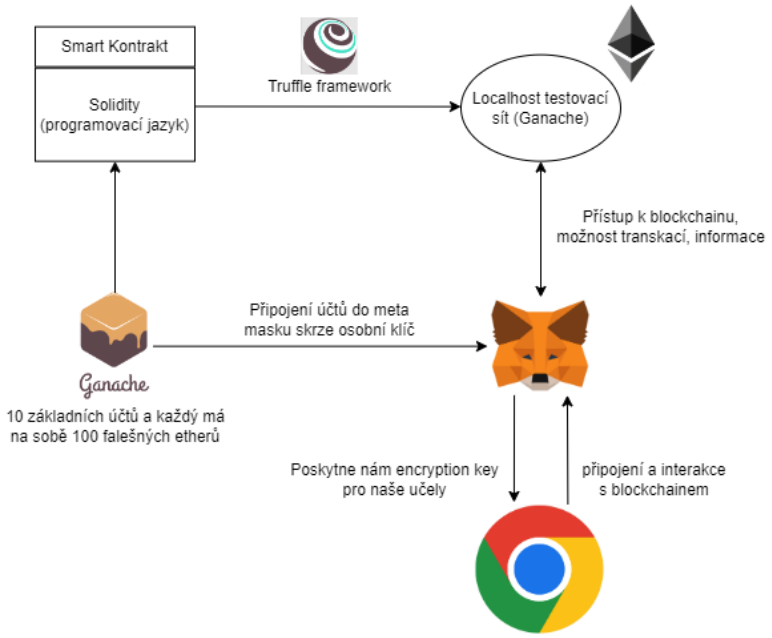
Další nástroj je Ganache, lokální in-memory blockchain. Ganache je osobní blockchain pro rychlý vývoj distribuovaných aplikací Ethereum a Filecoin. Ganache můžeme používat v celém vývojovém cyklu; umožňuje nám vyvíjet, nasazovat a testovat naše decentralizované aplikace v bezpečném a deterministickém prostředí. Poskytne nám 10 externích účtů s adresami v našem lokálním blockchainu Ethereum. Na každém účtu je přednastaveno 100 falešných etherů.

Další a poslední nástroj je rozšíření Metamask pro Google Chrome. Abychom mohli využívat blockchain, musíme se k němu připojit. Abychom mohli používat blockchain Ethereum, musíme si nainstalovat speciální rozšíření prohlížeče. K tomu slouží metamask. Budeme se

moci připojit k našemu lokálnímu blockchain Ethereu pomocí našeho osobního účtu a komunikovat s naší chytrou smlouvou.

Obrázek níže ukazuje schéma architektury našeho systému elektronického hlasování na základě technologii blockchain.

Obrázek 3:Popis architektury aplikace



***Zdroj**: Autor*

Poté na řadu přišla tvorba jednotlivých částí naší aplikace, počínaje chytrou smlouvou. Kde popisujeme jednotlivé části kódu, které využívá naše aplikace jako část kódu solidity naší testovací chytré smlouvy viz obrázek 4.

Obrázek 4: Ukázka kódu testovací chytré smlouvy

```
pragma solidity 0.4.25
contract Volby {
   string public kandidat;
   constructor () public {
      kandidat = "kandidat 1";
   }
}
```

***Zdroj**: Autor*

Dalším krokem po úspěšném dopsání chytré smlouvy bylo vytvoření testovacího souboru, jelikož na testy se klade velký důraz kvuli nemenosti po nasazení. Ná obrázku 5 je vidět úspěšný průchod.

Obrázek 5: Úspěšný průchod testů

```
Azazel@DESKTOP-0GVHGBE MINGW64 ~/Desktop/github/volby
$ truffle test
Using network 'development'.


Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Volby.sol
> Artifacts written to C:\Users\hitma\AppData\Local\Temp\test--7856-yZyVjhijL9HU
> Compiled successfully using:
   - solc: 0.4.25+commit.59dbf8f1.Emscripten.clang


  Contract: Volby
    √ zacina se dvemy kandidaty
    √ zacinaji kandidati správnymi hodnotami
    √ dovolit volici odevzdat hlas (70ms)
    √ neplatny kandidati (153ms)


  4 passing (326ms)
```

***Zdroj**: Autor*

A nakonec zpracování naší webové aplikace skrze JavaSscript jako nástroj pro back-end a HTML, CSS bootstrap framework pro front-end.

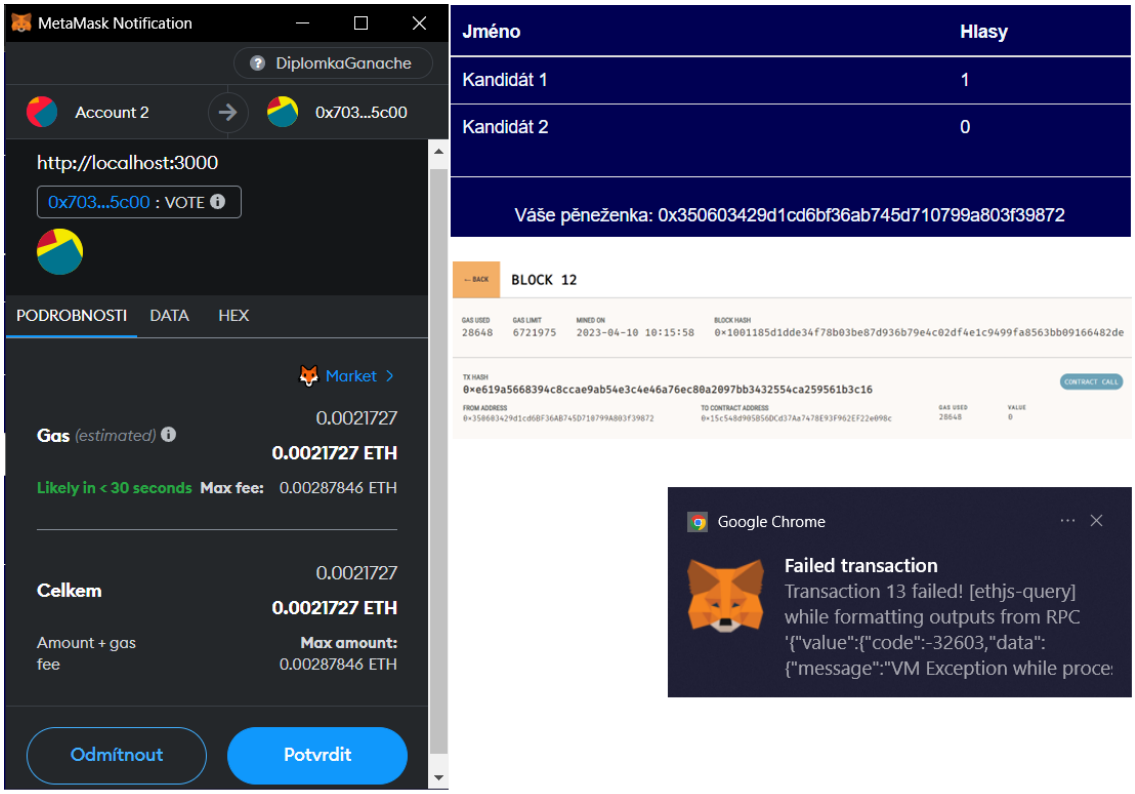
Obrázek 6: Ukázka naší webové stránky

***Zdroj**: Autor*

Výsledky

Po našem testování můžeme říct, že aplikace funguje a splňuje to, co jsme od ní požadovali. Z hlediska grafického designu jsou tu velké ústupky, které by v plném nasazení chtěli vyřešit, jako je responzivita samotné stránky a kompatibilita se všemi dostupnými zařízeními. Do budoucna by se určitě dali přidat i další věci, které by nám zpříjemnily používání, jako grafy s vyhodnocením či bohatší grafický styl stránky.

Obrázek 7: Potvrzení převodu, výsledky volbě a neuspešný pokus o double voting



***Zdroj**: Autor*

Z hlediska chytrého kontraktu nedošlo k žádné chybě, kterou bychom zaznamenali, jelikož jsme hlídali jednotlivé vytěžené bloky kdykoliv došlo k volbě a zavolání samotného kontraktu. Jediná věc, která nás zaujala, byla změna gas fee pro různá zařízení což by mohlo být způsobeno různýma verzema aplikace metamask, která pro nás slouží jako kryptopeněženka.

Z hlediska back-endu stránky jsme narazili na určité nuance, které bychom nyní už vytvořili jinak, například dříve zmiňovaná funkce initWeb3, v našem případě je funkce zaměřena čistě na Metamask a třeba s Coinbase nefungovala. V budoucnu by bylo vhodné se zaměřit na univerzálnost, jak z hlediska grafiky a responzivního designu pro všechna zařízení, tak z hlediska back-endu na čistotu a stabilitu kódu, ale i využití s více programy a zařízeními což pomůže vytvořit přívětivější uživatelské prostředí.

Závěr

Navrhnutá aplikace by měla zastoupit centralizovaný volební systém, který se v minulosti setkal s mnoho podvody a neshledává se s nejlepší kritikou. Naše aplikace umožnuje decentralizované volby, které jsou zaštítěné právě technologiemi blockchain a chytrými smlouvami, které nám dávají důvěru ve svoji neměnnost a IoT sít jí dává možnost zvětšit svůj maximální dosah co se týče využití.

Testování aplikace prokázalo její funkčnost a bezpečnost a propojitelnost se zařízením internetu věcí. Aplikace splnila všechna svá očekávání, i když je zde určitě místo pro zlepšení.

Závěrem lze říct, že tato diplomová práce přinesla poznatky a vyzdvihla potenciál technologie blockchain a chytrých kontraktů v IoT. Práce ukazuje, že tyto technologie lze využít k vytvoření bezpečných a efektivních aplikací či systémů. Práce by mohla posloužit jako zdroj informací pro další výzkum, který by se zaměřil na další vývoj aplikací a systémů s využitím těchto technologiích.

Seznam literatury použité v tezích

Plný seznam použité literatury je uveden v textu diplomové práce.

[1] Bjørnstad, M. V., Harkestad, J. G., & Krogh, S. (2017). *A study on blockchain technology as a resource for competitive advantage.* [Diplomová práce, Norwegian University of Science and Technology]. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2472245/17527_FULLTEXT.pdf?sequence=1&isAllowed=y

[2] Lee, C. -H., Neo, H. -F., & Teo, C. -C. (2022). Secure E-Voting System based on Blockchain Technology. *Journal of System and Management Sciences*, *2022*(1), 1-18. https://doi.org/10.33168/JSMS.2022.0508

[3] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org*, *1*(1), 1-9. https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[4] Smart Contracts Alliance, & Deloitte. (2016). Smart Contracts: 12 Use Cases for Business & Beyond: A Technology, Legal & Regulatory Introduction — Foreword by Nick Szabo. Website, 1(1), 1-56. https://www.the-blockchain.com/docs/Smart%20Contracts%20-%2012%20Use%20Cases%20for%20Business%20and%20Beyond%20-%20Chamber%20of%20Digital%20Commerce.pdf

[5] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Další bibliografické údaje

Type of thesis:	Master
Author:	Petr Knotek
Academic Year:	2022/2023
Department:	Department of Applied Mathematics and Informatics,Faculty of Economics, University of South Bohemia in Ceske Budejovice, Czech Republic
Thesis supervisor:	doc. Ing. Ladislav Beránek, CSc., MBA
Number of pages:	73
Language od thesis:	CZ
Title of Thesis:	Application of blockchain technology and smart contacts in IoT

Annotation: This thesis focuses on the use of blockchain and smart contract technology in the context of the Internet of Things (IoT). The thesis aimed to map different blockchain and smart contract technologies, select the most suitable ones and create an application that works with IoT devices. The theoretical part of the thesis provides a comprehensive overview of blockchain technology, smart contracts and the Internet of Things. The thesis explores individual technologies such as blockchain platforms supporting smart contracts or smart contract applications for data transfer through IoT networks. The analysis of different blockchain platforms allowed us to choose the most suitable one for the development of our application, which was Ethereum. Solidity became our programming language for smart contracts because of its compatibility with Ethereum. The practical part of the thesis starts with a brief description of the decision on the purpose, what the application will focus on and what technology will be chosen to develop our application. Within this description, we will focus on what tools will be needed for our development and the functioning of the application itself, and finally the solution of the application's architecture itself. In the second half of the practical part, we focus on the actual programming of the different parts of our application such as the smart contract or its test suite through frameworks. And lastly, the web application itself is written in HTML, CSS, and JS, which ties all these parts together. The proposed application should replace the centralized voting system, which has faced a lot of fraud in the past and is not met with the best criticism. Our app enables decentralized elections that are secured by blockchain and smart contract technologies specifically, which gives us confidence in its immutability and the IoT network gives it the ability to maximize its reach in terms of usage. Testing of the app has demonstrated its functionality and security and connectivity with IoT devices. The app has met all its expectations, although there is room for improvement.

Key words: Internet of Things, smart contract, blockchain, programming, technology, application, election system

---

Přílohy volně vložené: Soubory aplikace

Přílohy vázané v práci: žádné