UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO – SPRÁVNÍ

DIPLOMOVÁ PRÁCE

2022 IVO SEEMANN

UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO – SPRÁVNÍ

VYUŽITÍ BLOCKCHAIN TECHNOLOGIÍ PRO ZAJIŠTĚNÍ BEZPEČNOSTI A DŮVĚRYHODNOSTI PŘI ELEKTRONICKÝCH VOLBÁCH.

DIPLOMOVÁ PRÁCE

2022 IVO SEEMANN

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ivo Seemann**
Osobní číslo:	**E200043**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Využití blockchain technologií pro zajištění bezpečnosti a důvěryhodnosti při elektronických volbách.**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je provedení systematické literární rešerše porovnávající různé přístupy a zkušenosti s využitím blockchain technologií při elektronických volbách. Práce s anglickou literaturou je podmínkou.

Osnova:
- Princip fungování blockchain technologie.
- Volby a jejich procesní zajištění.
- Elektronické volby – možnosti technického řešení.
- Příklady států s e-volbami, kde je blockchain již využíván – zkušenosti, výhody, problémy.

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

BRUNCLÍK, M., NOVÁK, M. Internetové volby: budoucnost, nebo slepá ulička demokracie?. Praha: Sociologické nakladatelství (SLON), 2014. Studijní texty (Sociologické nakladatelství). ISBN 978-80-7419--168-8
MERTA, M. JAK POCHOPIT BITCOIN. ČR: Michael Merta, 2021. ISBN 999-00-030-7519-2
Kryptoměny z účetního a daňového pohledu. Praha: Svaz účetních České republiky, 2020. Metodické aktuality Svazu účetních. ISBN 978-80-7626-008-5
STROUKAL, D., SKALICKÝ, J. 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
TAPSCOTT, D., TAPSCOTT, A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Portfolio, 2016. ISBN 978-1101980132

Vedoucí diplomové práce: **doc. Ing. Hana Kopáčková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2021**
Termín odevzdání diplomové práce: **30. dubna 2022**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2021

Prohlašuji:

Práci s názvem Využití blockchain technologií pro zajištění bezpečnosti a důvěryhodnosti při elektronických volbách jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 25.11. 2022

Ivo Seemann

Poděkování

Na tomto místě bych rád poděkovat vedoucí diplomové práce doc. Ing. Haně Kopáčkové Ph.D. za cenné rady, věcné připomínky, vstřícnost, trpělivost a pomoc při konzultacích a vypracování diplomové práce. Mé poděkování patří též mé rodině za podporu během studia.

Anotace

Cílem práce je provedení systematické literární rešerše porovnávající různé přístupy a zkušenosti s využitím blockchain technologií při elektronických volbách. Práce je rozdělena na dvě části. První část je teoretická a popisuje historii a vybrané principy blockchainu, dále se zabývá stručným popisem voleb a požadavky na elektronické volby. Druhá část je praktická, kde za pomoci systematické literární rešerše jsou zkoumány odborné články a publikace zaměřené na přístupy k elektronickým volbám s využitím technologie blockchain. Samotné hodnocení přístupu k elektronickým volbám je řešeno pomocí vybraných atributů zkoumaných implementací. Praktická část se v závěru věnuje reálným zkušenostem vybraných států s elektronickými volbami na bázi blockchainu.

Klíčová slova

blockchain, konsensus, DLT, ETHEREUM, šifrování, hash, e-volby, distribuovaný systém

Title

Use of blockchain technologies to ensure security and reliability in electronic elections.

Annotation

The work aims to conduct a systematic literature search comparing different approaches and experiences with using blockchain technologies in electronic elections. The result is divided into two parts. The first part is theoretical and describes the history and selected principles of blockchain it also deals with a brief description of elections and requirements for electronic elections. The second part is practical, where, with the help of systematic literature research, expert articles and publications focused on approaches to electronic elections using blockchain technology are examined. The evaluation of access to electronic elections is solved using selected attributes of the investigated implementations. In the end, the practical part is dedicated to the real experiences of selected states with blockchain-based electronic elections.

Keywords

blockchain, consensus, DLT, ETHEREUM, encryption, hash, e-voting, distributed system

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

Úvod

Volby provázejí lidstvo již několik staletí, a to od doby svého vzniku v řeckých městských státech. Během těchto staletí se stejně jako lidská společnost vyvíjely i samotné volby, a to až do podoby kterou známe dnes, kdy jsou vhazovány volební lístky do volebních uren, či prováděny na elektronických přístrojích ve volebních místnostech.

S příchodem jednadvacátého století a rozšířením tzv. e-technologií dochází k obrovskému nárůstu využívání těchto technologií jak v soukromé, tak také ve státní sféře. Pro tento převod státní sféry z papírové formy do digitální se zažil pojem e-government. Tento pojem představuje usnadnění komunikace mezi úřady a veřejností, kdy občané již nemusí trávit drahocenný čas v čekárnách, ale vše potřebné vyřídí z pohodlí domova. Jedním z nových atributů posledních let e-governmentu, který získává čím dál více pozornosti, jsou elektronické volby založené na nových technologiích, tzv. e-volby. Mnoho států ve světě sice již implementuje systémy elektronického hlasování využívající informační technologie, ale tyto systémy jsou založeny na technologiích z přelomu tisíciletí a přesně neodrážejí dnešní význam slova e-volby.

Nový druh e-voleb, které se jejich tvůrci snaží přinést až do domovů voličů, se potýkají se zásadními otázkami jejich zabezpečení a důvěryhodností. Částečné vyřešení těchto problémů je spojeno s příchodem kryptoměn a novým typem distribuovaných databází, pojmenovaných blockchain. Díky vlastnostem blockchainů a způsobem jakým jsou vytvářeny je možné dosáhnout určitého stupně zabezpečení při odevzdávání hlasů, manipulaci s nimi, jejich sčítáním, zpětném ověřováním a zveřejňování výsledků voleb.

Cílem této diplomové práce je provedení systematické literární rešerše porovnávající různé přístupy a zkušenosti s využitím blockchain technologií pro zabezpečení a zvýšení důvěryhodnosti při elektronických volbách. Jako podklady pro tuto systematickou rešerši jsou využity odborné články dostupné v databázích WoS a Scopus. Jelikož je blockchain a problematika voleb na něm založená otázkou poslední dekády, jsou veškeré použité články publikovány výhradně od zahraničních autorů a psané v anglickém jazyce.

Práce je rozdělena na dvě části, a to teoretickou a praktickou. První část, teoretická, obsahuje pět kapitol. Ty jsou postupně věnovány stručné historii vzniku a vývoje samotného blockchainu, nastínění vybraných principů fungování technologie blockchain, volbám a jejich procesnímu zajištění, požadavkům na elektronické volby a jejich možná technická řešení. Druhá část, praktická, obsahuje dvě kapitoly. Kapitola šest, ve které je řešen přístup

k elektronickým volbám na základě systematické literární rešerše vybraných odborných článků, které popisují jednotlivá řešení e-voleb založených na technologii blockchain. Kapitola sedm, uvádí příklady států, které již mají určité zkušenosti s tímto druhem e-voleb.

1 Historie

Počátky vzniku technologie blockchain sahají až do osmdesátých let dvacátého století. V těchto letech byly položeny základy technologií, které jsou využívány i technologií blockchain.

Jednou z prvních technologií je tzv. Merkel Hash Tree. Tato technologie je pojmenována po vědci Ralphu Merkelovi, který ve své disertační práci z roku 1979 na Stanfordově univerzitě popisuje přístup k distribuci veřejných klíčů a digitálních podpisů nazvaný jako „stromové ověřování“[1]. [1] Tento postup ověřování si Merkel nechal později patentovat.

Další technologií, která stojí na počátku blockchainu, je tzv. trezorový systém. Systém popsal ve své disertační práci David Chaum v roce 1982 na Kalifornské univerzitě v Berkley. [1] Zjednodušeně lze říct, že trezorový systém popisuje vznik, udržení a důvěryhodnost počítačových systémů mezi vzájemně si nedůvěřujícími skupinami. Jedná se o veřejný systém vedení záznamů s konzistentní příslušností ke skupině a výpočtem soukromých transakcí, který chrání soukromí jednotlivců pomocí fyzické bezpečnosti. [2] Dále tento systém v sobě obsahuje mnoho prvků, které jsou součástí dnešních blockchainů.

V roce 1991 je publikován článek Stuarta Habera a W. Scotta Stonera, který se zabývá digitálním označováním elektronických dokumentů a návrhem řešení pro zamezení jejich zpětného antidatování. [1] Autoři v roce 1992 svůj návrh řešení aktualizovali o Merkel Hash Tree, což umožnilo existenci více digitálně podepsaných dokumentů v jednom bloku.

V těchto a následujících letech došlo ke vzniku spoustě další návrhů, řešení a událostí, které měly za následek vznik a rozvoj technologie blockchain. [1] Jednalo se například o vznik a rozmach sítí P2P[2], které v letech 1999–2001 zpopularizovala společnost Napster. Dalším příkladem je koncepce PoW[3], která se zabývá ověřením výpočetní náročnost a zamezení kybernetickým útokům.

Milník v technologii blockchainu nastal v roce 2008, kdy Satoshi Nakamoto vydal tzv. Bílou knihu, která představuje koncepci Bitcoinu[4] a blockchainu. [1] O osobě samotného Satoshiho Nakamota se toho mnoho neví. Spekulovalo se o tom, že se jedná o jednu osobu,

[1] angl. „tree authentication“.
[2] Peer to peer, počítačová síť, kde spolu komunikují přímo klienti bez přispění serveru.
[3] Proof – of – work, forma kryptografického důkazu o vynaloženém určitém množství konkrétního výpočetního úsilí.
[4] Kryptoměna využívající k transakcím P2P sítě.

nebo spolek osob vystupujících pod tímto pseudonymem. Jeho koncepce popisuje transakce pomocí sítě P2P, kde každá provedená transakce obdrží časové razítko a je přidána do řetězce PoW za pomocí hashovací funkce. [3] Toto vše se odehrává bez zásahu třetí strany, tedy banky, vlády či jiné organizace. V roce 2009 tento koncept přešel v realitu, když 3. ledna 2009 Satoshi Nakamoto vytěžil první blok Bitcoinu, čímž potvrdil platnost celého konceptu blockchain. [1] Tento první vytěžený blok byl znám jako Genesis neboli blok 0 a obsahoval 50 „mincí" Bitcoinu. Během dalšího týdne, konkrétně 8. ledna 2009 Nakamoto vydává Bitcoin v 0.1 na Source Forge jako open source software a 12. ledna uskutečnil první bitcoinovou transakci, když poslal Halu Finneyovi deset Bitcoinů v bloku sto sedmdesát. Koncem října téhož roku byla založena první bitcoinová burza Bitcoin Market, na které mohli lidé nakupovat Bitcoiny.

Nakamoto celý systém nastavil tak, aby obsahoval maximálně dvacet jedna miliónů Bitcoinů. [1] V dnešní době je již vytěženo něco asi přes osmnáct miliónů Bitcoinů a zbytek se nynějším tempem očekává vytěžit někdy kolem roku 2140.

Zhruba rok po spuštění systému zneužil hacker chybu v kódu blockchainu a vytvořil více než sto osmdesát čtyři miliard Bitcoinů v bloku 74 638, čímž utrpěla pověst Bitcoinu. [1] Nakamoto na tento útok zareagoval vydáním nové verze Bitcoinu a před koncem roku 2010 se stáhl z online světa do ústraní.

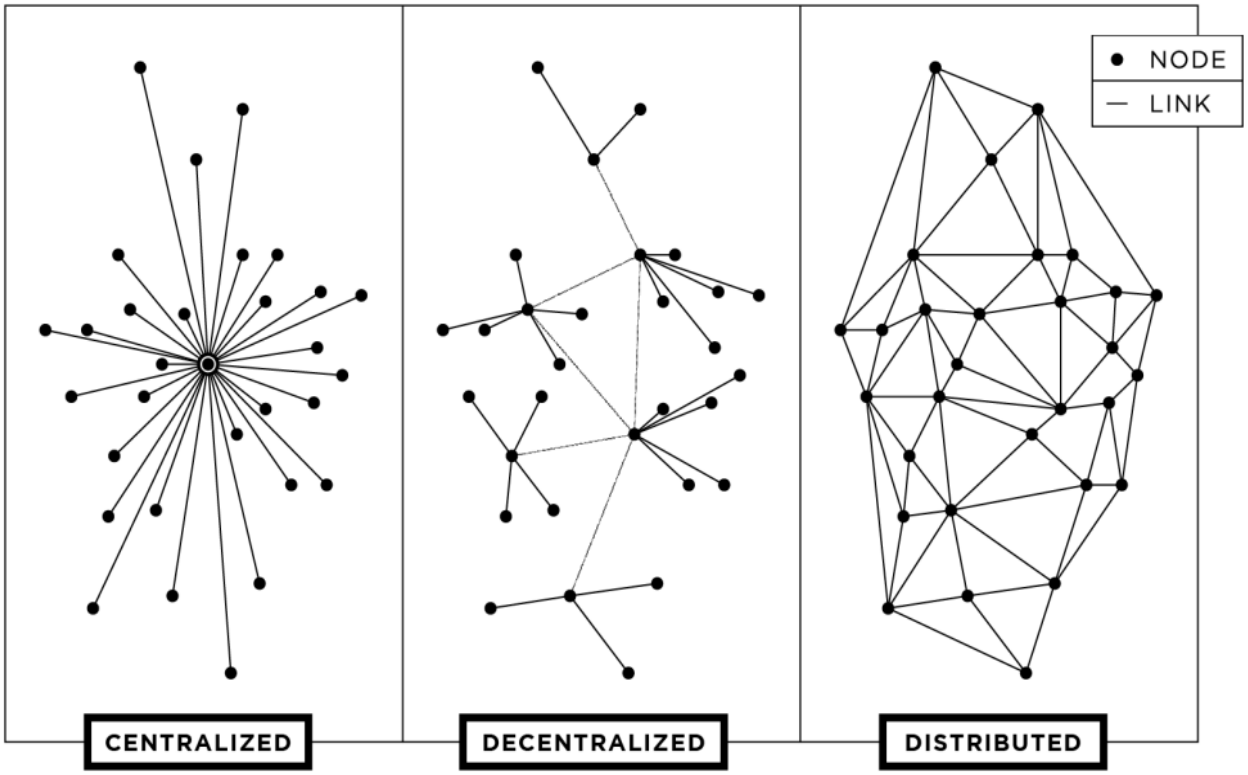
V roce 2013, kdy byl Bitcoin na vzestupné trajektorii, Čína a Thajsko zakazují kryptoměny. [1] O rok později představuje Vitalik Buterin svoji „Bílou knihu" o decentralizovaných aplikačních platformách, což vede k vytvoření nadace Ethereum Foundation. Tato nadace začala zkoumat a využívat blockchain i pro jiné účely a oblasti, něž pouze pro oblast kryptoměn. Výsledkem byla implementace chytrých smluv do technologie blockchain a aplikací DeFi[5]. V roce 2015 dochází ke spuštění sítě Ethereum Frontier a projektu Hyperledger[6] společností NASDAQ.

Od roku 2016 začíná být technologie blockchain čím dál tím více vnímána jako technologie s velkým technologickým potenciálem, a to ne jenom v oblasti kryptoměn. [1] Po roce 2020 je blockchain přijímán organizacemi po celém světě napříč všemi obory.

[5] Blockchaine aplikace zvládající provádět finanční transakce.
[6] Open source projekt vytvořený na podporu vývoje distribuovaných účetních knih, tzv. DLT (z angl. *Distributed Ledger Technology*).

1.1 Architektura systémů

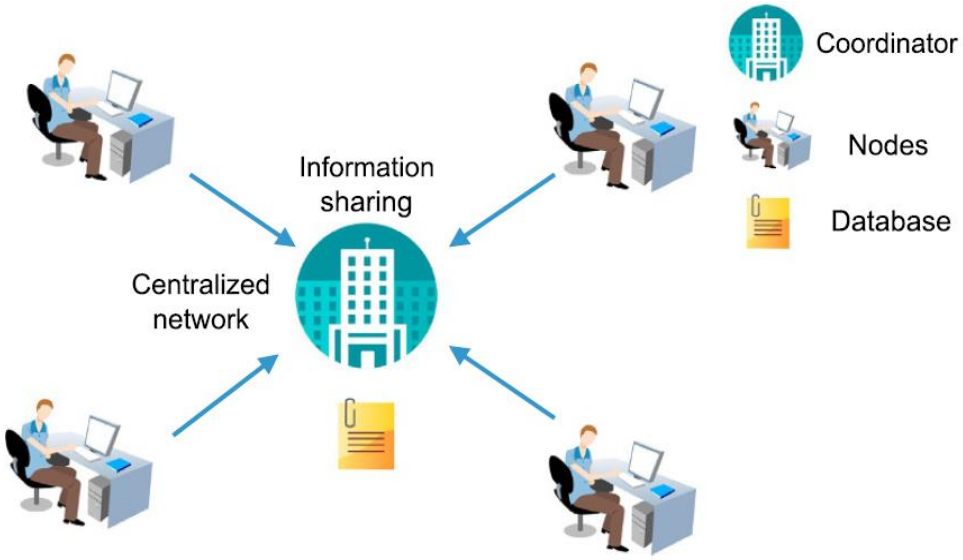
V souvislosti se systémem blockchain, Bitcoinem a dalšími kryptoměnami, jsou velmi často zmiňovány pojmy decentralizované a distribuční systémy. Tato kapitola vysvětluje principy, rozdíly, výhody a nevýhody těchto systémů a pro úplnost je doplněna o popis centralizovaných systémů. Grafické vyjádření struktur jednotlivých systému viz Obrázek 1.



Obrázek 1 – Struktura systémů

Zdroj: [63]

Centralizovaný systém – Jedná se o systémy, kde středem celé sítě je jeden centrální uzel a ostatní uzly jsou k tomu centrálnímu uzlu připojeny. [4, s. 136] V tomto systému centrální uzel spravuje a ukládá veškerá data, ke kterým mohou ostatní uzly přistupovat. [5] Příklad centralizovaného systému viz Obrázek 2.



Obrázek 2 – Centralizovaný systém

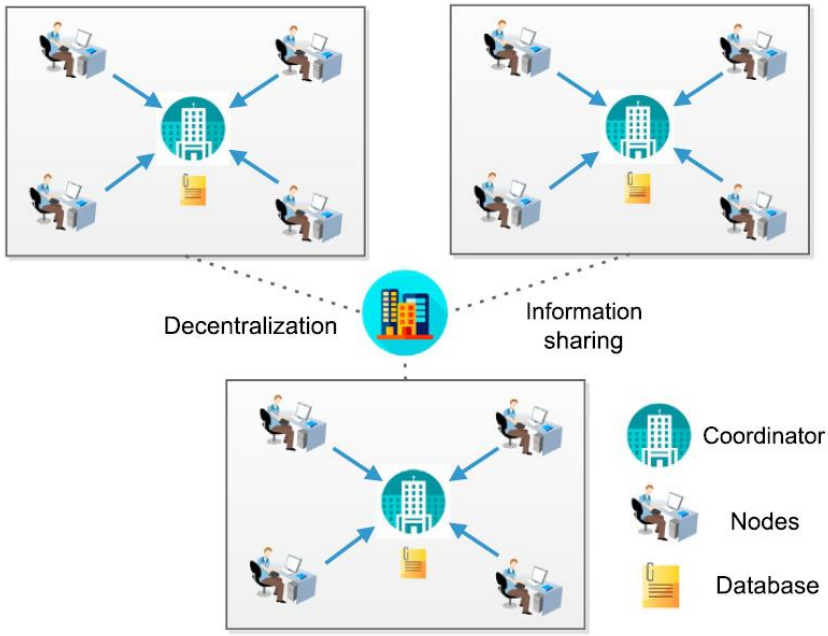
Zdroj: [4, s. 137]

Jednoznačnou výhodou tohoto systému je právě existence jednoho centrálním uzlu, který má pod kontrolou celou síť. [5] S tímto přímo souvisí i fyzická bezpečnost uložených a zpracovávaných dat, kdy veškerá data jsou uložena právě na tomto centrálním uzlu a tím je usnadněna jejich ochrana a integrita. Výhodou je také úspora v HW[7] a SW[8] vybavení, kde nejnákladnějším prvkem celého systému na SW a HW je pouze centrální uzel (server).

Nevýhody tohoto systému jsou paradoxně též v tom, že systém obsahuje pouze jeden centrální uzel. Celý systém je totiž závislý na funkčnosti centrálního uzlu a pokud dojde k jeho selhání, dojde k zhroucení celého systému. [5] Tento systém může být také náchylný k přetížení centrálního uzlu, kdy v důsledku malého výpočetního výkonu tohoto uzlu, není schopen obsloužit všechny požadavky od připojených uzlů. Dalším problémem je údržba a aktualizace centrálního uzlu. Tyto procedury musí probíhat za chodu celého systému a existuje zde poměrně velké riziko zhroucení celého systému.

[7] Hardware, fyzické technické vybavení počítače.
[8] Software, programové vybavení počítače.

Decentralizovaný systém – Jak je již z názvu patrné, tento typ systému nemá pouze jeden centrální uzel. Namísto toho v systému existuje několik „centrálních uzlů“ s připojenými koncovými uzly a tyto všechny prvky systému spolu navzájem komunikují a spolupracují. [4, s. 136-137] Chování celého systému je souhrn rozhodnutí jednotlivých uzlů. [5] Architektura tohoto systému může být dvojího typu. Prvním typem jsou P2P systémy, kde všechny uzly v síti jsou zároveň klienty i servery. Každý uzel tak poskytuje služby všem ostatním jako server a využívá služby ostatních uzlů jako klient. Všechny uzly jsou si tedy rovny jak ve funkcích, tak i rolích. Druhým typem jsou systémy master/slave, kde uzel (master) má jednosměrnou kontrolu nad jedním či více uzly (slaves). Příklad decentralizovaného systému viz Obrázek 3.



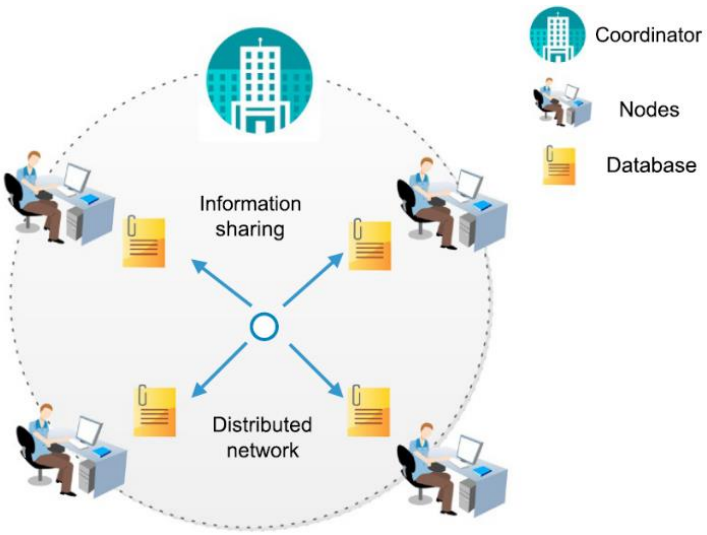
Obrázek 3 – Decentralizovaný systém

Zdroj: [4, s. 137]

Výhody decentralizovaného systému spočívají v rozdělení systému do většího počtu podsystémů. [4, s. 137] Pokud dojde ke kolapsu jednoho či více uzlů, dojde pouze k omezení přístupu k některým informacím nebo částečnému snížení výkonu celého systému. [6] S tímto je spojena i jednodušší a bezpečnější údržba jednotlivých uzlů. Celý systém je mnohem rychlejší a výkonnější než centralizovaný systém. To je způsobeno tím, že každý uzel může být rozšířen o HW či SW a koncentrace uzlů je řízena dle aktivity uživatelů. To znamená, že v oblastech s vyšší aktivitou uživatelů, je koncentrace uzlů vyšší a naopak.

Nevýhodami systému jsou především obtížnější dohledání uzlu, který selhal, vyšší náklady spojené s údržbou a upgradem a nekonzistentní výkon v jednotlivých částech systému. [5] [6] Další nevýhodou je obtížnější dosažení globálního cíle, což je řešeno pomocí konsensuálních algoritmů.

Distribuovaný systém – V tomto druhu systému neexistuje žádná centrální autorita, viz Obrázek 4. Jedná se o propojení autonomních uzlů, které navzájem spolupracují, sdílí informace a chovají se jako jeden celek, tvoří tedy takzvanou koherentní síť. [4, s. 137] V reálném světě jsou uzly naprogramovány k dosažení společných cílů, čehož dosahují pomocí zpráv, které si vzájemně vyměňují. [7] V distribuovaném systému uživatel přesně neví, kde jsou jednotlivé úlohy zpracovávány. Ve většině případů jsou tyto úlohy rozděleny na dílčí úlohy, které jsou přiděleny jednotlivým uzlům v systému, které je po zpracování opětovně odesílají uzlu zodpovědnému za distribuci. Důležitým faktem v distribuovaných systémem je absence společného času, kdy každý uzel má své vlastní pojetí času a dochází tu k problémům v synchronizaci a koordinaci.



Obrázek 4 – Distribuovaný systém

Zdroj: [4, s. 138]

Tento typ systému v sobě skýtá mnoho výhod. Těmi jsou například vysoká odolnost vůči selhání jednoho či více uzlů. [5] [6] Pokud dojde k selhání jednoho či více uzlů nedojde tím k ovlivnění výkonu systému. [8] Další výhodou tohoto systému je jeho flexibilita. Ta spočívá v možnosti zvýšení výkonu systému přidáním dalšího uzlu přímo za běhu celého systému. Dále je to vysoká škálovatelnost celého systému. Ta může být horizontální nebo vertikální. U horizontální škálovatelnosti dochází k přidávání či ubírání prvků systému.

Principem vertikální škálovatelnosti je to, že systém umím upravit vlastnosti uzlů dle aktuálních potřeb systému.

Mezi nevýhody tohoto systému lze jednoznačně zařadit bezpečnost a ochranu dat. Oproti jiným systémům, distribuované systémy poskytují větší prostor k útokům na data v systému, což je způsobeno právě architekturou celého systému. [8] Každý uzel představuje potencionální vstupní bránu pro útok na data v systému. Dále jsou to vysoké náklady na údržbu a provoz celého systému.

1.2 Distribuovaná účetní kniha DLT

Tradiční databáze, jejichž architektura je založena na centralizovaném systému, udržují, ukládají a umisťují informace na jedno místo, které je řízeno centrální správou databáze, která zajišťuje její celkovou integritu. [9, s. 125] V takto pojatém typu databáze jsou ve většině případů data uložena v syrové, nezpracované formě a databáze je chráněna proti útokům pomocí určitého druhu zabezpečení.

Distribuované databáze jsou rozděleny na jednotlivé části, které jsou rozprostřeny mezi uzly v síti, jejich správa, kontrola a integrita je přesto řešena centrálně. [9, s. 125] Uzly, mezi kterými jsou tyto databáze sdíleny, jsou označeny jako důvěryhodné a přístup k nim je řízen administrátorem dané sítě.

Technologie DLT[9], využívá základního mechanismu distribuované databáze. Ten spočívá v udržování vlastní identické kopie sdílené účetní knihy u každého člena sítě. [9] Odlišnost vůči klasickým distribuovaným databázovým systémům je následující:

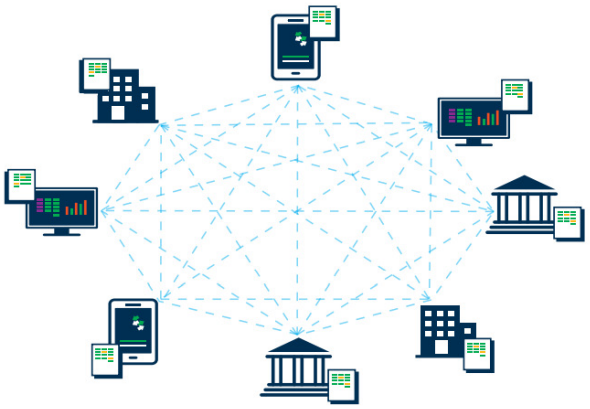
- *Decentralizace* – obsluha a řízení databáze je prováděno bez potřeby třetí strany. Všechny operace nad databází jsou řízeny a prováděny samotnými uzly v síti.
- *Dosažení konsensu* – většina, nebo všechny uzly v síti se shodnou na podobě DLT a její kopie jsou uloženy na tyto uzly, tento mechanismus je nazýván konsensuální algoritmus.
- *Šifrování* – k tomu, aby bylo možné dosáhnout předchozích dvou bodů, DLT implementuje kryptografické nástroje.

[9] Distributed Ledger Technology – Distribuovaná účetní kniha.

Uzly pomocí konsensuálních algoritmů hlasují o aktualizacích hlavní účetní knihy, což zajistí, že s aktualizací souhlasí většina uzlů. [10]. Jakmile se uzly „dohodnou“, je hlavní účetní kniha aktualizována a její kopie uložena na všech uzlech.

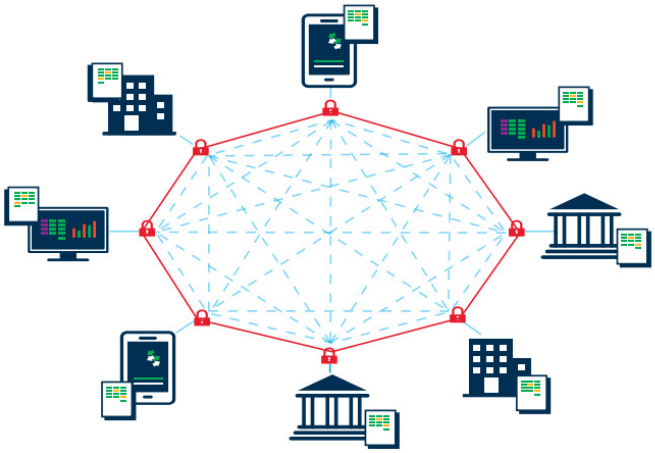
1.3 Přístupová a ověřovací práva

Účetní knihu DLT lze klasifikovat ze dvou pohledů, a to z pohledu přístupu k datům a z pohledu oprávnění ověřování transakcí. [11] [12, s. 321] Podle přístupu k datům se DLT dělí na soukromé (private) a veřejné (public). Dále jsou rozlišovány DLT bez oprávnění (permissionless) viz Obrázek 5 a s oprávněním (permissioned) viz Obrázek 6. V případě DLT s oprávněním může transakce ověřovat pouze určitá skupina uzlů, v případě DLT bez oprávnění může transakce ověřovat každý uzel sítě.



Obrázek 5 – DLT bez oprávnění

Zdroj: [65, s. 19]



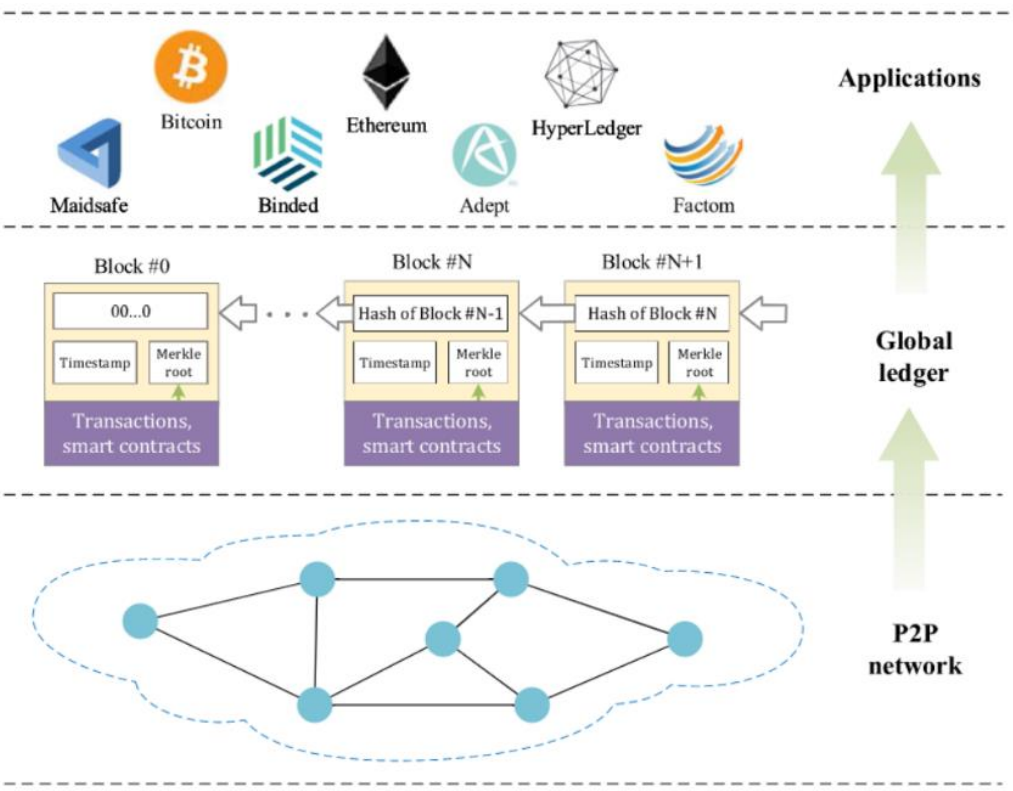
Obrázek 6 – DLT s oprávněním

Zdroj: [65, s. 19]

2 Blockchain

Blockchain poskytuje mechanismus, jehož prostřednictvím mohou vzájemně nedůvěřivé vzdálené strany (uzly) dosáhnout konsensu o stavu účetní knihy. [2] Pro pochopení toho, jak blockchain funguje je potřeba identifikovat jeho základní prvky. Blockchain je distribuovaná účetní kniha obsahující bloky (záznamy) informací, včetně informací o transakcích mezi dvěma nebo více stranami. Bloky jsou kryptograficky propojeny, aby vytvořily neměnnou účetní knihu. Uzly mohou přidávat informace do hlavní knihy prostřednictvím vyvolání transakcí.

Zásady přístupu určují, kdo smí informace číst. [2] Zásada kontroly určuje, kdo se může podílet na vývoji blockchainu a jak potenciálně mohou být nové bloky připojené k blockchainu. Konsensuální politika určuje, který stav blockchainu je platný, řeší případné spory, pokud se objeví konfliktní možná pokračování.



Obrázek 7 – Základní struktura technologie blockchain

Zdroj: [64]

2.1 Generace technologie blockchain

V průběhu existence blockchainu došlo k jeho technologickému vývoji, principy, na kterých je blockchain postaven zůstaly však stejné. [13] V důsledku tohoto technologického vývoje jsou rozeznávány různé generace blockchainu. K dnešnímu dni jsou známy tři funkční generace blockchainu. Stručný popis těchto generací je následující:

Blockchain první generace (blockchain 1.0) – Jedná se první typ blockchainu spojený s aplikacemi pro kryptoměny. [13] Zjednodušeně řečeno je to způsob, jak jsou potvrzovány transakce v DLT. První verzi implementace blockchainu a kryptoměny navrhl Satoshi Nakamoto a nazval ji BITCOIN. Jedná se o peer – to peer sériovou strukturu, která vyřešila problém udržení pořadí transakcí a problém double – spending, pomocí mechanismu řetězce složeného z uzlů a propojených pomocí hashů.

Blockchain druhé generace (blockchain 2.0) – Vznik druhé generace blockchainu je spojen s Ethereem. [13] V této generaci je implementován konsensuální algoritmus PoW (Proof of Work) a sada nových funkcí, které umožňují využití blockchainu i mimo oblast kryptoměn. Jednou z hlavních novinek v této generaci jsou chytré smlouvy a decentralizované aplikace DAPPS.

Blockchain třetí generace (blockchain 3.0) – Tato generace blockchainu je evolucí blockchainu 2.0 se zaměřením na rozšíření technologie do více aspektů společenského života. [13] Hlavním přínosem nové generace je umožnění interoperability a zvýšení rychlosti sítě za dodržení základních rysů blockchainu.

2.2 Typy technologie blockchain

V závislosti na tom, jak uživatelé přistupují k blockchainu a jak je řešen přístup k datům uložených na blockchainu jsou rozlišovány následující typy blockchainů:

Privátní blockchain – Přístup k blockchainu je řízen jeho vlastníkem, který dále rozhoduje o dalších otázkách týkajících se fungování blockchainu. [14] Těmito otázkami jsou především to, jaké jsou odměny za těžbu, které uzly jsou určeny jako validátory sítě atd. Z důvodu existence jediného vlastníka je tento typ blockchainu více považován za úzce zabezpečenou distribuovanou databázi, čehož je využíváno v určitých prostředích, kde jsou účastnící blockchainu velmi dobře známí, nebo kde je potřeba provádění auditů.

Veřejný blockchain – Přístup k tomuto typu blockchainu není žádným způsobem schvalován, tudíž kdokoli může na tomto typu blockchainu publikovat a ověřovat transakce, za což jsou těžaři odměňováni. [14] Tento typ blockchainu je využíván v kryptoměnách Bitcoin a Ethereum. Další užitečnost těchto blockchainů je tam, kde je požadována vysoká úroveň transparentnosti nebo masivní interakce.

Konsorcium – Jedná se o typ blockchainu, který je provozován skupinou vlastníků. [14] Tito vlastníci omezují přístup uživatelů k blockchainu a omezují jejich prováděné akce. Konsensuální algoritmus je provozován na předem vybrané skupině uzlů, což zvyšuje soukromí a rychlost ověřování transakcí. Typickým představitelem je Hyperledger – Fabric, kdy jeho účetní kniha je obsluhována více entitami.

2.3 Chytré kontrakty

Jedná se o jednoduché programy uložené na blockchainu, které běží v případě, že jsou splněny předem stanové podmínky. [15] Typicky jsou využívány pro automatické provádění dohod, takže jejich účastníci jsou si okamžitě jisti jejich výsledkem, a to bez jakéhokoliv zapojení dalšího zprostředkovatele a ztráty času.

Fungují na základě toho, že se řídí jednoduchými příkazy zapsanými v kódu na blockchainu. [15] Uzly sítě provádějí v rámci transakce požadované akce za předem stanovených a ověřených podmínek, po dokončení těchto akcí je ukončena i transakce a dojde k aktualizaci celé sítě blockchainu. Tím je zabezpečeno to, že již provedenou transakci nelze změnit a výsledek transakce je viditelný pouze předem definovaným stranám, kterým bylo uděleno povolení.

2.4 Konsensuální algoritmy

Jedná se o algoritmus, který je základní součástí každé blockchainové sítě a jeho funkce spočívá v tom, že každá transakce, která je na blockchainu provedena je ověřena a zcela bezpečná. [16]. Algoritmus je založen na postupu, kdy všechny uzly v síti blockchainu dosáhnou společné shody o stavu DLT. Zjednodušeně řečeno, algoritmus zajišťuje to, že každý nově přidaný blok do sítě je jedinou verzí pravdy, na které se shodly všechny uzly v síti. Konsensuální protokoly jsou založeny na specifických cílech, tedy na způsobu, pomocí kterého dosahují shody. Těmi jsou například dosažení dohody, spolupráce, stejná práva pro každý uzel atd. Níže jsou stručně popsány vybrané příklady konsensuálních algoritmů.

Proof of Work (PoW) – Tento konsensuální algoritmus je používán k ověření transakce a vytvoření nového bloku na síti. [16] Základní myšlenka tohoto algoritmu spočívá ve vyřešení složité matematické úlohy s možností jednoduchého ověření. Vyřešení této matematické úlohy je velmi výkonově náročné a uzel, který tuto úlohu vyřeší jako první má právo k těžbě dalšího bloku.

Proof of Stake (PoS) – Jedná se o algoritmus, který je velmi často využíván jako alternativa k PoW. [16] Princip tohoto algoritmu spočívá v investování mincí systému validátory. Ti některé své mince označí jako sázky a poté začnou ověřovat bloky na síti. Validátor ověří blok tím, že na něj vsadí, a to pouze tehdy, pokud si myslí že našli blok, který by mohl být přidán do blockchainu. Na základě bloků, které byly přidány do blockchainu, všichni validátoři obdrží odměnu v závislosti na výši jejich sázek a úměrně k tomu se zvýší jejich příští sázka. Na konci je vybrán validátor na základě jeho ekonomického podílu v síti, který vygeneruje nový blok.

Zero Knowledge Proof (ZKP) – Algoritmus, který je založen na prokázání tvrzení, aniž by bylo odhaleno samotné tvrzení. [17] Aby bylo možné prokázat pravdivost tvrzení, aniž by byl jeho obsah odhalen, spoléhá tento algoritmus na algoritmy, které mají na vstupu určitá data a na výstupu vracejí buď „pravda“ či „nepravda“.

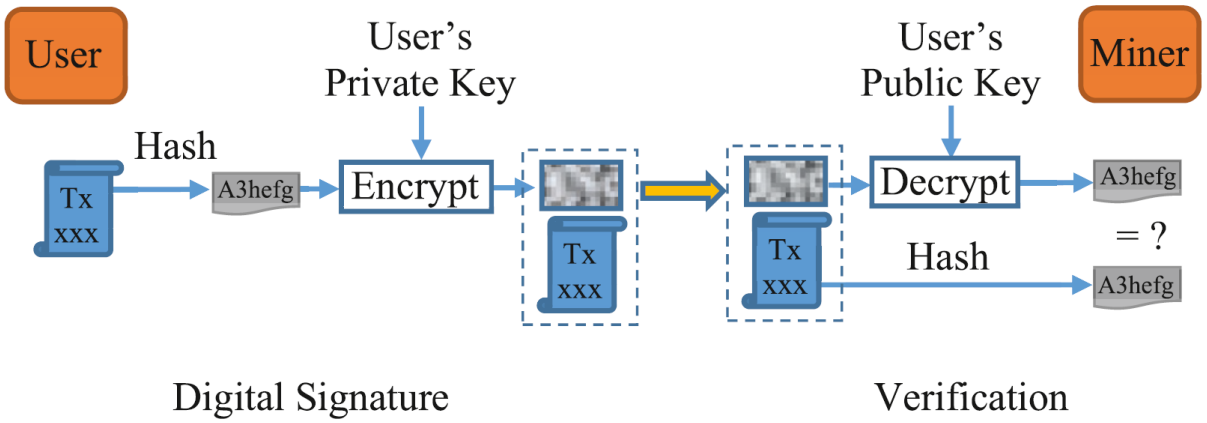
Byzantine Fault Tolerance (BFT) – Typ algoritmu vycházející z „Problému byzantských generálů “k dosažení shody na síti, které je dosaženo i přes to, že některé uzly nereagují, nebo podávají nesprávné informace. [16] Cílem mechanismu tohoto algoritmu je chránit se před selháním celého systému pomocí kolektivního rozhodování s cílem omezit vliv chybných uzlů. Tohoto je dosaženo pomocí dohody fungujících uzlů na určitých hodnotách a tím dosáhnout shody o tom, které uzly selhaly.

2.5 Zabezpečení blockchainu

Zabezpečení blockchainu je řešeno pomocí kryptografie, konkrétně šifrováním pomocí veřejného klíče a Hash funkcí. [18]

Šifrování pomocí veřejného klíče – V technologii blockchain je tento druh asymetrického šifrování využíván k prokázání, že transakce na blockchainu byla vytvořena správnou osobou. [18] Soukromý klíč je v blockchainu uchováván buď v hardwarové peněžence, nebo jakékoli softwarové peněžence. Pro podepsání zprávy přenášené na blockchain je využíván uživatelův soukromý klíč, a veřejný klíč je využit pro potvrzení, že

zpráva přišla od uživatele, který je jejím původcem. Názorný příklad viz obrázek. Obrázek 8. Algoritmus je páteří blockchainu umožňující podepisování a ověřování uživatelem prováděných transakcí. Široce využívaný algoritmus k vytvoření páru veřejného a soukromého klíče v blockchainu je Elliptic Curve Digital Signature Algorithm (ECDSA). Veřejný klíč uživatele je v blockchainu velmi často využíván ke skrytí reálné identity uživatele.



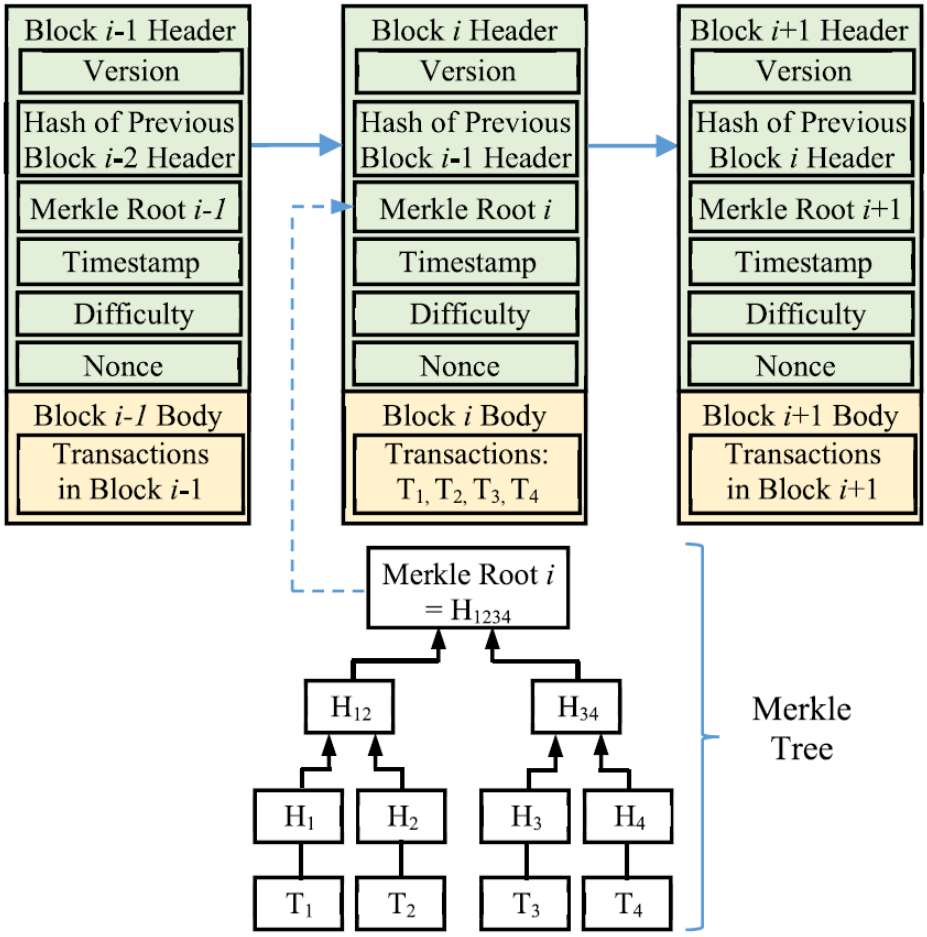
Obrázek 8 – Šifrování a dešifrování v blockchainu

Zdroj: [18]

Funkce Hash – Jedná se o klíčovou technologii využívanou v blockchainu. [18] Jedná se o matematickou rovnici s důležitými vlastnostmi pro kryptografii. Těmito vlastnostmi jsou:

- **Pevná velikost** – hashovací funkce má jakkoli dlouhý vstup, který matematicky přetransformuje na pevně velký výstup,
- **Odolnost předlohy** – po matematickém transformování vstupu na výstup není možná zpětná matematická transformace. Jedinou možností je náhodné vkládání dat do hashovací funkce, dokud není vytvořen stejný vstup,
- **2. odolnost předlohy** – pokud je zadán vstup1 a jeho hash1, je výpočetně neproveditelné získání vstupu2, který je rozdílný od vstupu1, a který má hash2 roven hash1,
- **Odolnost proti kolizi** – je výpočetně nemožné nalézt dva rozdílné vstupy, které by měli stejné hashe,
- **Velká změna** – pokud je ve vstupu změněn jakýkoliv bit, je vytvořen zcela nový hash na výstupu.

Propojení jednotlivých bloků blockchainu je založeno na principu, kdy hash předchozího bloku je uložen v záhlaví bloku následujícího. Graficky je tento princip propojení zobrazen viz Obrázek 9. Blockchain také hashuje každou transakci pro Merkel Tree (zobrazen pod *Blokem i*), jehož kořen je uložen v hlavičce každého bloku. Tímto způsobem je vytvářena DLT. Pokud dojde ke změněn jakéhokoli bloku, transakce či informace v tomto bloku, je tato změna okamžitě odhalena a spojení mezi tímto blokem a blokem následujícím (potažmo všemi následujícími bloky) je přerušeno.



Obrázek 9 – Propojení bloků v blockchainu

Zdroj: [18]

3 Volby

Definice voleb dle [19] říká, že se jedná o techniku, pomocí které je možno vybrat omezený počet možností dle daných pravidel, která jsou předem stanovena.

Dnes jsou volby základním stavebním kamenem demokracie, ve které si voliči volí své preferované kandidáty, kteří za ně rozhodují. [19] Princip voleb je založena na tom, že každý volič disponuje právě jedním hlasem, pomocí kterého zvyšuje šanci svého preferovaného kandidáta na jeho zvolení. Tento hlas je voličem různými způsoby odevzdáván před volební komisí, která je vytvořena z nezávislých pozorovatelů.

Způsobů, kterými jsou hlasy odevzdávány, existuje velké množství, od klasických papírových lístků vhazovaných do volební urny až po různé druhy elektronických voleb, tzv. e-voleb. [19]. Nové typy e-voleb by v ideálním případě mohl volič využívat odkudkoli, nicméně e-volby skýtají některá úskalí. Jedním z těchto úskalí je samotná registrace občana, kdy je nutné zajistit, aby volič odevzdal právě jeden hlas.

Samotné volby by měli být:

- rovné – váha a počet hlasů každého občana by měl být shodný,
- tajné – volba každého jednotlivce je známá pouze jemu a nikomu jinému,
- všeobecné – voleb se může zúčastnit kdokoliv, kdo splní stanovená omezení,
- přímé – bez účasti třetí strany. [19]

3.1 Druhy voleb

Volby lze rozlišit dle několika různých kritérií. Těmi jsou především volby podle bezprostřednosti, územního rozsahu a periodicity. [20]

Podle bezprostřednosti volby

- Přímé volby – volby, kde voliči hlasují pro daného kandidáta a rozhodují tak přímo o tom, zda bude či nebude daný kandidát zvolen. [20]
- Nepřímé volby – v tomto druhu voleb neřeší samotnou volbu vhodných kandidátů přímo voliči, ale tzv. volitelé (poslanci, senátoři, ...).

Podle územního rozsahu

- Všeobecné – volby, kde je volen např. celý zákonodárný orgán (v ČR např. Poslanecká sněmovna). [20]
- Dílčí – v tomto případě je volena pouze část zákonodárného orgánu (v ČR jedna třetina senátu každé dva roky).
- Doplňovací – volby, kde jsou voleni kandidáti na volná místa způsobená rezignací, úmrtím atd.

Podle periodicity

- Řádné – volby uskutečněné po skončení funkčního období pro daný orgán. [20]
- Mimořádné – volby uskutečněné před uplynutím řádného funkčního období daného orgánu.

3.2 Volební právo

Volební právo dává občanům možnost účastnit se všech možných druhů voleb daného státu, samosprávy atd. Volební právo je rozlišováno na aktivní a pasivní.

Aktivní volební právo – Občan má právo stát se voličem, a tudíž hlasovat pro svého kandidáta, jestliže není omezen volebním cenzem, což znamená, že mu je z jistého důvodu toto právo odepřeno. [21] V minulosti tímto cenzem býval majetek, nebo příjem. V dnešní době je cenzem především věk (v ČR mohou volit pouze občané starší osmnácti let).

Pasivní volební právo – Jedná se o právo, kdy má občan nárok na to, aby mohl být volen. [21] Toto právo připadá většinou všem držitelům aktivního volební práva, ale za jiných podmínek, a to především těch, které se týkají dosaženého věku občana (členem Poslanecké sněmovny v ČR se může stát pouze občan starší jedenadvaceti let a Senátu pouze občan, který dosáhl věku čtyřicet let v den voleb).

3.3 Volební systém

Jedná se o označení způsobu, kterým jsou ve volbách obsazovány jednotlivé funkce na základě odevzdaných hlasů jednotlivých hlasujících. [22] Zahrnuje v sobě veškerá pravidla, kterými jsou povinni se řídit všichni účastníci voleb, dále obsahuje mechanismy pro příděl mandátů pro jednotlivé kandidáty, dle počtu získaných hlasů. Dále tyto systémy určují způsoby provedení a organizaci voleb. Volební systémy jsou rozděleny na základě principů, kterými přidělují mandáty na:

- majoritní systémy,
- proporční systém,
- semiproporční systémy. [22].

Majoritní systémy – Majoritní neboli většinový systém je založen na principu, který lze nejlépe vystihnout jako „*vítěz bere vše*“. [22] Ten, kdo vyhrál volby v daném volebním okrsku získává veškeré mandáty daného okrsku. Tento systém je charakteristický pro volbu prezidenta či starostů. Jsou rozeznávány následující typy majoritních systémů:

a. Jednokolové
    i. nominální – jako hlavní měřítko slouží relativní většina,
    ii. ordinální – voliči přímo určují to v jakém pořadí se jednotlivý kandidáti umístí.
b. Vícekolové

Proporční systémy – V tomto případě volebního systému jsou jednotlivé mandáty rozdělovány tak, aby odrážely určitý poměr. [22] Nejvíce využívanou metodou pro stanovení poměrného rozdělení mandátů je D'Hondtova metoda, která je více příznivá pro strany s nejvíce získanými počty hlasů. Dělí se na:

a. jmenné – hlasy jsou odevzdávány ve prospěch jedinců (kandidátů),
b. listinné – hlasy jsou odevzdávány ve prospěch kandidující strany.

Semiproporční systémy – Jedná se o systémy voleb, kdy jsou v jednotlivých okrscích pomocí principu majoritního systému přiřazeny mandáty právě těm voleným zástupcům, kteří obdrželi od voličů nejvíce hlasů. [22] Tento systém však nezaručuje, že jedna kandidátka obdrží veškeré mandáty. Tyto systémy jsou děleny na:

a. Volič disponující více hlasy
    i. neomezené hlasování,
    ii. kumulované hlasování,
    iii. souhlasné/nesouhlasné hlasování,
    iv. Bordovo hlasování,
    v. bodové hlasování.
b. Volič disponující jedním hlasem
    i. omezené hlasování,
    ii. hlasování jednoho nepřenosného hlasu.

4 Elektronické volby – požadavky na bezpečnost

Volby, ať již tradiční, v podobě papírových volebních lístků, prostřednictvím digitálních volebních zařízení nebo online hlasovacích systémů, musí vždy splňovat určité požadavky na bezpečnost. Tyto požadavky jsou zmiňovány v každém článku zabývajícím se problematikou elektronických voleb. Zde jsou představeny pouze některé vybrané bezpečnostní požadavky, které by měl každý systém elektronických voleb splňovat.

Soukromí – Jedná se o prevenci v asociování voliče a hlasu. [23] Soukromí voliče musí být zachováno jak během voleb, tak i po nich. Aby byl tento požadavek splněn, musí být zajištěna nepropojitelnost a nevysledovatelnost voliče. Voliče lze identifikovat pomocí dvou identit. Těmi jsou registrační identita a veřejný klíč voliče. Nikdo nesmí být schopen odvodit vztah mezi těmito dvěma identitami a odevzdaným hlasem. [24] Pokud je toto zajištěno je splněna podmínka nepropojitelnosti. O nevysledovatelnosti mluvíme v tom případě, jestliže je zajištěna nedohledatelnost IP adresy počítače voliče, nebo vztahu mezi voličem a hlasem.

Způsobilost – Tento požadavek říká, že voleb se mohou zúčastnit pouze oprávnění voliči. [23] [24]Ti se před samotnými volbami musí zaregistrovat prostřednictvím jedinečných identifikátorů, jakými jsou dokumenty vydané státem. Tímto volič potvrdí svou způsobilost.

Jedinečnost – Voliči, který se zúčastnil hlasování, je započítán pouze jeden hlas. [23]

Spravedlnost – Bezpečnostní požadavek zaměřen na to, zdali před koncem hlasování nedošlo ke zveřejnění částečného součtu hlasování a tím k ovlivnění dalšího průběhu voleb. [23] [24]Toto se týká také sčítacích orgánů.

Nedonutitelnost – Jedná se o zabezpečení odevzdání hlasu pod nátlakem. [23] Tedy žádná třetí strana by neměla být schopna ovlivnit odevzdání voličova hlasu do systému. [24] Každý volič musí mít zajištěnou svobodnou volbu.

Receipt Freeness – Volič by neměl být schopen prokázat třetí straně, jak hlasoval. [23] [24] Systém musí kryptograficky zajistit odevzdání hlasu do systému pomocí tzv. „hashe“. Tento bezpečnostní požadavek má za úkol zabránit kupování a prodeji hlasů.

Přesnost – Výsledek hlasování musí odpovídat součtu odevzdaných hlasů. [23] [24] Tento požadavek lze rozdělit na dvě dílčí podmínky. Tou první je úplnost, tedy že je třeba sečíst všechny platné hlasy. Druhou podmínkou je důkladnost, což znamená, že hlasy, které byly odevzdány neoprávněným nebo neověřeným voličem, nebo je samotný hlasovací lístek neplatný, nesmějí být započítány.

Individuální kontrola – Systém musí voliči umožnit kontrolu odevzdaného lístku pomocí potvrzení o hlasování. [23] Ta musí spočívat v kontrole toho, zda byl hlasovací lístek do systému skutečně odevzdán a zda byl započítán do konečného výsledku hlasování. [24] Tato kontrola nesmí voliči umožnit kontrolu toho, jak hlasoval.

5 Elektronické volby – technická řešení

Elektronické hlasování, známé také pod pojmem „*e-voting*“ je hlasování využívající elektronické prostředky, které pomáhají nebo se starají o odevzdání a sčítání hlasů. [25] Systémy pro elektronické hlasování jsou využívány již od šedesátých let dvacátého stolení, kdy byly na trh uvedeny systémy děrných štítků, které následovaly systémy optického skenování, systémy DRE a internet. V závislosti na konkrétní implementaci lze elektronické hlasování rozdělit na dvě skupiny. První skupinou je e-voting využívající samostatné elektronické hlasovací přístroje, známé také jako EVM (*Electronic Voting Machine*). Druhou skupinou je e-voting, který pro potřeby hlasování využívá počítače připojené k síti Internet. Tento způsob implementace může využívat celou řadu internetových služeb, od přenosu výsledků v podobě tabulek až po plně funkční online hlasovací systém. Stupeň automatizace může být definován od označování papírových hlasovacích lístků až po sofistikovaný systém odevzdávání hlasů, šifrování a přenos dat na servery, konsolidace a sumarizace volebních výsledků.

Elektronických volebních systémů existuje mnoho různých typů. V následujících podkapitolách jsou představeny ty nejběžnější. Jsou zmíněny také systémy, které se již přestaly používat.

5.1 Systém děrných štítků

Tento typ elektronického volebního systému byl poprvé použit v USA v prezidentských primárních volbách v roce 1964 ve státě Georgia. [26] Princip systému spočívá v děrování karty voličem pomocí dodávaného děrovacího zařízení. Tímto způsobem volič hlasuje pro své vybrané kandidáty. Poté co volič odhlasuje, může proděravěný štítek vložit přímo do počítačového zařízení ve volební místnosti sloužícího k zaznamenávání hlasování. Druhou možností je vložení štítku do volební urny, která je po skončení hlasování převezena na centrální místo, kde dojde k vložení štítků do stejného zařízení jako ve volební místnosti.

Typů děrných štítků bylo mnoho, ale nejpoužívanějšími byly VOTOMATIC a DATAVOTE. [26] Štítky VOTOMATIC obsahovaly místa, ve kterých bylo možné prorazit otvor a tím označit hlas, přiřazená číslům. Tato čísla jsou jediné vytištěné informace na štítku. Pro to, aby volič věděl, jaké číslo odpovídá, kterému kandidátovi a jakým způsobem prorazit otvor, musel používat vytištěnou brožuru. Naproti tomu štítky DATAVOTE měly na sobě vytištěna jména kandidátů, vedle kterých byla místa k proražení otvoru.

5.2 Optické skenovací systémy

Systémy elektronických voleb založených na optickém skenování lze rozdělit do tří základních skupin.

Marksense – U tohoto typu optického skenovacího systému se jedná o kombinaci papírového hlasovacího lístku a elektronického zařízení. [27] Volič hlasuje tak, že na papírovém hlasovacím lísku tužkou označí zvoleného kandidáta. Takto označený hlasovací lístek vhodí do volební urny. Po skončení hlasování jsou lístky vyjmuty a vloženy do OSVM (Optical Scan Voting Machines) pro elektronickou tabelaci. Tento systém využívá ke čtení hlasovacích lístků techniku optického rozpoznávání značek OMR. Jedná se o proces čtení značek vytvořených na papíře nebo dokumentu. Novější systémy využívají technologii OCR, která oskenuje celý dokument jako obrázek a pomocí počítačového softwaru rozpozná tvar tištěných či psaných znaků. [26]

Electronic ballot marker EBM – Elektronické označování hlasovacích lístků EBM je část hlasovacího systému, který volič využívá pouze k vyplnění papírového hlasovacího lístku. [27] Jedná se především o dotykové obrazovky, klávesnice atd. EBM zaznamená hlasování buď na papírovém hlasovacím lísku, nebo ho vytiskne. Tyto lísky jsou poté manuálně sčítány pomocí skeneru.

Digitální pero – Tento typ systému využívá digitální pero, což je zařízení schopné vyznačovat a skenovat značky na hlasovacím lístku. [27] K tomuto účelu využívá hlasovací lístek na digitálním papíře. Digitální pero obsahuje malou kameru, která rozpozná, kde na hlasovacím lístku volič udělal značku a po dokončení hlasování odešle zaznamenané značky do počítače. Pero je poté vráceno volebnímu úředníkovi.

5.3 Direct Recording Electronic (DRE) voting system

Tento systém elektronického hlasování vznikl v důsledku rozvoje výpočetní techniky na konci devadesátých let dvacátého století. [26] Princip tohoto systému spočívá v označování hlasů voličů přímo do elektronického zařízení skrze dotykové obrazovky, tlačítka a další obdobná zařízení. V systému tedy nejsou využívány papírové hlasovací lístky. Údaje o hlasování jsou uloženy elektronickým zařízením na různé druhy paměťových médií, jakými jsou například pevné disky, CD-ROM, čipové karty atd. Pro účely zálohování a ověřování hlasování je prováděno kopírováním dat o hlasování na více paměťových medií. Po ukončení hlasování jsou data přenesena do centrálního uzlu, kde jsou za pomocí výpočetní techniky sečteny. Přenos dat je uskutečněn fyzickým přenesením paměťových médií do centrálního uzlu.

5.4 Public Network DRE

Jedná se o vylepšený systém elektronických DRE. [28] Rozdíl spočívá v odevzdávání hlasovacích lístků. Ty jsou přenášeny elektronicky pomocí veřejné sítě do centrálního serveru. Hlasovací lístky mohou být přenášeny jednotlivě, tak jak jsou odevzdávány, nebo mohou být odesílány periodicky jako dávky v průběhu voleb anebo jako jedna dávka po skončení hlasování. V tomto typu elektronických voleb je možné od konce devadesátých let minulého století využít pro hlasování i mobilní telefon. [26] Voliči postupují dle předem zaznamenaných pokynů, identifikují se pomocí osobních identifikačních čísel PIN (*Personal Identification Number*) a hlasují pomocí klávesnice mobilního telefonu, kde je toto hlasování zaznamenáno přímo do sčítacích systémů.

5.5 Internetové hlasování

Lze rozlišit tři různé formy systémů elektronického hlasování prostřednictvím globální sítě Internet. [26]

Pooling Site Internet voting – Jedná se o systém hlasování, kde volič odevzdává hlas pomocí internetu a klientských zařízení, která jsou fyzicky umístěna v oficiálních volebních místnostech. V těchto místnostech dochází také ke kontrole HW a SW klientských zařízení. Identifikace a autentizace voliče probíhá prostřednictvím tradičních prostředků.

Kiosk internet voting – Hlasování voličů probíhá prostřednictvím klientských zařízení, ve kterých je SW a HW pod kontrolou volebních úředníků. [26] Tato klientská zařízení jsou umístěna na veřejných místech, kde fyzické prostředí, identifikace a autentizace voličů není pod přímou kontrolou volebních úředníků.

Remote internet voting – V tomto případě internetového hlasování nejsou klientské stanice ani fyzické prostředí pod kontrolou volebních úředníků. Oproti předchozím formám internetového hlasování, je tato forma nejméně bezpečná. Identifikace, autentizace a samotné hlasování voliče je prováděno z prostředí domova, pracoviště či veřejného internetového terminálu.

6 Hodnocení přístupů k elektronickým volbám

Tato kapitola se věnuje systematické literární rešerši na téma „Využití blockchain technologií pro zajištění bezpečnosti a důvěryhodnosti při elektronických volbách“.

Pro zpracování samotné systematické literární rešerše bylo nutné nalezení relevantních článků zabývajících se zadanou problematikou. Pro tyto účely byly využity databáze WoS a Scopus. V první fázi byly ve zmíněných databázích vyhledány články, které splnili fultextové vyhledávání „*blockchain and vote*“. Toto vyhledávání bylo uskutečněno v dubnu roku 2022, což mělo za následek menší počet vyhledaných článků v roce 2022. V databázi WoS tomuto vyhledávání odpovídalo čtyři sta sedmdesát šest článků a v databázi Scopus tři sta padesát tři článků. Bibliometrické údaje těchto článků byly z obou databází exportovány do sešitu MS Excel pro účely další analýzy. Ta spočívala v odstranění duplicitních článků. Po odstranění duplicit zbylo pro další fázi výzkumu sto padesát osm článků, jež byly publikovány mezi roky 2017 a 2022 (viz Graf 1).

Graf 1 – Rozložení publikovaných článků mezi jednotlivé roky

Zdroj: Vlastní zpracování

Ve druhé fázi výběru relevantních podkladů pro systematickou literární rešerši byla provedena analýza abstraktů všech sto padesáti osmi článků se zaměřením na to, zda daný článek popisuje systém elektronických voleb s použitou technologií blockchain. Pokud daný

článek toto první kritérium splňoval byl podroben analýze i jeho celkový obsah. Ze seznamu článků pro výzkum byly dále vyřazeny články, které nesplňovaly minimální počet stran. Tento minimální počet stran byl stanoven na šest. Na konci druhé fáze výběru bylo nalezeno dvacet šest vhodných článků pro využití ve finální fázi. V rámci druhé fáze byly také identifikovány atributy, dle kterých byl proveden vlastní výzkum nad vybranými články.

Samotný výzkum probíhal tím způsobem, že zvolené články byly podrobeny detailní analýze, která se snažila v každém z nich najít popis implementace jednotlivých atributů. Výsledky výzkumu jsou zobrazeny viz Tabulka 1. Z této tabulky je na první pohled patrné, že ne vždy zkoumaný článek řešil všechny atributy, které byly předmětem výzkumu.

V následujících podkapitolách jsou popsány zvolené atributy a jejich implementace ve vybraných příkladech systémů elektronických voleb založených na technologii blockchain. V závěru této kapitoly, konkrétně v podkapitolách 6.12 a 6.13, jsou detailněji představeny dva systémy řešení elektronických voleb, jež lze označit jako nejvíce reálné implementace elektronických voleb založených na technologii blockchain, které byly zkoumané v rámci této diplomové práci.

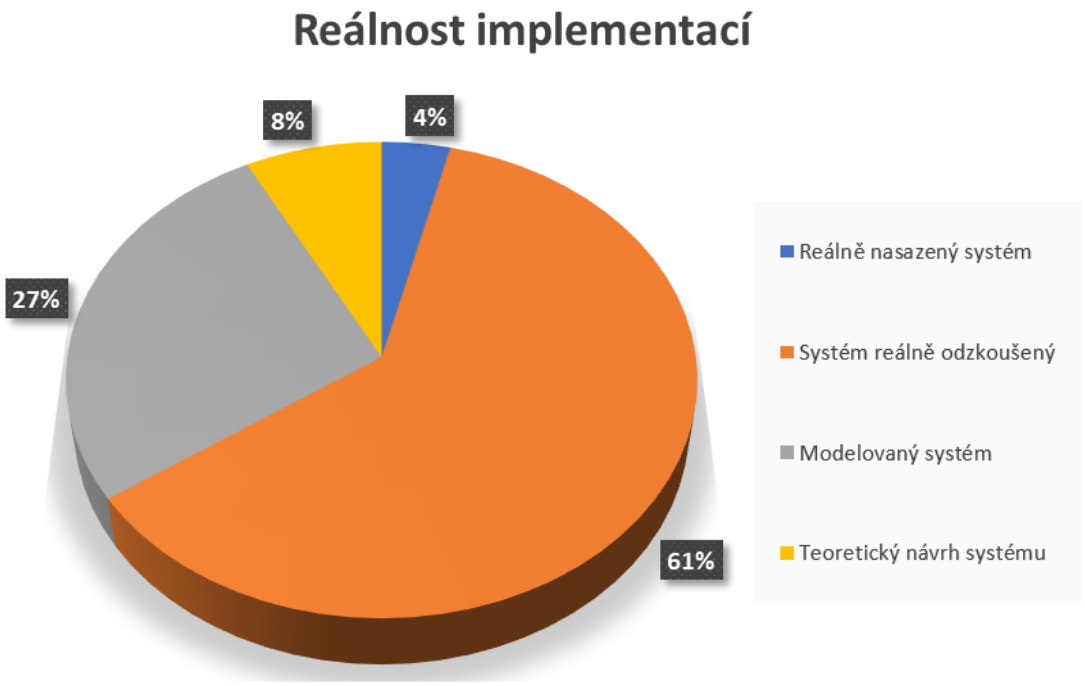
Tabulka 1 – Přehled zkoumaných řešení a vybraných atributů elektronických voleb využívající blockchain

Zdroj: Vlastní zpracování

Zdroj	Blockchain	Konsensus	Šifrování	Fáze	Entity	Registrace	Dostupnost	Potvrzení o hlasování	Ověření hlasování	Re-Voting
[29]	Ethereum	-----	Paillier	-----	3	Online	-----	-----	-----	-----
[30]	-----	-----	-----	3	3	Offline	Volební místo	Papírová forma	VIT	-----
[31]	-----	-----	-----	3	-----	Offline	Volební místo	Papírová forma	VIT	-----
[32]	-----	BFT	ECC	5	3	Offline	-----	Online	Protihodnoty	ANO
[33]	Ethereum	PoW	-----	5	2	Offline	Internet	Online	Chameleon hash	NE
[34]	Bitcoin	-----	-----	3	-----	Online	Internet	Online	ID transakce	NE
[35]	-----	-----	Paillier	6	4	Offline	Internet	Online	Protihodnoty	ANO
[36]	Monero	NI-ZKP	El Gamal	4	3	Offline	-----	-----	-----	ANO
[37]	Ballot Box	-----	-----	-----	-----	-----	Internet	Online	AV ID	ANO
[38]	Ethereum	PoW	-----	4	5	Online	Internet	Online	ID transakce	NE
[39]	Ethereum	PoS	El Gamal	5	6	Offline	Internet	Online	-----	ANO
[40]	-----	NI-ZKP	-----	7	4	Online	-----	-----	-----	-----
[41]	Ethereum	-----	-----	6	-----	Offline	Volební místo	-----	-----	NE
[42]	Ethereum	BFT	ECC	6	4	Online	Internet	Online	Hash transakce	-----
[43]	Bitcoin	-----	-----	5	4	Online	-----	-----	-----	-----
[44]	Ethereum	-----	-----	3	-----	Online	Internet	Online	-----	NE
[45]	-----	-----	Paillier	6	4	Online	Internet	-----	ID transakce	NE
[46]	Ethereum	-----	LRS	6	2	Online	-----	-----	Smart contracts	NE
[47]	Ethereum	-----	-----	5	5	Offline	Internet	Online	ID transakce	NE
[48]	-----	-----	-----	7	7	Offline	Volební místo	-----	ID transakce	ANO
[49]	Ethereum	PBSC - chain	-----	9	4	Online	Internet	-----	-----	NE
[50]	-----	-----	-----	3	3	Offline	Internet	Online	ID transakce	NE
[51]	Ethereum	NI-ZKP	-----	-----	-----	Offline	Volební místo	Papírová forma	Papírová forma	-----
[52]	-----	ZKP	-----	4	4	-----	-----	-----	-----	NE
[53]	Ethereum	PoSV	-----	3	10	Online	Internet	Online	TIN	-----
[54]	Ethereum	NI-ZKP	El Gamal	5	2	Online	Internet	Online	-----	-----

6.1 Reálnost implementací

V průběhu výzkumu, kdy byly jednotlivé články zkoumány na základě vybraných atributů, byla také sledována reálnost jednotlivých implementací elektronických voleb. Byly identifikovány čtyři druhy implementací, jejichž rozložení mezi zkoumané články je vyjádřeno graficky viz Graf 2.



Graf 2 – Reálnost implementací zkoumaných systémů voleb

Zdroj: Vlastní zpracování

Prvním druhem implementace je nasazení systému elektronických voleb v reálných podmínkách, tedy při reálných volbách. Z výše uvedeného grafu vyplývá, že takto realizovaných systémů jsou pouze čtyři procenta, což odpovídá jednomu reálně nasazenému systému. Tím je systém BroncoVote [29] použitý v USA při univerzitních volbách.

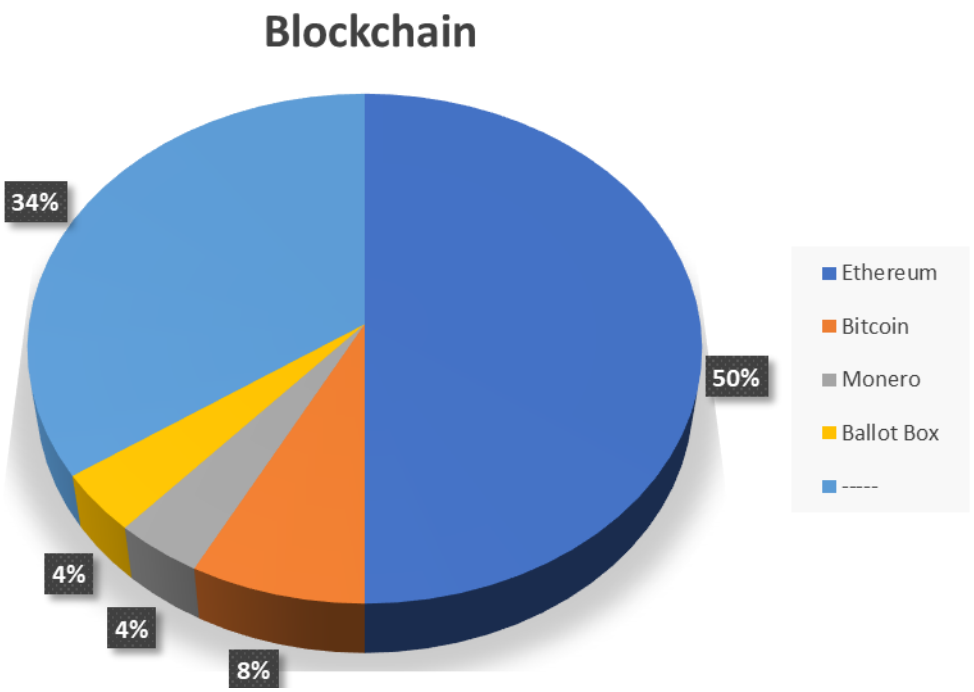
Druhým typem implementace jsou systémy elektronických voleb, které byly reálně odzkoušeny na testovacích blockchainových sítích. Tento způsob implementace je ve zkoumaných článcích nejvíce zastoupen, konkrétně v šedesáti jedna procentech.

Druhý nejpočetnější typ implementace elektronických voleb, dvacet sedm procent případů ve zkoumaných článcích je modelování systémů voleb pomocí modelovacího softwaru.

Posledním typem implementace je teoretický návrh volebního systému. Ve zkoumaných článcích se tato implementace objevila pouze ve dvou případech, tedy v osmi procentech.

6.2 Blockchain

Nejčastěji je pro potřeby elektronických voleb založených na technologii blockchain využit blockchain Ethereum (viz Graf 3). Z grafu je dále patrné, že třicet čtyři procent zkoumaných článků neuvádí použitý typ blockchainu vůbec.



Graf 3 – Využité typy blockchainů

Zdroj: Vlastní zpracování

Autoři [29] uvádějí, že pro potřeby jejich navrhovaného systému elektronických voleb byl použit blockchain Ethereum v nijak upravené či pozměněné formě. Jejich systém, nazvaný Bronco Vote, využívá funkcionality a vlastnosti poskytované Etherem, které mu umožňují vytvářet hlasovací lístky a hlasovat s nimi. Systém je tvořen třemi chytrými kontrakty vytvořenými v programovacím jazyce Ethereum's Solidity, jeden pro přípravu hlasování a definování kandidátů, druhý pro registraci voličů a třetí umožňuje odevzdat voličům jejich hlasy pomocí zašifrovaných hlasovacích lístků. Dále dvěma scripty napsaných v JavaScriptu a jednou HTML stránkou. Autoři [29] dále uvádějí, že aby uživatel mohl v jejich systému volit, musí vlastnit účet Ethereum. Pro tyto účely autoři navrhli dvě možná řešení, a to stažení a nainstalování pluginu Meta Mask do prohlížeče, nebo spuštění Ethereum uzlu na uživatelově PC a jeho synchronizaci s blockchainem.

V [33] autoři představují blockchain Ethereum jako jeden z nejpopulárnějších veřejných blockchainů v současnosti. Toto tvrzení zdůvodňují tím, že tento blockchain poskytuje vestavěný programovací jazyk zvaný Solidity. Dále se věnují podrobnější implementaci svého systému, kde popisují využití webového frameworku Truffle k psaní, kompilaci a ladění chytrých kontraktů vytvořených pomocí jazyka Solidity. Pro nasazení těchto chytrých kontraktů využívají typ blockchainu Ethereum zvaný Ganache. Dále autoři představují plugin MetaMask, sloužící ke správě voličských účtů a provádění transakcí.

V případě [38] autoři uvádějí, že pro své řešení elektronických voleb zvolili Ropsten Ethereum, což je testovací síť blockchainu založená na Ethereum. Autoři se dále zmiňují, že tato testovací síť poskytuje stejné prostředí jako hlavní síť Ethereum, s tím rozdílem, že Ropsten Ethereum je bezplatná. Autoři k této testovací síti přistupují skrze Remix online IDE, který umožňuje vývoj, nasazení a správu chytrých kontraktů pro blockchain Ethereum.

V [39] autoři využívají blockchain Ethereum především pro jeho velkou popularitu. Navrhují dvě verze implementace systému d-BAME, a to desktopovou aplikaci a aplikaci pro smartphony. Obě verze jsou založené na chytrých kontraktech psaných v jazyce Solidity, které jsou nasazovány skrze testovací síť blockchainu Ropsten Ethereum. Pro správu účtů a odevzdání hlasů v desktopové aplikaci autoři využili plugin MetaMask2, v aplikaci pro smartphony implementovali do kódu knihovnu web3swift.

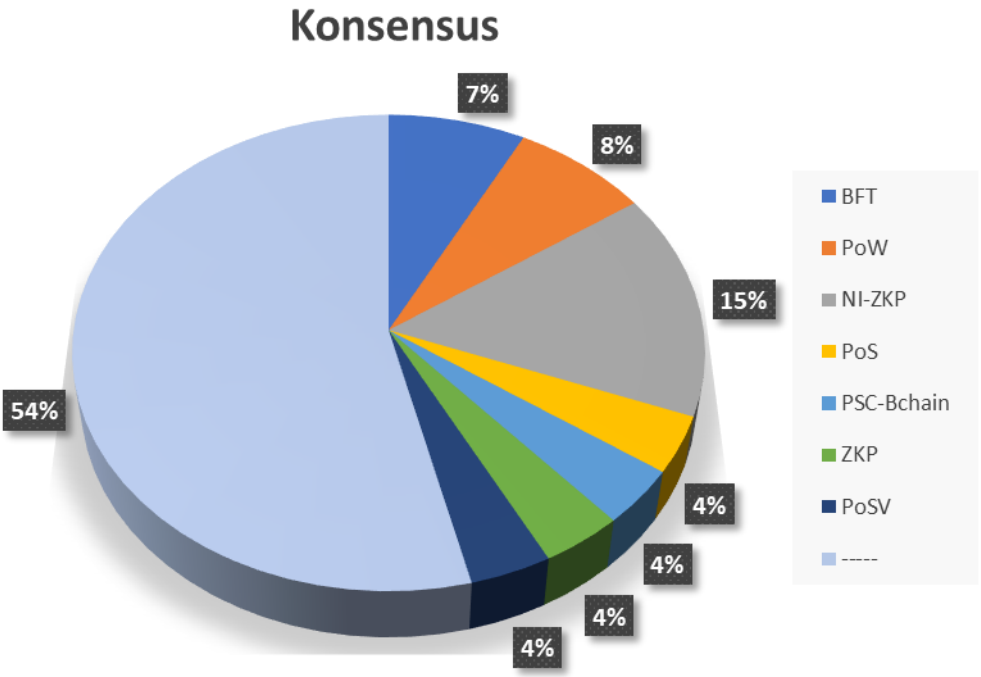
Autoři v [41] se pouze zmiňují o využití Ethereum blockchain API v jejich navrhovaném řešení elektronických voleb. Využití tohoto blockchainu zdůvodňují tím, že blockchain Ethereum je bezplatný a široce uznávaný pro tvorbu blockchain aplikací.

V [42] autoři popisují využití ekosystém blockchainu Ethereum, kde úložiště údajů a hlasovací schránka jsou implementovány v jednom chytrém kontraktu, který ukládá stav hlasování, informace o voličích a volební údaje.

Autoři článku [44] implementují své řešení pro E-Voting pomocí Ganache, což je osobní typ blockchainu založeném na Ethereum, který lze využít k nasazení smluv, vývoji aplikací a testování. Dále autoři využívají pro chytré kontrakty psané v jazyce Solidity framework Truffle Suite. Protože Ganache podporuje dvě možná rozhraní, CLI a GUI, autoři se rozhodli pro využití rozhraní GUI.

6.3 Konsensus

Ve zkoumaných článcích jednoznačně nepřevyšuje použití jednoho konsesu nad ostatními, jako je tomu u typu blockchainu. Je nutné také zdůraznit, že více jak v padesáti procentech články vůbec neuvádějí použitý typ konsensu. Z procentuálního zastoupení použitých typů konsesů (viz Graf 4) lze vyčíst, že pokud článek zmiňoval konsesus, tak se jednalo především o NI - ZKP, PoW a BFT.



Graf 4 – Využité typy konsensů

Zdroj: Vlastní zpracování

V [36] autoři zvolili typ konsensu neinteraktivní důkaz nulových znalostí neboli NI – ZKP, který použili ve fázi hlasování pro prokázání platnosti n-tice vytvořené voličem. Pro odevzdání hlasu si každý oprávněný volič sestaví hlasovací n-tici, která obsahuje jeho zašifrovaný hlas, zašifrované pověření a sadu neinteraktivních důkazů o nulových znalostech, které dokazují správnost n-tice. Dále autoři stručně popisují samotný protokol NI-ZKP, jako kryptografická primitiva umožňující jedné straně, nazývané „prověřovatel“, prokázat druhé straně, nazývané „ověřovatel“, že zná tajemství, aniž by odhalila tajemství samotné nebo jakákoli jiná.

Autoři [51] implementují dva konsensy NI-ZKP. Jeden ve fázi samotné volby a druhý ve fázi sčítání. Jedná se o autory vylepšený konsensus NI-ZKP navržený [55], který nazvali

1 – out – of – n NI-ZKP. Dále v článku autoři podávají důkaz o tom, že původní konsensus není navržen správně z důvodu nesplnění vlastnosti nerozlišitelnosti svědka důkazu o nulových znalostech. Předkládají také data z vlastních testů, která ukazují potenciál protokolu v reálném světě.

V [54] autoři využívají konsensus NI-ZKP ve fázi volební a ve fázi sčítání. Volební fáze je rozdělena do dvou kol. V prvním kole každý účastník voleb musí vypočítat svůj volební klíč za použití NI-ZKP, vygenerovaný pomocí Schnorrova podpisu. V druhém kole každý účastník vygeneruje NI-ZKP, který je spojen s jeho hlasovacím lístkem a slouží jako důkaz o správnosti hlasování. Ve fázi sčítání autoři využili NI-ZKP k zajištění toho, aby všichni účastníci striktně dodržovali protokol. Stejně jako volební fázi, tak i fázi sčítání rozdělili autoři na dvě kola. V prvním kole každý účastník zveřejní NI-ZKP, aby prokázal své znalosti o exponentech (x_{i1}, x_{i2} …, x_{ik}). Ve druhém kole každý účastník zveřejní „k“ NI-ZKP, aby dokázal, že jeho zašifrovaný hlas je permutací (a_1, a_2, …, a_k), aniž by věděl kterou.

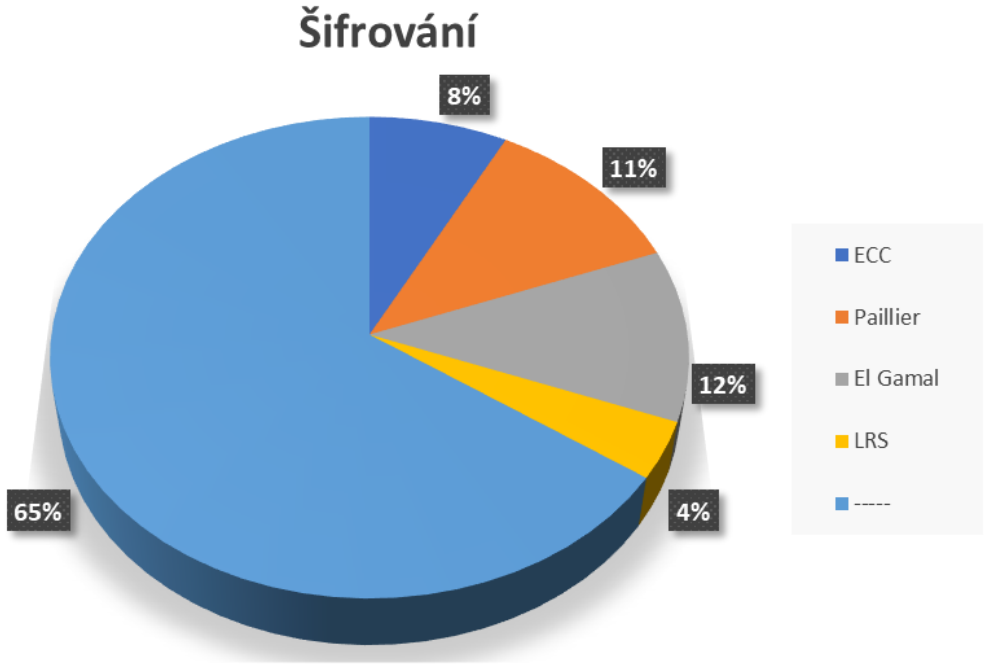
V případě [33] autoři nezmiňují detailní použití konsensu PoW v jejich práci. Pouze v kapitole, kterou nazvali „Background“, popisují vkládání a ověřování transakcí do řetězce speciálními uzly zvanými „těžaři“, kdy tyto uzly mohou svou práci vykonat až po výpočtu vykonané práce, tzv. Proof of Work.

Autoři [38], obdobně jako v předešlém případě, nezmiňují konkrétněji použití konsensu PoW. Pouze konstatují, že použili Ropston Ethereum blockchain, což je veřejný blockchain využívající konsensus PoW.

Autoři v [32] v kapitole „Background“ popisují základy konsensu „*Byzantine Fault Tolerance (BFT)”*. Vlastní nasazení tohoto konsensu autoři popisují v podkapitole 3.3, kde postupně prochází jednotlivé fáze jejich řešení systému elektronických voleb, nazvané DABSTERS. Samotný konsensus je využit ve fázi „Validace“, ve které je použit pro ověření správnosti seznamu způsobilých voličů. Tato transakce obsahuje pět kroků. Dále tento konsensus autoři použili ve fázi „Volební“, kde ho je využito „Sčítací autoritou“ k zasílání zašifrovaných volebních lístků voličům prostřednictvím blockchainu. I zde tato transakce prochází pěti kroky. Poslední fáze, ve které autoři využili konsensus BFT, je fáze „Sčítání“. Zde je tento konsensus autory využit k transakci, která čte odevzdané zašifrované hlasovací lístky voličů z blockchainu.

6.4 Šifrování

Obdobně jako je tomu u použitého typu konsensu ve zkoumaných článcích, tak i v případě využitého typu, nebo lépe systému šifrování, není v článcích jednoznačně preferován jeden systém před druhým. I zde je nutno zmínit, že přes šedesát procent zkoumaných článků vůbec nezmiňuje použitý typ šifrování. Z grafu níže je zřejmé, že pokud byl v článku uveden typ šifrování, jednalo se buď o šifrovací systém El – Gamal, Paillier, LRS nebo využití kryptografie eliptických křivek (ECC). V následujících příkladech je popsána implementace těchto kryptografických systémů.



Graf 5 – Využité typy šifrování

Zdroj: Vlastní zpracování

V [29] autoři využili šifrování pomocí systému Paillier homomorphic encryption pro zašifrování a dešifrování všech volebních hlasů. Pro tyto účely autoři vytvořili entitu Crypto.js (JavaScript pojmenovaný Crypto), který funguje jako kryptografický server. Nový hlas je na tento server odeslán pro jeho zašifrování pomocí veřejného klíče, který byl na tomto serveru již dříve vygenerován. Na tomto kryptografické serveru je dále prováděno homomorfní sečtení aktuálně zašifrovaných hlasů a již dříve zašifrovaných hlasů. V závěru se autoři zmiňují o plánování integrace systému šifrování Paillier jako knihovny do jazyka Solidity. Přínosem by mělo být zlepšení individuálního ověření hlasování a možnost vygenerování soukromého

a veřejného klíče pro každý hlasovací lístek, což by umožnilo individuální auditování voličů a jejich hlasovacích lístků, bez ohrožení ostatních hlasovacích lístků.

Autoři [35] využívají ve svém systému elektronických voleb kryptografický systém Paillier ve fázi „*Autentizace*“ pro zajištění zašifrování a dešifrování autentizačních parametrů voliče a následného ověření jeho legitimity. Dle popisu autorů volič zašifruje své autentizační parametry veřejným administrátorským klíčem, podepíše je svým podpisovým tajným klíčem a takto zašifrované autentizační parametry zašle administrátorovi. Následně administrátor ověří podpis voliče, čímž potvrdí jeho legitimitu. Dále administrátor dešifruje autentizační parametry, vypočítá dle zadaného vzorce hodnoty, které porovná s hodnotami autentizačních parametrů voliče. Pokud najde stejné hodnoty, volič je zaregistrován a obdrží právo volit. Systém Paillier autoři použili i pro další fázi nazvanou „*Hlasování*“. V této fázi sčítací autorita náhodně vybere hlasovací lístek pro každého voliče, zašifruje jej veřejným klíčem voliče a zašle jej voliči v transakci pomocí blockchainu. Volič pomocí svého tajného klíče dešifruje hlasovací lístek, vybere kandidáta a lístek zašifruje. Poté odevzdá svůj hlasovací lístek pomocí blockchainu sčítací autoritě.

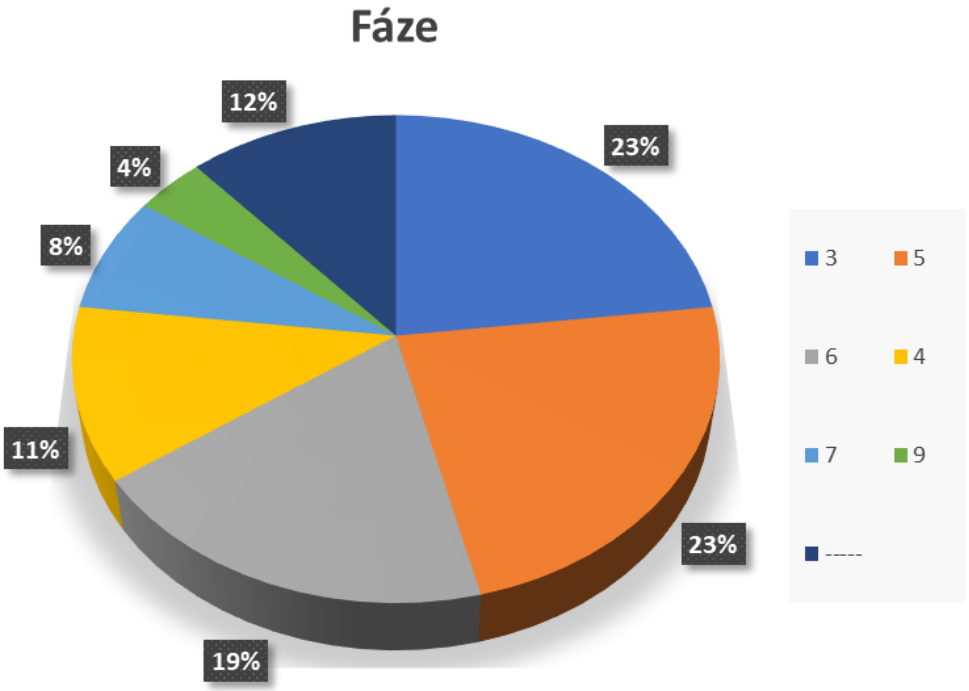
V případě [36] autoři využívají kryptografický systém El – Gamal, jehož podrobnější použití ve své práci nerozebírají. Pouze v kapitole „*Základní pojmy*“ stručně popisují jeho princip při generování klíče, šifrování a dešifrování. Dále se autoři letmo zmiňují o jeho využití ve fázích „*Nastavení*“ a „*Sčítání*“.

V [39] se autoři stejně jako v předcházejícím případě rozhodli o využití kryptografického systému EL – Gamal. A obdobně jako v předcházejícím případě, tak i zde je pouze zmínka o využití tohoto kryptografického systému ve fázi „*Získání hlasovacího lístku*“, kde entita zvaná „*Registratorl*“ pomocí tohoto kryptografického systému digitálně podepíše jím vygenerovaný hlasovací lístek.

Autory článku [46], ve kterém popisují svoje řešení voleb pomocí blockchainu, je využíván kryptografický systém zvaný „*Linkable Ring Signature (LRS)”*. Autoři tento systém využívají ve fázi „*Hlasování*“, kde tento systém slouží ke skrytí identity každého voliče a k zabránění vícenásobného hlasování. Skrytí identity voliče je dle autorů dosaženo tak, že LRS umožňuje každému voliči vygenerovat podpis ze seznamu veřejných klíčů a tajného klíče, jehož odpovídající veřejný klíč je v seznamu. Nikdo tedy, vyjma toho, kdo podpis vygeneroval, neví, kdo daný podpis vygeneroval. Kontroly vícenásobného hlasování autoři dosahují pomocí detekce dvou a více vygenerovaných podpisů stejným signatářem.

6.5 Fáze

Zkoumané články nabízejí celkem široké rozpětí v počtu fází, kterými jednotlivá navrhovaná řešení elektronických voleb založených na použití blockchainu procházejí. Nutno říct, že i zde se našla malá skupina článků, která se vůbec nezmiňovala o počtu fází, kterými navrhované řešení prochází. Celkem těchto článků bylo dvanáct procent, což odpovídá třem zkoumaným řešením. Články, které fáze zmiňovaly, udávaly počet těchto fází mezi třemi a devíti. Nejpočetnější skupinou byly články zmiňující tři, pět a šest fází. Vše je graficky znázorněno viz Graf 6.



Graf 6 – Počet navržených fází elektronických voleb

Zdroj: Vlastní zpracování

Autoři [30] představují systém elektronických voleb nazvaný „*Auditable Blockchain Voting System (ABVS)*“, ve kterém volby procházejí třemi fázemi. Těmi jsou „*Initiation phase*, *Voting phase, Counting and verification phase*“. Jak popisují autoři, v „*Initiation phase*“ jsou vybrány důvěryhodné instituce za účelem vytvoření sítě uzlů pro správné fungování technologie blockchain. Dalším krokem v této fázi je příprava vhodného hardwaru a softwaru, který je následně ověřen a certifikován příslušnými úředníky. Posledním krokem v první fázi je vygenerování čísel VIT (*Vote Identification Tokes*). Dle autorů druhá fáze obsahuje instalaci HW a SW v příslušných volebních okrscích a následné spuštění samotného hlasování, kde každý volič po odhlasování obdrží potvrzení o odevzdání hlasu. Poslední fáze „*Counting and verification phase*“nastává po uplynutí předem stanovené doby určené k hlasování. V této fázi

dochází ke sčítání a ověřování odevzdaných hlasů a zveřejnění blockchainu ABVS, a to z toho důvodu, aby voliči mohli vyhledat a ověřit své hlasy. Pokud by došlo k nesrovnalostem, mohou voliči nahlásit chybu, která bude ověřena oproti vydanému potvrzení o hlasování.

V případě [34] autoři představují systém elektronického hlasování, který stejně obdobně jako předchozí řešení, prochází třemi fázemi s tím rozdíle, že zde má každá fáze ještě dvě až tři pod fáze. Autoři tyto fáze nazvali jako „*Pre-voting phase, Voting phase, Post-voting phase*“. První fáze „*Pre-voting phase*“ obsahuje dvě další pod fáze. První z těchto pod fází se zabývá procesem schvalování kandidátů způsobilých na určité pozice ve volbách. Cílem je získání seznamu kandidátů, kteří vlastní několik asymetrických klíčů sloužících k identifikaci a ověření kandidáta. Druhá pod fáze je zaměřena na schvalování voličů, která, jak uvádějí autoři, musí být zcela digitální vzhledem k možnému velkému počtu voličů. Druhá fáze je dle autorů rozdělena na tři pod fáze zabývající se postupně ověřením voliče, samotným hlasováním a předáním a potvrzením hlasování. Těchto pod fází je dosaženo pomocí operací nad voličovou peněženkou v blockchainu, která je v tomto systému elektronických voleb nutností. Třetí fáze obsahuje také tři pod fáze. Těmi jsou sčítání odevzdaných hlasů, výsledek hlasování a auditování. Dle autorů je fáze sčítání složitější než všechny fáze předchozí. Jeden z důvodů je ten, že aby byla transakce platná musí pocházet od oprávněného voliče a končit na adrese registrovaného kandidáta.

V [43] autoři využívají pro systém elektronického hlasování pět fází. V první fázi nazvané „*Registering*“ je každý účastník, v tomto případě volič, kandidát a další entita nazvaná „*Mixer“*, povinen podat žádost o registraci k vrcholové entitě nazvané „*Supervisor*“. Pokud tak neučiní nebude mu v systému poskytnuta relevantní funkce. Druhá fáze je autory nazvána „*Confusing Voter's Identity*“. V této fázi dochází k anonymizaci voliče. Toho je dosaženo pomocí dvou bitcoinových adres pro každého voliče, entity „*Mixer“*, která provádí mix Bitcoinů a jejich převod z původní na novou adresu bez zanechání stopy. Třetí fáze „*Generating ballots*“ slouží k vygenerování hlasovacích lístků, kdy každý volič pomocí veřejného klíče supervisora zašifruje informace o kandidátovi. Ve čtvrté fázi „*Constructing voting transaction*“ dochází k samotnému odevzdávání hlasovacích lístků. Autoři postup v této fázi popisují tak, že každý volič použije skript v protokolu Bitcoinu k vytvoření hlasovací transakce. Poslední, pátá fáze „*Collecting ballots*“ slouží k sčítání odevzdaných hlasovacích lístků. Supervisor prohledá transakce v blockchainu podle anonymního seznamu voličů, dešifruje hlasovací lístky pomocí svého soukromého klíče a spočítá je. Hlasování je úspěšné, pokud existuje kandidát, který před vypršením časového limitu získal dostatek hlasů.

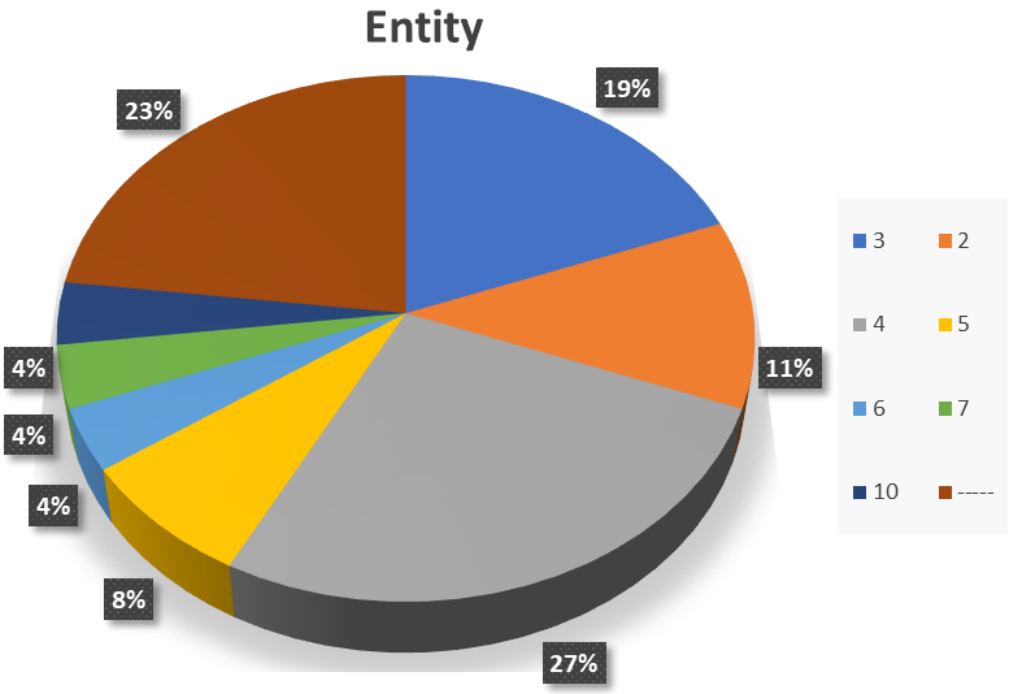
Autoři [47] pro své řešení elektronických voleb zavedli pět fází. První fází je fáze nazvaná „*Initialization phase*“, ve které entita „*Election Authority (EA)*“ inicializuje nové volby, poskytuje potřebné informace, jako je název volebního lístku, čas pro každou fázi, seznam kandidátů atd., které nasadily novou smlouvu na blockchain. EA dále nacení hlasovací lístek částkou 2 ETH[10], tuto cenu později zaplatí volič při provedení transakce hlasování. Druhou fázi autoři nazvali „*Registration phase*“, ve které se občané zaregistrují v nejbližší volební místnosti a ověří svoji totožnost. Poté jim je vygenerován účet v hlasovacím systému a mohou se zúčastnit voleb. Volič, který byl v dřívějších volbách zaregistrován a vlastní účet, tak se již nemusí registrovat. Ve třetí fáze „*Voting phase*“ se voliči přihlásí do systému pomocí vygenerovaného účtu, odevzdají hlas a poté je jim systémem zasláno potvrzení o hlasování, které použijí v další fázi k ověření zaznamenání jejich hlasování. Čtvrtá fáze nazvaná autory „*Result announcement*“ slouží po skončení hlasování k sečtení výsledků pomocí chytré smlouvy blockchainu a jejich následného zveřejnění. Zde voliči mohou zkontrolovat, zda byl jejich hlas správně započítán a zaznamenán do blockchainu. Poslední fázi „*Public audit phase*“ autoři využívají k provedení veřejného auditu voleb. Zde je zveřejněn obsah chytrých smluv, seznamy blockchainových adres a počet voličů. Zveřejněním těchto informací autoři zajišťují transparentnost voleb.

V případě [45] autoři zavedli ve svém systému šest fází elektronických voleb. Těmi jsou „*Smart Contract Verification, System Setup, Voter Preparation and Registration, Ballot Casting, Ballot Tallying, and Opening and Election Auditing*“. Jak autoři dále uvádějí, těchto šest fází se provádí chronologicky a spouští se autonomně pomocí chytré smlouvy. Fáze „*Smart Contract Verification, System Setup*“ je nutné v této posloupnosti provést pouze jednou, to znamená, že dvojice veřejných a tajných klíčů voličů a správců voleb lze použít v dalších volbách. Pro představu fungování jednotlivých fází voleb dávají autoři příklad voliče Alici, která je legitimní voličkou. Ta potřebuje se systémem komunikovat pouze ve dvou fázích, tou první je „*Voter Preparation and Registration”*, kde požádá o autorizaci a připraví hlasovací lístek. Tou druhou je fáze „*Ballot Casting*“, ve které Alice odevzdá hlas do blockchainu. Po skončení fáze „*Ballot Casting*“, sečte inteligentní smlouva hlasovací lístky a zveřejní informace. Alice v této další fázi může pouze zkontrolovat svou registraci a odevzdaný hlas. Autoři tohoto systému se rozhodli v poslední fázi využít pro rozhodnutí o správnosti voleb vybranou skupinu auditorů, a to z důvodu toho, že ne všichni voliči jsou technicky zdatní.

[10] ETH je zkratka měny systému ETHEREUM

6.6 Entity

Dalším vybraným atributem v porovnávání jednotlivých řešení voleb založených na technologii blockchain jsou tzv. entity neboli objekty hrající v daném systému určitou roli. Ne vždy se jedná pouze o osoby a instituce, ale také o HW, SW, procesy, JavaScript atd. Procento zkoumaných článků, které neuvádějí entity je v tomto případě rovno dvaceti třem procentům, tedy šesti zkoumaným článkům. Rozpětí v počtu entit je celkem velké a nejčastěji je tento počet stanoven na tři a čtyři entity viz Graf 7. V následujících příkladech budou zmíněny články s největším procentuálním zastoupením entit a články s nejmenším a největším počtem entit.

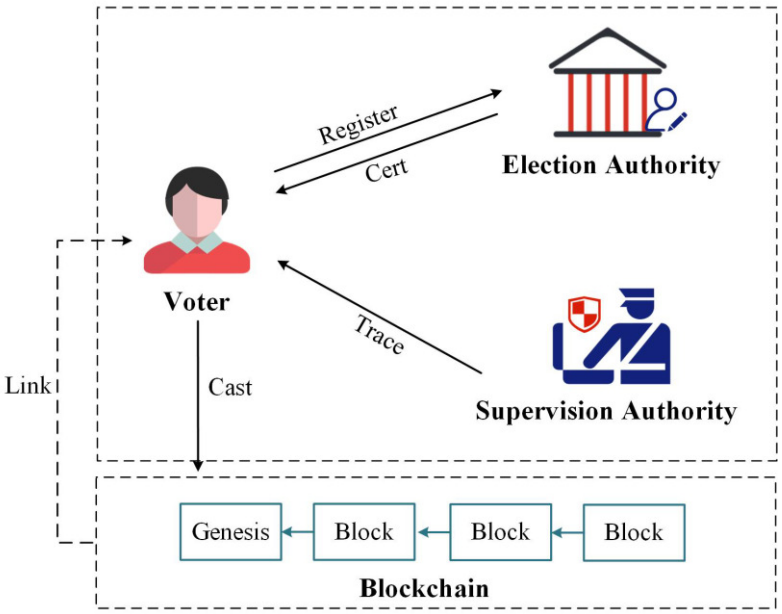


Graf 7 – Počet navržených participujících entit

Zdroj: Vlastní zpracování

Autoři [40] ve svém pojetí voleb založených na blockchainu využívají čtyři entity. Těmi jsou „*Election authority (EA), Supervision authority (SA), Voters, Smart contracts (SC)*“. Vztahy mezi těmito autoritami jsou znázorněny viz Obrázek 10. Úkolem *EA* je samotná organizace voleb a nahrání parametrů veřejných voleb na blockchain. Dále je tato entita zodpovědná za certifikaci a správu voličů, kterým vydává certifikáty a udržuje seznam způsobilých voličů. Entita *SA* má za úkol vysledovat a odhalit identitu voličů, kteří se v systému nechovají dle nastavených pravidel, dále odhalit vícenásobné hlasování a nelegální hlasovací lístky. Entita volič („*Voter*“) je v systému oprávněna pouze odevzdat hlasovací lístek, a to pod podmínkou, že se před hlasováním zaregistrovala u *EA*. Poslední entitou je entita *SC*, která

v systému shromažďuje zašifrované volební lístky, je schopna jejich ověření a propojitelnosti. Dále vyhodnocuje platné hlasovací lísky a zveřejňuje výsledky hlasování.



Obrázek 10 – Vztah jednotlivých entit

Zdroj: [40]

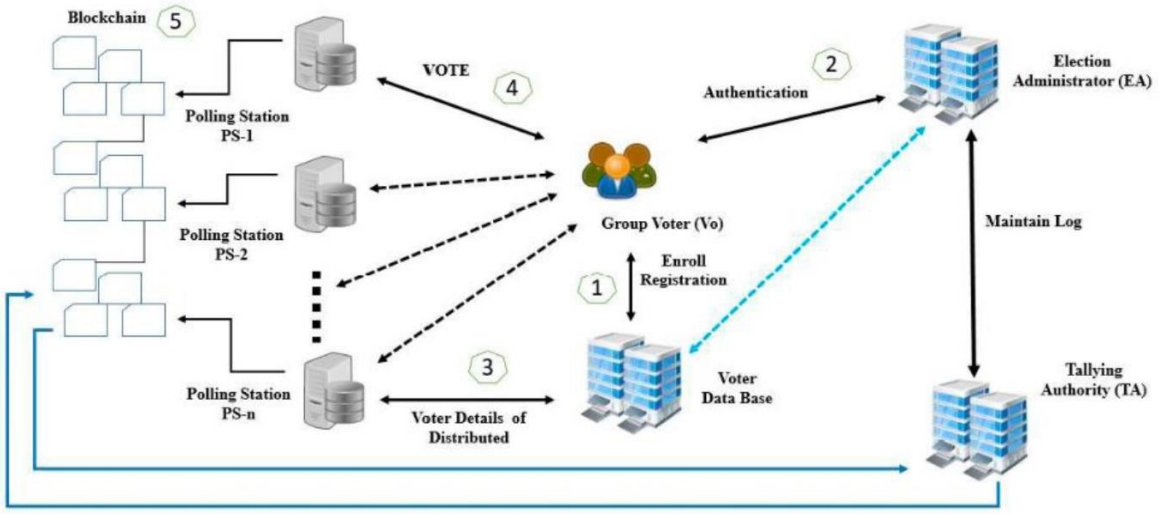
V případě [49] se autoři stejně jako v předchozím článku opírají o čtyři entity nazvanými „*Manage servers (MS), Blockchain network, Users (voters), Blockchain contract (smart contract)*“. Entita „*Blockchain network*“ je navržená blockchainová síť skládající se z několika blockchainů, které pracují vedle sebe. Díky této struktuře jsou autoři schopni provádět paralelní operace, což zlepšuje celkový výkon a škálovatelnost celého systému. K ukládání informací jednotlivých uzlů a registraci uživatelů slouží tzv. nižší řetězce. Horní řetězce slouží k ukládání blockchainových stavů, poté co se zvolení voliči úspěšně dohodnou na transakcích. Funkce entity *MS* je ukládání informací o uzlu v nižší blockchainové síti a jejich publikací ve vyšší blockchainové síti. Druhou funkcí je poskytování certifikátů uzlům, což umožňuje jejich autentizaci a zahrnuje přihlašovací údaje uživatele do systému. Další entitou v systému je entita „*Users*“, pomocí které autoři označují voliče. Ti mají dvě základní role. Tou první jsou to samotní voliči, kteří k tomu, aby mohli volit, musí obdržet digitální token. Druhou rolí je to, že tvoří volební komisi. Poslední entitou, kterou autoři implementovali je „*Blockchain contract*“. Jedná se o samostatně spuštěné úryvky kódu (funkce), které umožňují sledování transakcí v nejvyšší blockchainové vrstvě „*Blockchain network*“. Dle autorů je tedy možné, aby každý uzel provozoval „*Blockchain contract*“ nezávisle, což vede k flexibilitě celého systému.

Čtyři entity ve svém pojetí elektronických voleb založených na blockchainu využívají také autoři [52]. Tuto čtveřici tvoří „*Election Committee (EC), Certification Authority (CA), Blockchain Voting Platform, Voters*“. Entita *EC* je organizátorem voleb, který působí jako iniciátor hlasování, je zodpovědná za výpočet konečného výsledku voleb a jeho zveřejnění. Druhou entitou v pořadí je entita *CA* jejíž funkcí je vydávání certifikátů účastníkům, kteří chtějí tento certifikát získat. Třetí v pořadí je „*Blockchain Voting Platform*“ fungující jako veřejná nástěnka uchovávající oznámení a hlasovací lístky všech voličů. Poslední entitou v tomto systému jsou voliči, kteří si musí požádat o vydání certifikátu entitu *CA* a odevzdat své hlasy pomocí platformy blockchain.

Pouze dvě entity zvolili ve svém systému autoři [46]. Entita, která je zodpovědná za nastavení voleb, nastavení chytrých smluv, identifikaci oprávněných voličů pomocí jejich veřejných klíčů, zveřejnění seznamu veřejných klíčů a kandidátů se v tomto systému nazývá „*Election administrator*“. Druhou a zároveň poslední entitou jsou samotní oprávnění voliči vlastnící pár tajných soukromých klíčů. Tato entita je autory pojmenována jako „*Voter*“.

Oproti minimalistickému pojetí počtu entit v předešlém případě, se autoři [48] rozhodli pro entit sedm. Jak autoři uvádějí, v základu schéma e-voleb obsahuje čtyři entity, kterými jsou „*Registration server (RS), Election Administrator (EA), Telling Authority (TA), Voters (V)*“. V případě *RS* se jedná o důvěryhodnou entitu, která má pravomoc a odpovědnost zapojit všechny oprávněné voliče do systému a přidělit jim ověřovací parametry. Entita *EA* je zodpovědná za řízení voleb. Do tohoto řízení spadá inicializace, průběh, ukončení volebního procesu, nastavení parametrů voleb, autentizace voličů, sestavení hlasovacích lístků ve spolupráci s entitou *TA*. Co se týče rolí entity TA, těmi jsou především dešifrování odevzdaných hlasovacích lístků, výpočet konečného výsledku voleb, zveřejnění hodnot, dle kterých mohou voliči ověřit své hlasování. Poslední, dle autorů základní entitou jsou „*Voters*“. Každý volič v autory navrženém systému vlastní účet, který mu byl zřízen EA. Tato entita má v systému pouze právo hlasovat. Dále autoři uvádějí, že existuje i několik dalších komponent, které jsou v systému důležité, a proto se je rozhodli zařadit mezi entity, které se podílí na průběhu voleb. Těmito entitami jsou „*Voter ID Card, Polling Officials, Public Bulletin Board (BB)*“. *Voter ID Card* je entita, kterou volič získá v registračním centru. Jedná se o kartu obsahující ID voliče, jeho biometrické údaje a pár veřejného a soukromého klíče. Tato karta je digitálně podepsána volebním orgánem a propojuje identitu voliče s biometrickou šablonou. Entita nazývající se *Polling Officials* jsou fyzičtí úředníci zapojení do procesu e-voleb. Poslední entitou je *BB*, což je veřejná nástěnka na webové stránce zobrazující důležité parametry voleb. Hlavní předností

této entity je dle autorů to, že data, která jsou prezentována na *BB* nelze smazat. Schéma komunikace mezi jednotlivými entitami viz Obrázek 11.



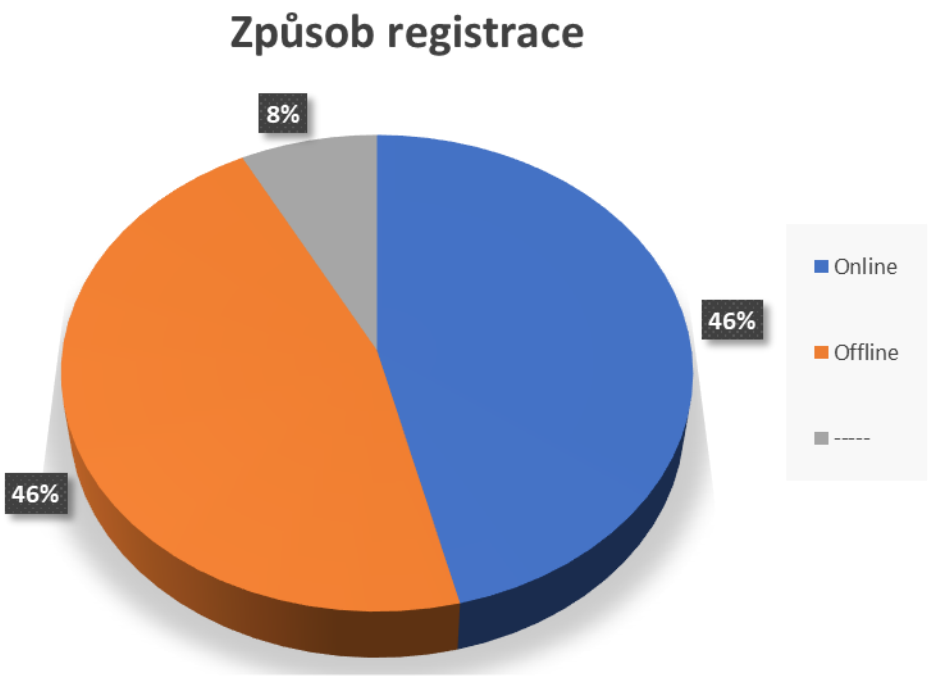
Obrázek 11 – Schéma systému entit dle [48]

Zdroj: [48]

Systém prezentovaný autory v [53] je systém s největším počtem entit. V tomto návrhu jich autoři vytvořili celkem deset. První entitou jsou „*Voters*“, což je skupina lidí, kteří jsou způsobilí a oprávněni volit. Entita „*Candidates*“ je podskupina voličů, kteří se ucházejí o volební post, jak je uvedeno na hlasovacím lístku volební komisí. Další, v pořadí třetí entitou je „*Electoral Commission (EC)*“, která je nezávislým orgánem zmocněným k provádění voleb a vyhlašování jejich výsledků. V případě entity „*Political Parties*“ se jedná o různé politické strany, které jsou zastoupeny ve volbách. „*Local Authority*“ je entita představující místní volební obvod, ve kterém se mají konat volby. Entitou „*Blockchain Network*“ je rozuměna nedůvěryhodná síť peer – to – peer, která je schopna uchovávat záznamy, jež jsou přístupné všem zúčastněným stranám. Sedmou entitou jsou „*Blockchains Admins*“. Tato entita představuje systémové administrátory a členy EC. „*Mining Nodes*“ je entitou představující sadu uzlů, které jsou zodpovědné za přidávání záznamů o hlasování do veřejné knihy. Předposlední entita „*Non-mining Nodes*“ je sada uzlů, jejichž úlohou je sledování a ověřování všech volebních záznamů a transakcí. Poslední, desátou entitou je „*Smart contracts*“, což je softwarový kód řídící volební proces a provádějící tabelaci a sčítání hlasů.

6.7 Registrace

Aby se občané mohli zúčastnit elektronických voleb, je nutné jejich zaregistrování před samotnou volbou u příslušné autority. Registrace mohou být online či offline. Při offline registraci je většinou prováděna kontrolou dokladů a uložení jejich identifikátorů do systému, někdy jsou ukládány i biometrické údaje voliče, kde se jedná především o otisky prstů. Jelikož je tento proces pro elektronické volby velmi důležitý, je dalším zkoumaným atributem právě samotná registrace voliče před volbami. V rámci zkoumaných článků bylo vyhodnoceno, že osm procent zkoumaných článků neřešilo registraci voliče, čtyřicet šest procent využívá offline registraci na předem stanovených místech a zbylých čtyřicet šest procent využívá v různé formě online registraci.



Graf 8 – Způsoby registrace k volbám

Zdroj: Vlastní zpracování

V případě [31] autoři využívají offline registraci. Ta spočívá ve dvou fázích. Tou první je, že v přípravné fázi voleb jsou pro voliče vygenerovány příslušnou důvěryhodnou autoritou „*Vote Identification Tokens (VIT)*“, které slouží k identifikaci a ověření hlasů v pozdější fázi. Tyto *VIT* jsou po jednom vytištěny a uloženy do obálek, které jsou přiděleny a distribuovány mezi volební místnosti. Ve druhé fázi se voliči dostaví do volební místnosti, kde se identifikují u pověřeného úředníka (v případě Polska, kde byl tento systém vyzkoušen, se voliči identifikovali předložením průkazu totožnosti a podpisem do registru) a náhodně si vyberou

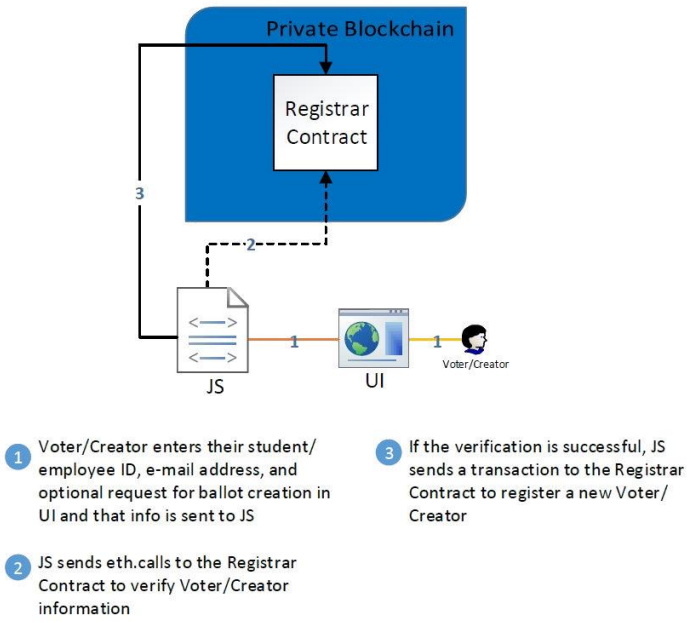
obálku s číslem *VIT*, které použijí v další fázi pro potvrzení při odevzdání hlasovacího lístku do blockchainu.

Pro využití offline registrace se rozhodli také autoři [47]. Ti zvolili takový systém registrace, kde se každý občan, který se chce zúčastnit vole, musí dostavit do nejbližší volební místnosti. Zde předloží svůj občanský průkaz nebo cestovní pas entitě „*Registration authority (RA)*“ k ověření totožnosti oproti databázi občanů. Po úspěšném ověření voliče RA pro něj vygeneruje účet v hlasovacím systému. Volič, který se již zúčastnil předešlých voleb a má systémový účet se již registrovat nemusí. Po obdržení účtu se musí volič do účtu přihlásit a nastavit si blockchainový účet tak, aby mohl hlasovat. Tento blockchainový účet nelze při jeho ztrátě obnovit. Voliči je na tento účet přidělen paušál v měně ETH, který slouží k potvrzení provedení transakce, kterou je odevzdání hlasovacího lístku na blockchain.

Autoři [51] ve svém návrhu systému elektronických voleb využívají offline registraci voličů, která je spojena s poskytnutím biometrických údajů, konkrétně otisku prstů. Registrace voliče probíhá v přípravné části voleb, a to konkrétně ve fázi „*Voter registration*“. Dle návrhu autorů tato fáze může probíhat celý rok před volbami. Proces registrace probíhá tím způsobem, že se volič dostaví do registračního centr, kde předloží úředníkovi průkaz potvrzující jeho totožnost (občanský průkaz, cestovní pas, voličský průkaz, …). V dalším kroku si volič nechá sejmou otisk prstu a za pomocí šifrovacího algoritmu *Fuzzy Vault* dojde k navázání náhodně vygenerovaného klíče do dat otisku prstu. Automat v registračním centru vygeneruje dvě náhodná čísla, ri1 a ri2. Číslo ri1 funguje jako jeden z tajných klíčů a je nezávislé na biometrii, tudíž ho lze změnit či upravit. Voliči je vystavena čipová karta, na které je uloženo číslo ri2 a zašifrovaná biometrická data. Tato karta bude vyžadována při autentizaci voliče do systému hlasování.

Opačný přístup k registraci voličů oproti předcházejícím příkladům zvolili autoři [29]. Ti ve svém systému využívají online registraci. Ta spočívá v tom, že systém *Bronco Vote* je vytvořen pro univerzitní prostředí, ve kterém každý potencionální volič disponuje jednoznačným identifikačním číslem a e-mailem s příslušnou doménou. Pokud volič ve webovém rozhraní vyplní svoje ID číslo a e-mail, jsou tyto informace odeslány do JavaScript aplikace *VotingApp.js*, která zavolá *Registrator.sol*, což je chytrá smlouva napsaná v jazyce Solidity, a ověří, zda doména e-mailu je v tzv. *whitelist* a zda se daný uživatel již dříve nezaregistroval. Pokud volič touto kontrolou projde, jsou do *Registrator.sol* uloženy jeho informace v podobě čísla ID, e-mailu a přidělené adresy Ethereum. Tento proces je zobrazen

viz Obrázek 12. Propojením adresy Ethereum a e-mailu je dosaženo toho, aby se volič nemohl dvakrát zaregistrovat.



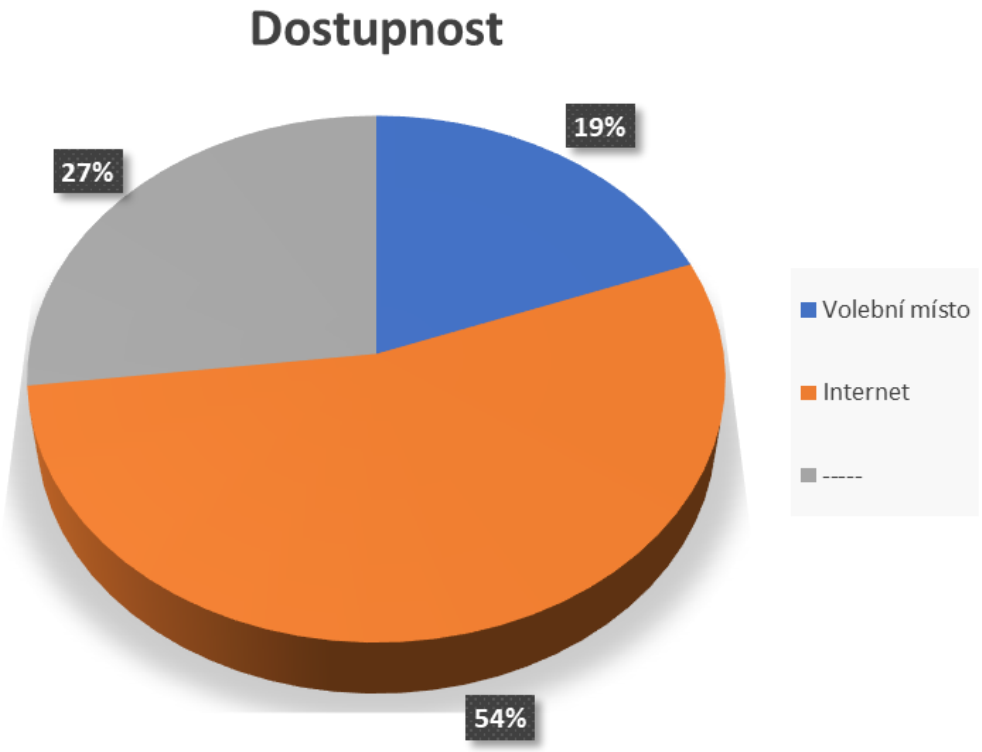
Obrázek 12 – Proces registrace voliče v [29]

Zdroj: [29]

Online registraci využili ve svém systému i autoři [44]. Online registrace probíhá ve třech fázích. V té první si uživatel zobrazí webové rozhraní systému registrace a je vyzván k výběru uživatelského jména a hesla, dále k vyplnění osobního profilu včetně jména, data narození, identifikačního čísla (číslo občanského průkazu, řidičského průkazu, …), e-mailové adresy, telefonního čísla atd. Dále je uživatel vyzván k pořízení snímku obličeje. Díky tomuto snímku je zajištěno, že každý uživatel bude mít v systému pouze jeden jedinečný účet. V druhé fázi je na poskytnutou e-mailovou adresu zasláno jednorázové heslo OTP („*One-Time Password*“) k ověření a jsou vygenerovány vektory rysů obličeje. Systém poté vytvoří nový účet asociovaný s uživatelským jménem a heslem pro uživatele jako voliče Vi a vygeneruje token Ti, kde i je pořadí voliče v systému. Ve třetí fázi registrace systém uloží uživatelské jméno a heslo v databázi, která vrací nové identifikační číslo voliče vIDi. Další citlivé informace o voliči, jako je jméno, telefonní číslo, vektory rysů obličeje jsou zašifrovány pomocí tokenu Ti, který byl vygenerován v předchozí fázi. Takto zašifrované informace jsou spolu s vIDi uloženy v blockchainu.

6.8 Dostupnost

Tento atribut představuje v systému voleb založených na technologii blockchain místo, na kterém mají voliči přístup do systému a kde mohou hlasovat. Mohlo by se zdát, že tento atribut je irelevantní, a to z důvodu toho, že když se mluví o e-votingu založeném na blockchainu, představa je jasná. Přístup do systému a samotné hlasování z jakéhokoli místa s dostupným internetovým připojením. Opak je ale pravdou. Ne všechny zkoumané návrhy e-votingu počítají s přístupem odkudkoliv. Namísto toho je přístup soustředěn do volebních center. Těchto případů je ve zkoumaných článcích devatenáct procent. Případů, kdy se článek nezmiňuje o dostupnosti je u tohoto atribut dvacet sedm procent. Zbylých padesát čtyři procent zkoumaných článků navrhuje přístup k hlasování na jakémkoli místě s dostupným internetem. Graficky je tento stav vyjádřen viz Graf 9.



Graf 9 – Dostupnost systémů elektronický voleb

Zdroj: Vlastní zpracování

V případě [48] autoři navrhují systém elektronického hlasování, ve kterém se volič, který chce hlasovat, musí dostavit do kterékoliv volební místnosti určené k hlasování. V této volební místnosti volič předloží svůj voličský průkaz, který mu byl vydán při registraci, volebním úředníkům. Ti ověří, že předložený voličský průkaz skutečně patří danému voliči. Toto ověření je provedeno na základě biometrických dat, která byla na voličský průkaz uložena

v předchozí fázi. Po ověření může volič odevzdat svůj hlas do blockchainu pomocí chytré smlouvy a voličského průkazu.

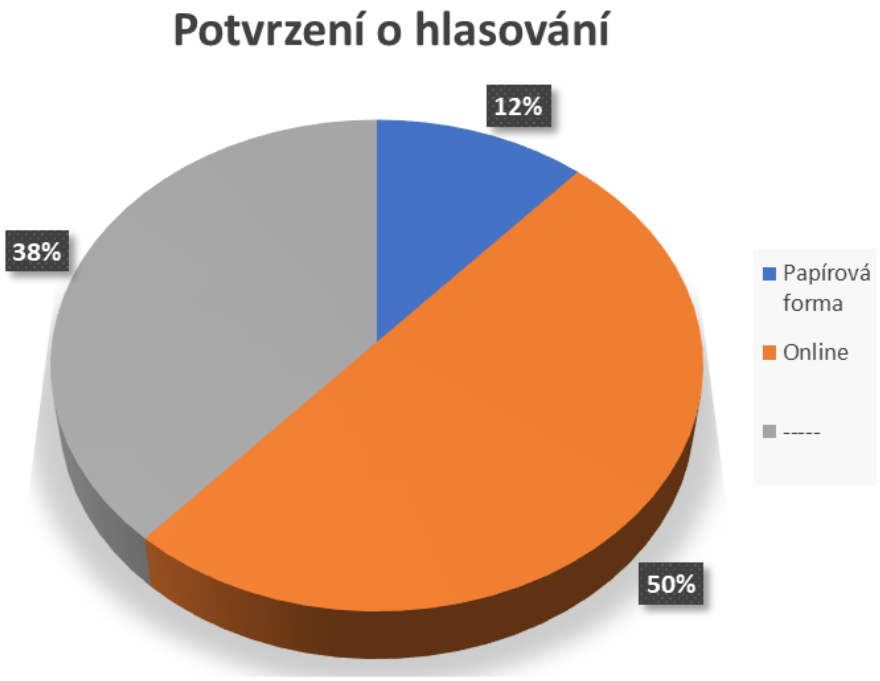
Obdobně jako autoři v předešlém případě, tak se také autoři [51] rozhodli pro dostupnost volebního systému pouze na místech k tomu určených. Volič se v den voleb dostaví do volební místnosti, kde předloží čipovou kartu obsahující data k jeho ověření vydanou ve fázi registrace, své voličské číslo „VOTER_ID“, které bylo vypočítáno rovněž ve fázi registrace. Dále také ověří svoji totožnost a způsobilost volit pomocí otisku prstu, který je zkontrolován oproti hashi biometrických dat uložených na čipové kartě. Volič po úspěšném ověření může přistoupit k samotnému hlasování.

Oproti předchozím příkladům dostupnosti systému elektronických voleb autoři [34] zvolili opačný přístup, a to takový, že volič má dostupný systém hlasování kdekoliv, kde je počítač s přístupem k internetu. Autoři navrhli systém elektronických voleb dostupný přes webové rozhraní. Toto webové rozhraní umožňuje dva způsoby hlasování, a to s vlastní peněženkou, nebo bez peněženky. V případě hlasování bez peněženky, může volič hlasovat, aniž by měl na daném PC nainstalovanou peněženku a pro hlasování stačí pouze samotné webové rozhraní. Pokud volič vlastní peněženku, která je kompatibilní s OAP („*Open Assets Protocol*“) a má ji na daném PC nainstalovanou, může ji využít k hlasování přes stejné webové rozhraní.

Pro stejný způsob dostupnosti hlasovacího systému, jako autoři [34], se rozhodli také autoři [53]. Dle jejich návrhu se voliči k hlasovací aplikaci připojí prostřednictvím svého webového prohlížeče bez nutnosti instalace jakéhokoliv dalšího klientského softwaru. Pro přihlášení voliče je využíváno dvoufázové ověření. V první fázi zadá volič zvolené uživatelské jméno a heslo. Ve druhé fázi je voliči na zvolené mobilní telefonní číslo, které zadal ve fázi registrace, zasláno OTP („*One Time Password*“). Poté, co volič zadá zaslané OTP do webové aplikace, je druhá fáze ověření dokončena. Webové rozhraní systému je rozděleno na administrativní a hlasovací. Administrativní uživatelské rozhraní slouží pro přístup ke kódování a nasazení chytrých smluv. Uživatelské rozhraní voličů poskytuje rozhraní pro interakci s chytrou smlouvou, která prezentuje hlasovací lístky pro jednotlivé kandidáty. Samotné webové rozhraní je dle návrhu autorů chráněno pomocí asymetrické kryptografie, konkrétně SSL certifikáty. Ochrana a bezpečnost samotných zařízení je v zodpovědnosti voličů.

6.9 Potvrzení o hlasování

Oproti tradičním volbám ve formě papírových hlasovacích lístků, je voliči v systému elektronických voleb založených na systému blockchain vydáváno potvrzení o hlasování. To slouží voliči k ověření stavu jeho odevzdaného hlasovacího lístku. Pokud ve zkoumaných článcích autoři popisovali vystavení tohoto potvrzení, jednalo se o dvě formy. Tou první bylo potvrzení v papírové podobě s potřebnými údaji o hlasovacím lístku. Druhou formou bylo elektronické potvrzení, a to především ve formě ID transakce. I u tohoto atributy se vyskytly články, ve kterých se autoři o vystavení potvrzení o hlasování vůbec nezmiňovali. Těchto článků bylo třicet osm procent, padesát procent článků preferovalo elektronické potvrzení a pouze dvanáct procent článků řešilo potvrzení o hlasování papírovou formou. Tato tvrzení jsou doložena graficky (viz Graf 10.)



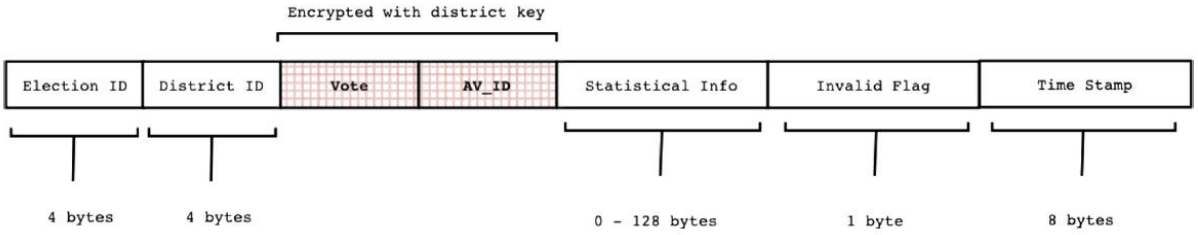
Graf 10 – Forma potvrzení o hlasování

Zdroj: Vlastní zpracování

Autoři [31] ve svém navrhovaném systému elektronických voleb zvolili, v případě zkoumaných článků, ojedinělý způsob vydávání potvrzení o hlasování. Každý volič v systému ABVS (*Auditable Blockchain Voting System*) obdrží po odevzdání a potvrzení hlasu VVPAT (*Voter-Verified Paper Audit Trails)*. Jedná se o papírovou formu potvrzení o hlasování, která je namapována na odpovídající blok v blockchainu prostřednictvím VIT (*Voter Identification*

Token). Po obdržení VVPAT volič toto potvrzení vhazuje do urny a odchází z volební místnosti pouze s vygenerovaným VIT.

V případě [37] se autoři, oproti předchozímu příkladu, rozhodli vydávat ve svém systému elektronických voleb online potvrzení ve formě vygenerované hodnoty AV-ID. Toto AV-ID je obsaženo v hlasovacím lístku, který je uložen v „*Cast Votes Register*“ viz Obrázek 13.



Obrázek 13 – Struktura hlasovacího lístku v systému TeV

Zdroj: [37]

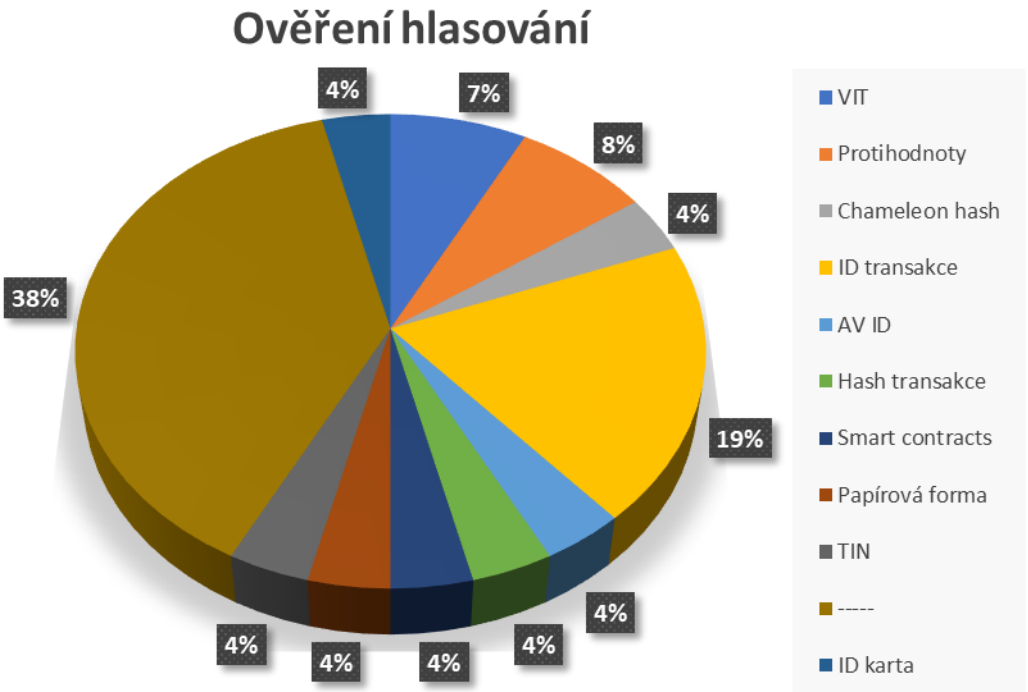
Pro online potvrzení o hlasování se ve svém návrhu systému elektronických voleb založených na technologii blockchain rozhodli také autoři [50]. Potvrzení je voliči vystaveno, jakmile je transakce zaznamenána do řetězce blockchainu. Odpovídající voličský token je přidán do seznamu použitých tokenů a následné ID transakce je voliči zasláno pomocí PUSH soketu jako potvrzení o hlasování.

Obdobně jako u dvou předchozích příkladů, tak se také autoři [42] rozhodli pro využití online potvrzení o hlasování. V tomto případě autoři zvolili postup vydávání potvrzení o hlasování v podobě, kdy je hlasovací lístek po podepsání, nahrání a zašifrování odeslán na anonymizační proxy server. Z tohoto serveru je odeslán na blockchain. Hash této transakce a odkaz na průzkumníka blockchainu je odeslán zpět voliči pro potřeby v další fázi voleb.

Pro online ověření se rozhodli také autoři v případě [38], kdy je systémem vygenerováno ID transakce, které může být voliči dále použito pro ověření hlasování. Postup vygenerování potvrzení je takový, že v průběhu voleb, každý volič převede pomocí své peněženky token do peněženky kandidáta. Tato transakce převedení tokenu představuje odevzdání hlasovacího lístku danému kandidátovi. Následně volič obdrží ID této transakce, které je možné využít v další fázi voleb, a to pro ověření správnosti odevzdání a započítání hlasu každého voliče.

6.10 Ověření hlasování

V systému elektronických voleb může volič zpětně zkontrolovat svůj odevzdaný hlasovací lístek, a to díky předchozímu atributu potvrzení o hlasování. Tato kontrola je zaměřena na to, zda voličův lístek byl skutečně odevzdán, zda byl odevzdán ve prospěch zamýšleného kandidáta a zda byl započítán do výsledku voleb. Kontrola dle zkoumaných článků probíhá v poslední fázi voleb, a to ve fázi sčítání a zveřejňování výsledků. Pro tyto potřeby zkoumané návrhy elektronických voleb využívají různá řešení. Jedná se především o ověřování online pomocí vygenerovaných potvrzení o odevzdání lístku ve fázi hlasování. Nacházejí se zde také články, ve kterých se autoři nezmiňují o ověřitelnosti hlasování. Těchto článků je třicet osm procent. Ve zbylých šedesáti dvou případech se jedná o různě vygenerované hodnoty, kde tou nejčastější hodnotou je ID transakce. Jednotlivé hodnoty a jejich procentuální zastoupení je znázorněno graficky viz Graf 11.



Graf 11– Způsob ověření hlasování

Zdroj: Vlastní zpracování

Ověření hlasování v [31] autoři rozdělili na dvě fáze. V té první volební úředníci deaktivují volební systém v jednotlivých volebních místnostech a otevřou obálky s nepoužitými VIT. Vytvoří seznamy těchto nepoužitých VIT a zašlou je centrální volební autoritě. Od tohoto okamžiku může nastat druhá fáze, kdy si každý volič, který stále vlastní

svůj VIT, může zkontrolovat nejenom svůj odevzdaný hlas, ale i prozkoumat celý blockchain. Centrální autorita ověřuje a porovnává výsledky hlasování pomocí VIT a voliči odevzdaných papírových potvrzení o hlasování tzv. VVPAT. Dále tato autorita kontroluje platnost VIT a také to, zda pocházejí z volebních místností, ke kterým byla přiřazena.

V případě autorů [48] je ověření prováděno pomocí předem vydané ID karty obsahující biometrické údaje, které slouží k autentizaci pro účely hlasování a ověřování. Dle autorů může tuto kartu použít každý volič k vyhledání transakce s příslušným ID karty na blockchainu. Nutno dodat, že tento přístup je možný pouze v oficiálních volebních místnostech, nebo na určených úřadech. Voliči tak mohou vidět své hlasy na blockchainu a ověřit, zda jsou jejich hlasy zahrnuty a správně započítány.

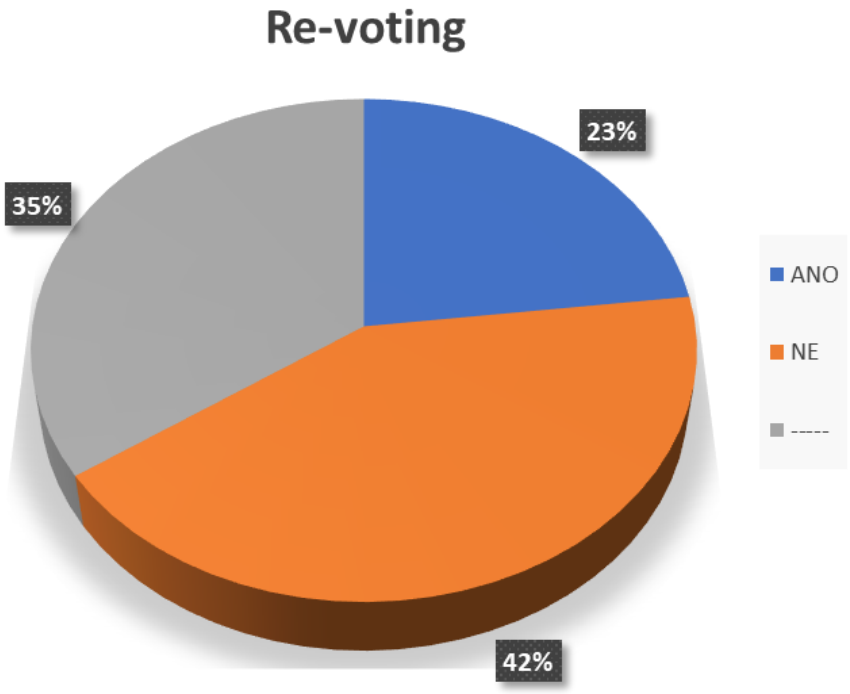
Autoři [47] v navrhovaném systému elektronických voleb provádějí ověření hlasování pomocí ID transakce. Toto ID transakce volič získá tím způsobem, že ve fázi hlasování odešle svůj hlas na blockchain. Systém mu nazpět zašle ID transakce. Po sečtení hlasovacích lístků je výsledek zveřejněn a voliči mohou použít své ID transakce k ověření, zda je jejich hlas správně započítán a zaznamenán do blockchainu. Mimo to, jsou zveřejněny i další údaje nutné k veřejnému auditu. Jedná se konkrétně o obsah hlasovacích chytrých smluv, seznam blockchainových adres, bez identifikací voličů, hlasujících pro každého kandidáta a počet občanů, kteří se voleb zúčastnili. Toto vše dle autorů vede k zajištění transparentnosti voleb.

V systému elektronického hlasování nazvaném SEVA („*Smart Electronic Voting Application*“), který autoři popisují v [53] je k ověření hlasování využito opět ID transakce. Autoři ve své práci toto ID nazývají TIN („*Transaktion Identification Number*“) a ve skutečnosti se jedná o číslo účtu Ganache. Poté co je hlasovací lístek odeslán na blockchain, je TIN uloženo do souboru, který je odeslán na mobilní telefon či email voliče. Po skončení hlasování může volič toto TIN využít k ověření odevzdání hlasu. Voliči jsou dostupné pouze informace o tom jakému kandidátovi hlas odevzdal a časové razítko transakce.

V případě [33] autoři k ověření hlasování využívají hodnotu vypočítanou při odevzdání hlasu na blockchain. Tato hodnota je vypočítána pomocí funkce chameleon hash. Dle autorů si může každý volič ověřit , zda byl jeho hlas započítán či nikoli. Tato vlastnost systému zvyšuje samotnou důvěryhodnost a transparentnost sčítání hlasů.

6.11 Re-voting

V klasickém pojetí voleb, kdy volič odevzdává do urny v obálce papírový hlasovací lístek, není povoleno a ani technicky možné opakované hlasování, či změna volby. Naproti tomu v systému elektronických voleb založenách na technologii blockchain tato volba existuje. Ne vždy je toto opakované hlasování realizováno, protože možnost opakovaného hlasování v určitém smyslu zatěžuje samotný systém hlasování a dále skýtá možnosti pro realizaci odevzdávání neplatných hlasovacích lístků. Ve zkoumaných článcích je tato možnost realizována pouze v dvaceti třech procentech článků, dalších třicet pět procent článků se o této možnosti vůbec nezmiňuje. Zbylých čtyřicet dva procent zkoumaných článků možnost realizace opětovného hlasování odmítá. Grafické vyjádření možnosti opakované volby viz Graf 12.



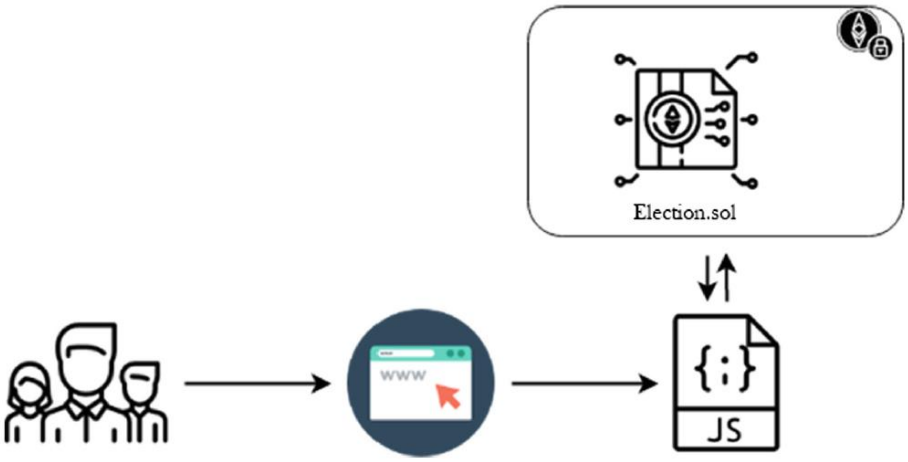
Graf 12 – Možnost opakovaného hlasování

Zdroj: Vlastní zpracování

V případě volebního systému DABSTER [32] autoři umožňují voliči vícenásobné hlasování. Celý proces vícenásobného hlasování funguje tak, že v průběhu fáze hlasování může oprávněný volič hlasovat vícekrát, přičemž se do výsledku hlasování započítává pouze jeho poslední hlas. To znamená, že v konečném sečtení odpovídá maximálně jeden hlas na jednoho voliče.

Obdobně jako u systému DABSTER, tak také autoři volebního systému LOKI Vote [36] umožňují voliči vícenásobné hlasování. Princip je také obdobný jako u systému DABSTER, a to tedy takový, že každý legitimní volič má možnost před koncem hlasovací fáze odevzdat hlasovací lístek vícekrát, ale započítává se vždy jen ten poslední.

Autoři [33] ve svém volebním systému popisují dosažení tzv. „jedinečnosti“, což je vlastnost systému, která zamezuje voliči hlasovat více než jednou. Tohoto zamezení je dosaženo pomocí chytré smlouvy, která je napsána v jazyce Solidity a souboru App.js, který je napsán v JavaScript (schéma viz Obrázek 14). Soubor Election.sol obsahuje mimo jiné funkce k zamezení dvojího hlasování. Pokud se tedy volič rozhodne hlasovat, přihlásí se přes webové rozhraní k systému. Během přihlašování je kontrolováno přes soubor App.js a Election.sol, zda již volič hlasoval. V případě, že již hlasoval, je mu zobrazena webová stránka s informací, že dvojí hlasování není povoleno.



Obrázek 14 – Framework systému Chaincracy

Zdroj: [33]

V případě [52] autoři zamezují dvojímu hlasování pomocí kontroly identifikátoru VID a tokenu s ním spojeným, který volič může odedvzdat v průběhu voleb pouze jednou. Každý token obsahuje dva tagy, první tag je spojovací t_1 a druhý tag je sledovací t_2. Kontrola probíhá nad spojovacím tagem, takže pokud se volič pokusí odevzdat hlas dvakrát, dva spojovací tagy povedou k propojení dvou tokenů se stejným hashem. Systém je tedy schopný přesně lokalizovat původce dvojího hlasování.

Autoři [47] kontrolují vícenásobné hlasování voliče hned dvakrát. Jednou na serveru a podruhé pomocí chytré smluvy při odesílání na blockchain. Dle autorů je tento způsob dostatečný k zamezení vícenásobného odevzdání hlasu.

6.12 BroncoVote

Jedná se o volební systém s použitou technologií blockchain navržený pro univerzitní volby. [29] Je postaven na chytrých smlouvách a blockchainu Ethereum. Díky tomu je schopen administrovat voliče, auditovat volební záznamy, zachovat soukromí voličů a transparentnost hlasování. Využívá několik kryptografických technik, včetně homomorfního šifrování k podpoře soukromí voličů.

Samotná implementace systému je složena z několika základních bloků. [29] Těmito bloky jsou tři chytré smlouvy napsané v programovacím jazyce Solidity Ethereum, dva skripty psané v JavaScriptu a jedna stránka HTML. Pro interakci s tímto systémem je nutné, aby všichni aktéři voleb (administrator, voter, creator) měli ve svém prohlížeči stažený plugin MetaMask nebo na svém PC spuštěný uzel Ethereum. Dále je pro interakci s blockchainem využíván WEB3. Využitím právě MetaMask a WEB3 odpadá potřeba stahování celého blockchainu a jeho následnou synchronizaci, jedinou potřebnou akcí uživatele při registraci je tedy pouze použití hesla k odemčení účtu Ethereum v pluginu MetaMask. Pokud uživatel nevyužije MetaMask, je nucen spustit a synchronizovat uzel Ethereum na svém PC, aby mohl pomocí WEB3 komunikovat se systémem.

Součásti systému – Systém BroncoVote obsahuje několik základních částí, které jsou nutné k zajištění je fungování. Tyto části lze rozdělit na entity, front/back-end části a chytré smlouvy.

a. Entity
    i. administrator – odpovídá za nasazení chytrých smluv *Registrar* a *Creator*. Má právo k povolení či zrušení vytvoření hlasovacího lístku,
    ii. voter – uživatel, který se registruje do systému pomocí e-mailu a ID studenta/zaměstnance,
    iii. creator – volič s povolením vytvářet hlasovací lístky.
b. Front/back-end
    i. VoteUI.html – webová stránka sloužící jako uživatelské rozhraní systému,
    ii. VotingApp.js – JavaScript pomocí které dochází k ověření, šifrování/dešifrování hlasů a uložení informací o hlasování,
    iii. Crypto.js – JavaScript sloužící jako šifrovací server využívající k šifrování a dešifrování systém Paillier.

c. Chytré smlouvy

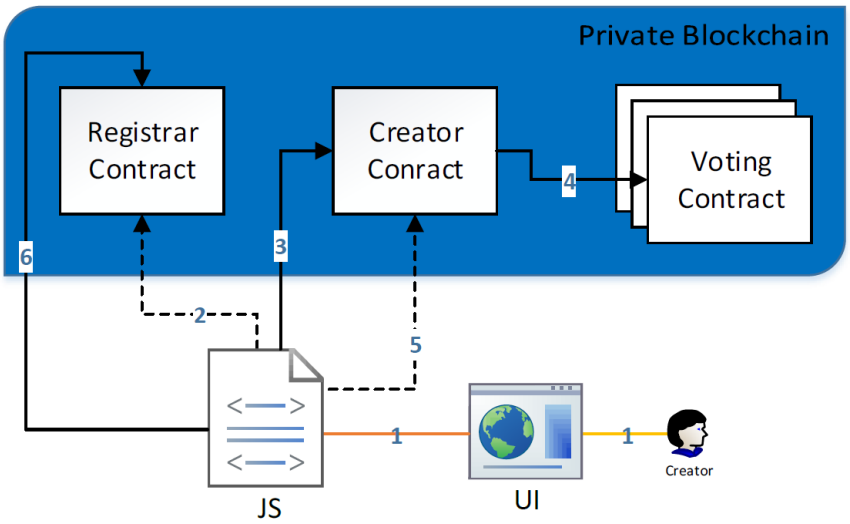
i. Registrar.sol – sleduje všechny entity, volební ID, e-maily a porovnává je oproti seznamu. Vlastníkem této smlouvy je *administrator*,

ii. Creator.sol – jedná se o zdroj pro Voting.sol. Definuje podrobnosti smlouvy o hlasování na základě informací z webového rozhraní. Vlastníkem je *administrator,*

iii. Voting.sol – jedná se o virtuální hlasovací lístek. V této smlouvě je také zahrnuta kontrola o vícenásobném hlasování a časový limit voleb. Vlastníkem je její tvůrce.

Registrace voliče – Registrovat se jako volič může kdokoli s ID studenta/zaměstnance a e-mailem s povolenou doménou. Potencionální volič vyplní své údaje na VoteUI.html, následně jsou tyto informace odeslány do VotingApp.js, který je ověří vůči Registrar.sol. Jestliže dojde k úspěšnému ověření, jsou tyto informace odeslány VotingApp.js do Registrar.sol. Graficky je tento proces znázorněn viz Obrázek 12.

Tvorba lístku – Pokud má uživatel právo k tvorbě hlasovacího lístku, může vytvořit novou chytrou smlouvu o hlasování tím, že zadá potřebné informace přes webovou stránku VoteUI.html. [29] Proces tvorby hlasovacího lístku se odehrává v šesti krocích, které jsou znázorněny viz Obrázek 15.



Obrázek 15 – Proces tvorby hlasovacího lístku

Zdroj: [29]

Popis toho, co se děje v jednotlivých krocích při tvorbě hlasovacího lístku je následující:

Krok 1. Creator zadá informace o hlasovacím lístku přes VoteUI.html, ty jsou poté odeslány do VotingAPP.js,

Krok 2. VotingApp.js pomocí eth.calls ověří Creatora u Registrar Contract,

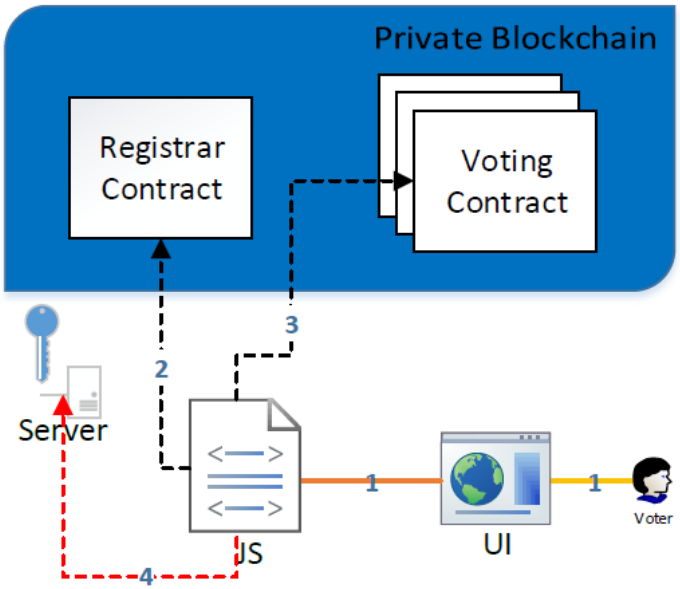
Krok 3. Pokud je Creator úspěšně ověřen, transakce k vytvoření hlasovacího lístku je odeslána do Creator Contract s požadavkem na vytvoření nové smlouvy obsahující informace o hlasovacím lístku,

Krok 4. Creator Contract odešle transakci k vytvoření nové smlouvy o hlasování (Voting Contract),

Krok 5. VotingApp.js pomocí eth.calls odešle požadavek na Creator Contract k získání adresy nové smlouvy o hlasování,

Krok 6. VotingApp.js odešle transakci do Registrar Contract s ID hlasovacího lístku a adresou smlouvy, za účelem registrace nového hlasovacího lístku.

Načtení lístku – Proces nahrání volebního lístku je graficky znázorněn viz Obrázek 16, kde černou tečkovanou čarou jsou vyznačeny eth.calls na blockchain a červenou dotazy na šifrovací server. [29]



Obrázek 16 – Nahrání hlasovacího lístku

Zdroj: [29]

Popis jednotlivých kroků při načítání hlasovacího lístku:

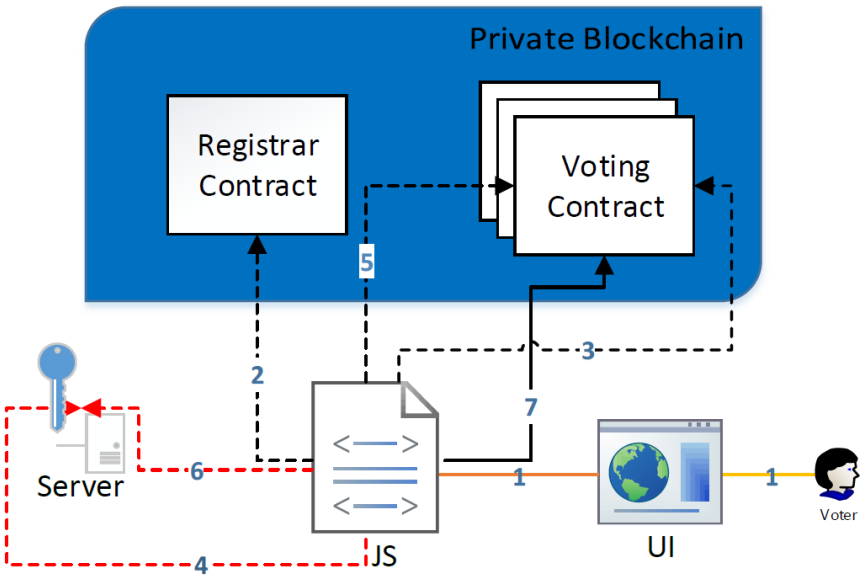
Krok 1. Volič zadá ID hlasovacího lístku do VoteUI.html a to je odesláno do VotingApp.js,

Krok 2. VotingApp.js odešle eth.calls do Registrar Contract, kde získá adresu smlouvy o hlasování spojenou s ID hlasovacího lístku,

Krok 3. VotingApp.js odešle eth.calls na smlouvu o hlasování přidruženou k adrese a načte volby a zašifrovaný počet hlasů pro každou volbu,

Krok 4. VotingApp.js odešle požadavek na šifrovací server k dešifrování počtu hlasů.

Hlasování – Proces hlasování v systému BroncoVote je zobrazen viz Obrázek 17, kde černá tečkovaná čára reprezentuje eth.calls, černá plná čára reprezentuje transakce do blockchainu a červená tečkovaná čára požadavky na šifrovací server. [29]



Obrázek 17 – Proces hlasování

Zdroj: [29]

Popis procesů v jednotlivých krocích při hlasování je následující:

Krok 1. Volič pomocí VoteUI.html zadá svoji e-mailovou adresu a volbu pro kterou chce hlasovat. Tyto informace jsou odeslány do VoteApp.js,

Krok 2. VoteApp.js pomocí eth.calls ověří voliče u Registrar Contract,

Krok 3. Pokud je volič úspěšně ověřen, VoteApp.js pomocí eth.calls zkontroluje u volební smlouvy stav voliče, zda již dříve nehlasoval a časový limit pro samotné hlasování,

Krok 4. Jestliže volič prošel všemi ověřeními, je jeho volba odeslána na šifrovací server k zašifrování,

Krok 5. VoteApp.js pomocí eth.calls zjistí u hlasovací smlouvy aktuální počet zašifrovaných hlasů,

Krok 6. VoteApp.js odešle na šifrovací server zjištěný aktuální počet zašifrovaných hlasů a zašifrovaný hlas voliče k jejich sečtení,

Krok 7. VoteApp.js odešle transakci do smlouvy o hlasování k uložení nového zašifrovaného počtu hlasů.

getVotes - Jedná se o funkci, která slouží VotingApp.js k načítání dat. [29] Kdykoliv dojde k načtení hlasovacího lístku nebo k úspěšnému hlasování je ve VotingApp.js vyvolán právě getVotes, který odešle eth. calls k získání aktuálního počtu odevzdaných zašifrovaných hlasů. V závislosti na typu voleb a časovém limitu tato funkce buď dešifruje hlasy a zobrazí je, nebo zobrazí časový úsek, ve kterém mohou uživatelé zpětně zkontrolovat výsledky voleb. Pro to, aby getVotes mohla dešifrovat počet zašifrovaných hlasů, musí tento počet odeslat na šifrovací server Crypro.js k jejich dešifrování pomocí soukromého klíče.

6.13 SEVA

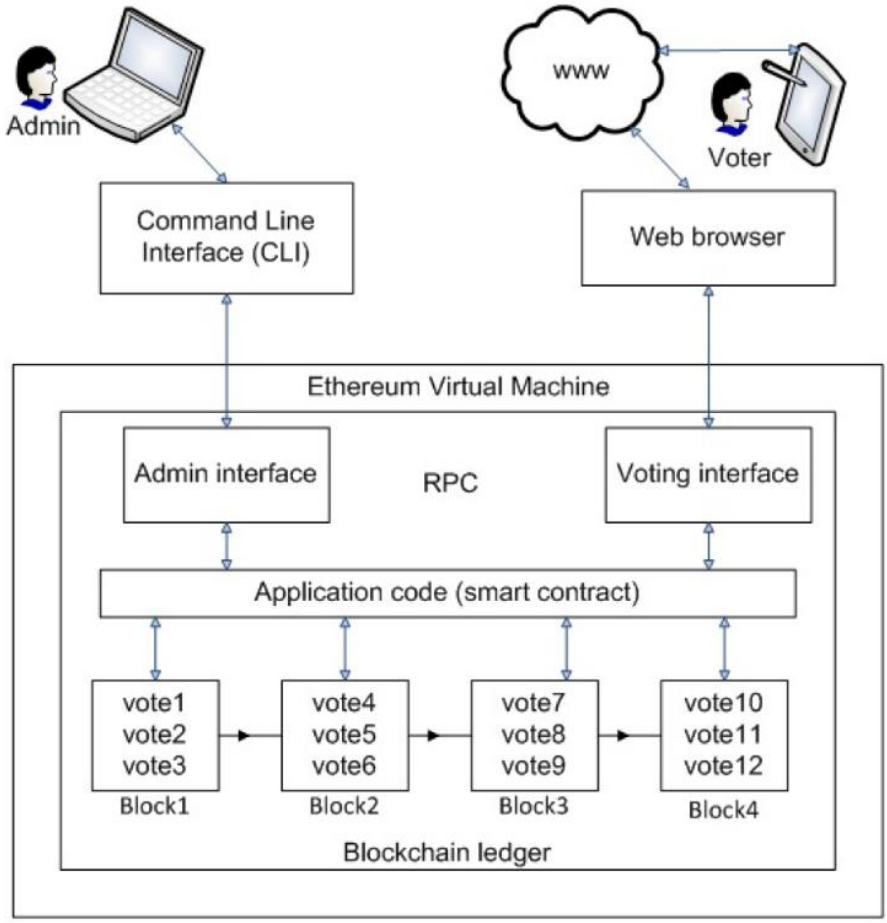
Jedná se o plně decentralizovaný systém elektronického hlasování, který je celý, kód i data, umístěný ve frameworku Ethereum, a to především z důvodu jeho ochrany před zranitelností. [53] Pro tento systém autoři navrhli nový konsensuální algoritmus PoSV (Proof of Smart Vote) jako alternativu k energeticky náročnému PoW (Proof of Work).

Proces hlasování v systému SEVA využívá rozdělení do volebních okrsků, kdy se voliči musí registrovat a hlasovat pouze ve svém volební okrsku. [53] Pro zvýšení transparentnosti voleb a snížení pravděpodobnosti útoku na jejich průběh je v každém volebním okrsku blockchainová sít se stejným počtem těžebních uzlů, které jsou vlastněny každou politickou stranou, entitou zvanou EC (Electoral Commission) a místním úřadem. Systém každému úspěšně ověřenému voliči poskytne účet Ethereum s určitým obnosem ETH, který je potřeba k odevzdání hlasovacího lístku na blockchain. Připojení k systému je realizováno pomocí webového prohlížeče uživatele, takže není zapotřebí žádný další obslužný software. Toto webové rozhraní je chráněno pomocí asymetrické kryptografie, konkrétně certifikáty SSL. Bezpečnost tohoto rozhraní je však na zodpovědnosti každého uživatele, který je zodpovědný za své zařízení.

Součásti systému – Hlasovací systém SEVA obsahuje následující komponenty a entity s přidělenými rolemi:

- **Node.js** – Soubor JavaScript, který je využíván pro distribuci aplikací mezi uzly,
- **Solidity** – Programovací jazyk pro psaní chytrých smluv pro framework Ethereum. Jedná se o silně typovaný, objektově orientovaný jazyk. Pro jeho tvorbu je využíván Solidity Compiler,
- **Ganache** – jedná se o softwarový nástroj k simulaci osobních blockchainových účtů, vývoj a nasazení chytrých smluv, poskytování RPC (Remote Procedure Call) funkcí a vlastností,
- **Truffle Framework** – Jedná se testovací framework pro Ethereum IDE (Integrated Development Environment), který je využíván pro testování, kompilaci, migraci a nasazení chytrých smluv,
- **Voters** – skupina lidí, která je splňuje kritéria toho, aby se mohla zúčastnit voleb,
- **Candidates** – podskupina lidí ze skupiny Voters, kteří se ucházejí o volební post,
- **Electoral Commission (EC)** – jedná se o nezávislý orgán, který je zmocněný k provádění voleb a vyhlašování výsledků,
- **Political Parties** – politické strany zastoupené ve volbách,
- **Local Authority** – místní volební úřad,
- **Blockchain network** – peer – to – peer síť obsahující veškeré záznamy voleb, které jsou přístupné všem zúčastněným stranám,
- **Blockchain Admins** – tým systémových administrátorů, členů EC,
- **Mining Nodes** – Skupina uzlů, které jsou zodpovědné za přidávání záznamů o hlasování do veřejné účetní knihy,
- **Non-mining Nodes** – skupina uzlů, která má za úkol sledovat a ověřovat všechny volební záznamy a transakce,
- **Smart Contracts** – softwarový kód, který řídí celý volební proces, provádí tabelaci a sčítání hlasů. [53]

Rozhraní systému – Uživatelské rozhraní systému je rozděleno na rozhraní administrátora a uživatele. [53] Rozhraní pro administrátora je složeno ze souboru nodes.js, což je program napsaný v JavaScriptu, poskytující rozhraní EVM (Ethereum Virtual Machine) ke kódování a nasazení chytré smlouvy. Uživatelské rozhraní obsahuje soubor web3.js, který poskytuje rozhraní s chytrou smlouvou pro prezentaci nabídky hlasování. Na všech uzlech v síti je dostupné jak administrátorské, tak i uživatelské rozhraní komunikující s backendem prostřednictví RPC. Celková architektura systému SEVA viz Obrázek 18.



Obrázek 18 – Architektura SEVA

Zdroj: [53]

Proces voleb v systému SEVA prochází třemi fázemi, těmi jsou Registrační fáze, Fáze hlasování a Fáze sčítání. [53]

Registrační fáze – Tato fáze hlasování zahrnuje proces kontroly, ověřování totožnosti a způsobilosti voličů. [53] Je prováděna pravidelně den před hlasováním a jejím produktem je seznam voličů.

Fáze hlasování – Fáze hlasování je rozdělena do tří fází, těmi jsou inicializace, ověření a hlasování. [53]

- Fázi inicializace provádí volební komise a obsahuje přípravu blockchainové sítě, nasazení chytrých smluv a zveřejnění webové adresy k hlasování.
- Fáze ověření vyžaduje od voliče poskytnutí jeho údajů použitých při registraci. V první fázi je požadováno přednastavené uživatelské jméno a heslo voliče. Po úspěšné první fázi je na zadané telefonní číslo voliče odeslán kód OTP (One Time Password). Po vložení kódu OTP do ověřovací aplikace je dvoufázové ověření dokončeno. Poté je voliči vygenerován a přidělen hlasovací účet Ethereum.
- Fáze hlasování zahrnuje výběr voličem preferovaného kandidáta pomocí rolovacího menu. Po jeho výběru, volič klikne na tlačítko „VOTE“ a provede odevzdání hlasu. Hlas je sečten, započítán a zapsán do blockchainu pomocí chytré smlouvy. Tato transakce je identifikována číslem TIN (Transaction Identification Number), což je číslo účtu GANACHE. Číslo TIN je zapsáno do souboru, který je po skončení voleb odeslán na telefonní číslo nebo e-mail voliče a lze ho použít k dohledání a ověření hlasování.

Fáze sčítání – Fáze sčítání je sčítání odevzdaných hlasů pro jednotlivé kandidáty, tak jak jsou zaznamenány v tabulce. [53] V aplikační simulaci, jsou hlasy tabelovány a sčítány automaticky během hlasování pomocí chytré smlouvy, což znamená, že systém SEVA je aplikace pro elektronické volby s automatickým počítáním. Nicméně výsledek je publikován až po skončení voleb.

7 Příklady států s e-volbami

Tato kapitola přináší příklady států, které využívají systémy elektronických voleb s technologií blockchain. Jsou zde zmíněny zkušenosti s implementací elektronických voleb, jejich výhody, nevýhody atd.

7.1 Sierra Leone

Dne 7. března 2018 se Sierra Leone stala první zemí, která ve volbách využila hlasovací systém založený na technologii blockchain. [56] Byl využit systém švýcarské společnosti AGORA, která v západním okrsku Sierra Leone poskytla tuto službu dvě stě osmdesáti volebním místům. [57] Společnost AGORA byla Národní volební komisí Sierry Leone (NEC) akreditována jako mezinárodní pozorovatel a souběžně s tímto procesem využívala technologii blockchainu k testovacímu sčítání hlasů jako nezávislý orgán.

Samotné volby probíhaly pomocí papírových hlasovacích lístků, které byly vhazovány do uren. [57] Po skončení hlasování byl každý jeden jednotlivý hlasovací lístek nahlas oznámen úředníky NEC a zaměstnanci společnosti AGORA tento hlas zanesli do systému blockchainu. Transparentnosti voleb v Sierra Leone bylo dosažena tak, že každý hlas byl uložen na společnou, soukromou blockchainovou síť, která byla přístupná pouze zaměstnancům společnosti AGORA. Ti po skončení voleb zveřejnili výsledek na webových stránkách společnosti AGORA, což vedlo ke snížení šance na zmanipulování jakéhokoli odevzdaného hlasu. NEC zveřejnila oficiální výsledky voleb, které byly odděleny od sčítání firmou AGORA, několik dní po volbách.

7.2 Thajsko

V listopadu 2018 nejstarší politická strana v Thajsku, opoziční Thajská demokratická strana, se stala první na světě, která využila technologii blockchain pro reálné elektronické volby zahrnující více než sto dvacet tisíc voličů. [58] Jednalo se o volby, kde si členové této politické strany království volili svého vůdce. K tomuto účelu bylo využito blockchainové platformy založené na kryptoměně s otevřeným zdrojovým kódem Zcoin, dále volebních stanic vybavených zařízeními Raspberry Pi a mobilní hlasovací aplikací, která pro ověření voličů vyžadovala předložení průkazu totožnosti s fotografií.

Data, zahrnující identifikační dokumenty a hlasovací záznamy byly zašifrovány a uloženy na decentralizovaném distribuovaném systému ukládání dat. [58] Hashe jednotlivých uložených záznamů o hlasování byly uloženy na blockchainu Zcoin. Ten sloužil jako neměnná

databáze a prostředek k zpětnému ověření hlasování pro thajskou volební komisi a členy Thajské demokratické strany.

Tajnost a integrita hlasování byla zabezpečena tak, že šifrovací klíče byly rozděleny šifrovací metodou Shamir's Secret Sharing Scheme, což zajišťovalo, že nikdo není schopen dešifrovat data o hlasování bez souhlasu a přítomnosti všech zúčastněných stran, tedy tři zástupci každého kandidáta, Thajská volební komise a Demokratická strana. [58] Identifikační doklady voličů k ověření jejich způsobilosti mohl dešifrovat pouze člen thajské volební komise nebo zástupce strany.

Tento projekt se v Thajsku ukázal jako velice úspěšný a byl označen za milník v politické historii země, který bude mít významné důsledky pro první národní volby v království.

7.3 USA

Ve státech Oregon, Colorado a Utah byl v roce 2019 spuštěn pilotní projekt, který měl za úkol zpřístupnit komunální volby pro voliče v zahraničí, vojenský personál v činné službě a zdravotně postiženým voličům pomocí aplikace založené na technologii blockchain v chytrých mobilních telefonech. [59] [60] [61]

K tomu, aby se oprávnění voliči mohli zúčastnit voleb, museli podat písemnou žádost o hlasování v nepřítomnosti a posléze dokončit proces ověření prostřednictvím mobilní aplikace Voatz. [59] [60] [61] Po úspěšném schválení a ověření mohli začít volit. Tímto se předem definovaná skupina voličů vyhnula nutnosti tisku a skenování dokumentů při normální volbě v nepřítomnosti. Voliči po odevzdání hlasu mohli ověřit, zda jejich hlas byl skutečně odevzdán.

Národní centrum kybernetické bezpečnosti USA (NCC), které se také účastnilo tohoto pilotního projektu, konstatovalo, že použití technologie blockchain v mobilním hlasování chrání elektronické volby před kybernetickými útoky a zajišťuje bezpečnost, auditovatelnost, transparentnost, přesnost sčítání volebních lístků a zvýšenou integritu volebnímu systému. [60] Naproti tomu byl Voatz kritizován ze strany politiků a komunitou zajišťující bezpečnost voleb. Na dotaz webového portálu Government Technology, kdy se dotazoval světově uznávaného bezpečnostního analytika Bruce Schneiera, zda si dokáže představit svět s online hlasováním, odpověděl následující:

„Musel by to být svět, kde téměř nikdy nedostanete aktualizaci zabezpečení od společnosti Microsoft. Může to být svět, kde téměř nikdy neslyšíte o narušení dat ve společnosti. Je to svět, kde ransomware neexistuje. Je to opravdu, opravdu jiný svět. Mám dobrou představivost, ale není to v dohledné době.“ [61]

7.4 Švýcarsko

Město Zug ve Švýcarsku provedlo v roce 2018 zkušební hlasování založené na technologii blockchain. [62] Občané města k odevzdání hlasu využili mobilní aplikaci založenou na technologii blockchain, kterou si stáhli do svých chytrých telefonů. K ověření identity voliče bylo využito již zavedené digitální identity, kterou město Zug svým občanům vydává již od zimy roku 2017.

Hlavním účelem tohoto hlasování bylo testování a vyhodnocení technických detailů použitého systému. [62] Dalším těžištěm vyhodnocení byla ochrana soukromí voliče, tajnost hlasování, jeho ověřitelnost, neměnnost a srozumitelnost.

Hlasování se zúčastnilo sedmdesát dva oprávněných voličů z dvě stě čtyřiceti. [62] V následném hodnocení systému voleb pomocí dotazníků, drtivá většinu zúčastněních voličů uvedla, že online hlasování bylo velmi snadné, pouze tři voliči uvedli opak.

Závěr

Cílem této diplomové práce bylo provedení systematické literární rešerše porovnávající různé přístupy a zkušenosti s využitím blockchain technologií pro zabezpečení a zvýšení důvěryhodnosti při elektronických volbách.

Práce byla rozdělena do dvou částí. První část se zabývala teoretickou rovinou, kde byla popsána stručná historie vzniku technologie blockchain, popsány základní principy, na kterých je technologie blockchain založena, dále bylo objasněno stručné procesní zabezpečení voleb, požadavky na systémy elektronických voleb a jejich možná technická řešení. V kapitole zabývající se technickým řešením elektronických voleb byla zmíněna nejenom řešení, která se používají v dnešní době, ale i řešení, která jsou již minulostí. Druhá část této práce byla praktická a zabývala se systematickou rešerší vybraných článků získaných z databází WoS a Scopus, ve kterých jsou popisovány jednotlivá řešení e-voleb založených na technologii blockchain. Jelikož výběr těchto článků byl proveden již v dubnu roku 2022, byl počet článků z tohoto roku minimální. V závěrečné kapitole byly uvedeny příklady států, které již e-volby založené na technologii blockchain určitým způsobem implementovaly.

Pro zodpovězení otázek ohledně bezpečnosti a důvěryhodnosti, bylo identifikováno deset atributů e-voleb využívající blockchain, na které byla rešerše vybraných článků zaměřena. Výsledná zjištění ohledně jednotlivých řešení a zvolených atributů byla zpracována do tabulky viz Tabulka 1. Je nutné podoktnout, že ne všechny zvolené atributy byly vždy popisovány v jednotlivých implementacích. Výsledná zjištění toho, pomocí kterých mechanismů blockchainu byly vybrané atributy týkající se zabezpečení a důvěryhodnosti e-voleb, zajištěny a v jaké míře, byly u každého atributu znázorněny pomocí grafu.

Na základě výše uvedených zjištění bylo autorem práce vyhodnoceno, že co se týče bezpečnosti dat, která jsou na blockchain ukládána nebo již uložena, je blockchain velkým přínosem pro e-volby, a to především na základě toho, jakým způsobem je blockchain vytvářen a jakým způsobem jsou do něj data ukládána. Toto samé lze říci i o důvěryhodnosti e-voleb, kdy data na blockchainu je velmi těžké, ne-li nemožné změnit, aniž by došlo k jeho poškození. Tyto závěry však neplatí o fázích e-voleb, kdy se voliči sami registrují do systému a přihlašují se do něj za účelem hlasování. Autor práce tyto fáze ze svého pohledu identifikoval jako velmi zranitelnou část celého systému, kdy největším rizikem spojeným se zabezpečením a důvěryhodností představuje samotný volič, jako faktor, který nese velkou část odpovědnosti za zabezpečení a důvěryhodnost samotných voleb (prozrazení hesla a jména k přístupu do

systému, aktualizace zabezpečení a samotného zařízení, pomocí kterého přistupuje k volebnímu systému … atd).

V poslední kapitole autor představil státy, které již mají určité zkušenosti s e-volbami založenými na blockchainu. V Sierra Leone e-volby sloužily k ověření výsledků klasických voleb a zabezpečení toho že nedošlo k jejich zmanipulování. Bylo reálně ověřeno snížení šance na zmanipulování voleb a velkou předností bylo uveřejnění výsledků ve velmi krátkém časovém úseku na stránkách nezávislého pozorovatele voleb.

V Thajsku bylo využito e-voleb ke zvolení vůdce místní nejstarší politické strany. Závěry těchto voleb byly jednoznačně kladné k použité technologii, kde byla vyzvednuta ochrana dat na blockchainu, tajnost hlasování, ověřitelnost voličů a transparentnost. Na základě tohoto vyhodnocení je v Thajsku do budoucna plánováno využití tohoto způsobu voleb nejenom na regionální úrovni, ale i na úrovni národních voleb.

V USA, kde volby založené na blockchainu proběhly jako pilotní programy ve třech státech, měli obrovský úspěch v účasti voličů. Na základě pokusů o hacknutí voleb se však státy vrátili k původním způsobům hlasování a další využití e-voleb je možné až po vylepšení zabezpečení.

Ve Švýcarsku bylo využito e–voleb ve městě Zug pro testovací hlasování, které mělo ověřit jeho výhody a ochotu voličů volit prostřednictvím mobilních telefonů. I přes malou účast bylo hlasování hodnoceno velmi pozitivně a většina dotázaných voličů by tuto volbu preferovala i v reálných volbách.

8 Literatura

[1] SHELDON, Robert. A timeline and history of blockchain technology. In: *EchTarget - Global Network of Information Technology Websites and Contributors: Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia* [online]. Newton: TechTarget, 2021 [cit. 2022-05-07]. Dostupné z: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

[2] SHERMAN, Alan, Farid JAVANI, Haibin ZHANG a Enis GOLASZEWSKI. *On the Origins and Variations of Blockchain Technologies* [online]. 2019, **17**(1), 72-77 [cit. 2022-05-09]. ISSN 1540-7993. Dostupné z: doi:10.1109/MSEC.2019.2893730

[3] NAKAMOTO, Satoshi. *The White Paper*. 1. vydání. Great Britain: Ignota, 2019. ISBN 978-19996759-2-9.

[4] KUMAR, Neeraj, Kumar NEERAJ a Raj PETHURU. *ADVANCES IN COMPUTERS: The Blockchain Technology for Secure and Smart Applications across Industry Verticals*. First edition. London: Academic Press, 2021. Volume 121. ISBN 978-0-12-821991-1.

[5] HOODA, Parikshit. Comparison – Centralized, Decentralized and Distributed Systems. In: *GeeksforGeeks | A computer science portal for geeks* [online]. Noida: GeeksforGeeks, 2021 [cit. 2022-05-17]. Dostupné z: https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/

[6] TOURON, Manfred. Centralized vs Decentralized vs Distributed Systems. In: *Berty Technologies* [online]. Berty, 2019 [cit. 2022-05-22]. Dostupné z: https://berty.tech/blog/decentralized-distributed-centralized

[7] VAN STEEN, Maarten a Andrew TANENBAUM. A brief introduction to distributed systems. *Computing*. 2016, **98**(10), 967-1009. ISSN 1436-5057. Dostupné z: doi:10.1007/s00607-016-0508-7

[8] What Are Distributed Systems?. In: *Splunk | The Data Platform for the Hybrid World* [online]. [cit. 2022-05-23]. Dostupné z: https://www.splunk.com/en_us/data-insider/what-are-distributed-systems.html#challenges-and-benefits

[9] BENOS, Evangelos, Rodney GARRATT a Pedro GURROLA-PEREZ. The Economics of Distributed Ledger Technology for Securities Settlement. *Ledger* [online]. 2019, **4** [cit. 2022-05-24]. ISSN 2379-5980. Dostupné z: doi:10.5195/ledger.2019.144

[10] SHAAN, Ray. The Difference Between Blockchains & Distributed Ledger Technology. In: *Towards Data Science* [online]. 2018 [cit. 2022-05-25]. Dostupné z: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92

[11] What are distributed ledger technologies (DLTs)?. In: *Hello future | Hedera* [online]. Hedera, b.r. [cit. 2022-05-26]. Dostupné z: https://hedera.com/learning/what-are-distributed-ledger-technologies-dlts

[12] VIJAI, C. a Worakamol WISETSRI. URR Blockchain and Distributed Ledger Technology (DLT): The Future of Accounting: The Future of Accounting. *Journal of Human Kinetics*. 2021, **58**, 320-323.

[13] COLOMO-PALACIOS, Ricardo, Mary SÁNCHEZ-GORDÓN a Daniel ARIAS-ARANDA. A critical review on blockchain assessment initiatives: A technology evolution viewpoint. *Journal of Software: Evolution and Process* [online]. 2020, **32**(11) [cit. 2022-11-22]. ISSN 2047-7473. Dostupné z: doi:10.1002/smr.2272

[14] FERNANDEZ-CARAMES, Tiago M. a Paula FRAGA-LAMAS. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access* [online]. 2019, **7**, 45201-45218 [cit.

2022-11-22]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2019.2908780

[15] What are smart contracts on blockchain?. In: *IBM* [online]. IBM, b.r. [cit. 2022-11-22]. Dostupné z: https://www.ibm.com/topics/smart-contracts

[16] MEET97_PATEL. Consensus Algorithms in Blockchain. In: *Geeksforgeeks* [online]. Geeksforgeeks, 2022 [cit. 2022-11-23]. Dostupné z: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/

[17] ZERO-KNOWLEDGE PROOFS. In: *Ethereum* [online]. Ethereum, 2022 [cit. 2022-11-23]. Dostupné z: https://ethereum.org/en/zero-knowledge-proofs/

[18] GUO, Huaqun a Xingjie YU. A survey on blockchain technology and its security. *Blockchain: Research and Applications* [online]. 2022, **3**(2) [cit. 2022-11-24]. ISSN 20967209. Dostupné z: doi:10.1016/j.bcra.2022.100067

[19] Volby - Politický slovník. In: *Politický slovník* [online]. Politický slovník [cit. 2022-11-12]. Dostupné z: http://www.politicky-slovnik.cz/volby/volby/

[20] UNIVERZITA PALACKÉHO V OLOMOUCI. *POLITICKÁ GEOGRAFIE: 7. přednáška: Volby (verze na web)*. Univerzita Palackého v Olomouci, b.r. Dostupné také z: https://geography.upol.cz/soubory/lide/fnukal/POG/POG_P_07.pdf

[21] VOLEBNÍ PRÁVO. In: *Politický slovník* [online]. Politický slovník, 2022 [cit. 2022-11-13]. Dostupné z: http://www.politicky-slovnik.cz/volby/volebni-pravo/

[22] VOLEBNÍ SYSTÉM. In: *Politický slovník* [online]. Politický slovník, 2022 [cit. 2022-11-13]. Dostupné z: http://www.politicky-slovnik.cz/volby/volebni-system/

[23] CETINKAYA, Orhan. Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract). In: *2008 Third International Conference on Availability, Reliability and Security* [online].

BArcelona: IEEE, 2008, s. 1451-1456 [cit. 2022-11-07]. ISBN 978-0-7695-3102-1. Dostupné z: doi:10.1109/ARES.2008.167

[24] SATIZÁBAL, Cristina, Rafael PÁEZ a Jordi FORNÉ. Secure Internet Voting Protocol (SIVP): A secure option for electoral processes. *Journal of King Saud University - Computer and Information Sciences* [online]. 2022, **34**(6), 3647-3660 [cit. 2022-11-21]. ISSN 13191578. Dostupné z: doi:10.1016/j.jksuci.2020.12.016

[25] Types of Voting. In: *Nigerian Scholars – School News, Scholarships, Past Questions, Free Tutorials* [online]. Nigerian Scholars, b.r. [cit. 2022-11-02]. Dostupné z: https://nigerianscholars.com/tutorials/electoral-systems-and-processes/types-of-voting/

[26] Elections and Technology. In: *ACE Electoral Knowledge Network* [online]. ACE, b.r. [cit. 2022-11-05]. Dostupné z: https://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b2

[27] Optical scan voting system. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2022 [cit. 2022-11-05]. Dostupné z: https://en.wikipedia.org/wiki/Optical_scan_voting_system#Digital_pen_voting_systems

[28] Supervised Public Network Direct Recording Electronic Voting (PNDRE Voting) on Existing Global System for Mobile Communication Infrastructure; a Panacea for Cheap E-voting System Implementation in Nigeria. *International Journal of Research Studies in Computer Science and Engineering* [online]. 2016, **3**(2), 21-28 [cit. 2022-11-06]. ISSN 23494859. Dostupné z: doi:10.20431/2349-4859.0302004

[29] DAGHER, Gaby, Praneeth MARELLA, Matea MILOJKOVIC a Jordan MOHLER. BroncoVote: Secure Voting System using Ethereum's Blockchain. *Proceedings of the 4th International Conference on Information Systems Security and Privacy* [online]. SCITEPRESS - Science and Technology Publications,

2018, 96-107 [cit. 2022-09-14]. ISBN 978-989-758-282-0. Dostupné z: doi:10.5220/0006609700960107

[30] PAWLAK, Michał a Aneta PONISZEWSKA-MARAńDA. *Blockchain e-voting system with the use of intelligent agent approach* [online]. New York, NY, USA: ACM, 2019, 145-154 [cit. 2022-09-14]. ISBN 9781450371780. Dostupné z: doi:10.1145/3365921.3365927

[31] PAWLAK, Michał, Jakub GUZIUR a Aneta PONISZEWSKA-MARAńDA. Voting Process with Blockchain Technology: Auditable Blockchain Voting System. *Advances in Intelligent Networking and Collaborative Systems* [online]. Cham: Springer International Publishing, 2019, 233-244 [cit. 2022-09-14]. Lecture Notes on Data Engineering and Communications Technologies. ISBN 978-3-319-98556-5. Dostupné z: doi:10.1007/978-3-319-98557-2_21

[32] CHAIEB, Marwa, Mirko KOSCINA, Souheib YOUSFI, Pascal LAFOURCADE a Riadh ROBBANA. DABSTERS: A Privacy Preserving e-Voting Protocol for Permissioned Blockchain. *Theoretical Aspects of Computing – ICTAC 2019* [online]. Cham: Springer International Publishing, 2019, 292-312 [cit. 2022-09-14]. Lecture Notes in Computer Science. ISBN 978-3-030-32504-6. Dostupné z: doi:10.1007/978-3-030-32505-3_17

[33] BRAGHIN, Chiara, Stelvio CIMATO, Simone COMINESI, Ernesto DAMIANI a Lara MAURI. Towards Blockchain-Based E-Voting Systems. *Business Information Systems Workshops* [online]. Cham: Springer International Publishing, 2019, 274-286 [cit. 2022-09-14]. Lecture Notes in Business Information Processing. ISBN 978-3-030-36690-2. Dostupné z: doi:10.1007/978-3-030-36691-9_24

[34] BISTARELLI, Stefano, Ivan MERCANTI, Paolo SANTANCINI a Francesco SANTINI. End-to-End Voting with Non-Permissioned and Permissioned Ledgers. *Journal of Grid Computing* [online]. 2019, **17**(1), 97-118 [cit. 2022-09-14]. ISSN 1570-7873. Dostupné z: doi:10.1007/s10723-019-09478-y

[35] CHAIEB, Marwa, Souheib YOUSFI, Pascal LAFOURCADE a Riadh ROBBANA. Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol. *Information Systems* [online]. Cham: Springer International Publishing, 2019, 16-30 [cit. 2022-09-14]. Lecture Notes in Business Information Processing. ISBN 978-3-030-11394-0. Dostupné z: doi:10.1007/978-3-030-11395-7_2

[36] CHAIEB, Marwa a Souheib YOUSFI. LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol. *Information Systems* [online]. Cham: Springer International Publishing, 2020, 151-168 [cit. 2022-09-14]. Lecture Notes in Business Information Processing. ISBN 978-3-030-63395-0. Dostupné z: doi:10.1007/978-3-030-63396-7_11

[37] VERWER, Michel, Ioanna DIONYSIOU a Harald GJERMUNDRøD. TrustedEVoting (TeV) a Secure, Anonymous and Verifiable Blockchain-Based e-Voting Framework. *E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age* [online]. Cham: Springer International Publishing, 2020, 129-143 [cit. 2022-09-14]. Communications in Computer and Information Science. ISBN 978-3-030-37544-7. Dostupné z: doi:10.1007/978-3-030-37545-4_9

[38] FERNANDES, Aaron, Karan GARG, Ankit AGRAWAL a Ashutosh BHATIA. Decentralized Online Voting using Blockchain and Secret Contracts. *2021 International Conference on Information Networking (ICOIN)* [online]. IEEE, 2021, 582-587 [cit. 2022-09-14]. ISBN 978-1-7281-9101-0. Dostupné z: doi:10.1109/ICOIN50884.2021.9333966

[39] ZAGHLOUL, Ehab, Tongtong LI a Jian REN. D -BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting. *IEEE Internet of Things Journal* [online]. 2021, **8**(22), 16585-16597 [cit. 2022-09-14]. ISSN 2327-4662. Dostupné z: doi:10.1109/JIOT.2021.3074877

[40] LI, Huilin, Yannan LI, Yong YU, Baocang WANG a Kefei CHEN. A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era. *IEEE Transactions on Network Science and Engineering* [online]. 2021, **8**(2), 1019-

1032 [cit. 2022-09-14]. ISSN 2327-4697. Dostupné z: doi:10.1109/TNSE.2020.3011928

[41] TAş, Ruhi, Ömer TANRıÖVER a Vincenzo CONTI. A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Security and Communication Networks* [online]. 2021, **2021**, 1-16 [cit. 2022-09-14]. ISSN 1939-0122. Dostupné z: doi:10.1155/2021/6673691

[42] RUSSO, Antonio, Antonio ANTA, Maria VASCO a Simon ROMANO. Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures. *2021 IEEE International Conference on Blockchain (Blockchain)* [online]. IEEE, 2021, 417-424 [cit. 2022-09-14]. ISBN 978-1-6654-1760-0. Dostupné z: doi:10.1109/Blockchain53845.2021.00065

[43] LU, Ning, Xin XU, Chang CHOI, Tianlong FEI, Wenbo SHI a Honghao GAO. BEvote: Bitcoin-Enabled E-Voting Scheme with Anonymity and Robustness. *Security and Communication Networks* [online]. 2021, **2021**, 1-14 [cit. 2022-09-14]. ISSN 1939-0122. Dostupné z: doi:10.1155/2021/9988646

[44] FAN, Wenjun, Shubham KUMAR, Vrushali JADHAV, Sang-Yoon CHANG a Younghee PARK. A Privacy Preserving E-Voting System Based on Blockchain. *Silicon Valley Cybersecurity Conference* [online]. Cham: Springer International Publishing, 2021, 148-159 [cit. 2022-09-14]. Communications in Computer and Information Science. ISBN 978-3-030-72724-6. Dostupné z: doi:10.1007/978-3-030-72725-3_11

[45] ZHANG, Shufan, Lili WANG a Hu XIONG. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security* [online]. 2020, **19**(3), 323-341 [cit. 2022-09-14]. ISSN 1615-5262. Dostupné z: doi:10.1007/s10207-019-00465-8

[46] LYU, Jiazhuo, Zoe JIANG, Xuan WANG, Zhenhao NONG, Man AU a Junbin FANG. A Secure Decentralized Trustless E-Voting System Based on Smart Contract. *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*

[online]. IEEE, 2019, 570-577 [cit. 2022-09-14]. ISBN 978-1-7281-2777-4. Dostupné z: doi:10.1109/TrustCom/BigDataSE.2019.00082

[47] THUY, Linh, Khoi CAO-MINH, Chuong DANG-LE-BAO a Tuan NGUYEN. Votereum: An Ethereum-Based E-Voting System. *2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)* [online]. IEEE, 2019, 1-6 [cit. 2022-09-14]. ISBN 978-1-5386-9313-1. Dostupné z: doi:10.1109/RIVF.2019.8713661

[48] SUWITO, Misni a Sabyasachi DUTTA. Verifiable E-Voting with Resistance against Physical Forced Abstention Attack. *2019 International Workshop on Big Data and Information Security (IWBIS)* [online]. IEEE, 2019, 85-90 [cit. 2022-09-14]. ISBN 978-1-7281-5347-6. Dostupné z: doi:10.1109/IWBIS.2019.8935763

[49] ABUIDRIS, Yousif, Rajesh KUMAR, Ting YANG a Joseph ONGINJO. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *ETRI Journal* [online]. 2021, **43**(2), 357-370 [cit. 2022-09-14]. ISSN 1225-6463. Dostupné z: doi:10.4218/etrij.2019-0362

[50] CHAISAWAT, Siriboon, Chalee VORAKULPIPAT a Jianting NING. Towards Achieving Personal Privacy Protection and Data Security on Integrated E-Voting Model of Blockchain and Message Queue. *Security and Communication Networks* [online]. 2021, **2021**, 1-14 [cit. 2022-09-14]. ISSN 1939-0122. Dostupné z: doi:10.1155/2021/8338616

[51] PANJA, Somnath a Bimal ROY. A secure end-to-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications* [online]. 2021, **59** [cit. 2022-09-14]. ISSN 22142126. Dostupné z: doi:10.1016/j.jisa.2021.102815

[52] LI, Peng, Junzuo LAI a Yongdong WU. Event-oriented linkable and traceable anonymous authentication and its application to voting. *Journal of Information Security and Applications* [online]. 2021, **60** [cit. 2022-09-14]. ISSN 22142126. Dostupné z: doi:10.1016/j.jisa.2021.102865

[53] ABEGUNDE, Jacob, Joseph SPRING a Hannan XIAO. SEVA: A Smart Electronic Voting Application Using Blockchain Technology. *2021 IEEE International Conference on Blockchain (Blockchain)* [online]. IEEE, 2021, 353-360 [cit. 2022-09-14]. ISBN 978-1-6654-1760-0. Dostupné z: doi:10.1109/Blockchain53845.2021.00056

[54] PANJA, Somnath, Samiran BAG, Feng HAO a Bimal ROY. A Smart Contract System for Decentralized Borda Count Voting. *IEEE Transactions on Engineering Management* [online]. 2020, **67**(4), 1323-1339 [cit. 2022-09-14]. ISSN 0018-9391. Dostupné z: doi:10.1109/TEM.2020.2986371

[55] LIN, Yikang a Peng ZHANG. Blockchain-based Complete Self-tallying E-voting Protocol. *2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* [online]. IEEE, 2019, 47-52 [cit. 2022-09-26]. ISBN 978-1-7281-3248-8. Dostupné z: doi:10.1109/APSIPAASC47483.2019.9023220

[56] KUMAR SHARMA, Toshendra. Top Countries That Conducted Elections On The Blockchain. In: *Blockchain-Council* [online]. Blockchain-Council, 2019 [cit. 2022-11-08]. Dostupné z: https://www.blockchain-council.org/blockchain/top-countries-that-conducted-elections-on-the-blockchain/

[57] PERPER, Rosie. Sierra Leone just became the first country in the world to use blockchain during an election. In: *INSIDER* [online]. INSIDER, 2018 [cit. 2022-11-08]. Dostupné z: https://www.businessinsider.com/sierra-leone-blockchain-elections-2018-3

[58] TAN, Aaron. Thailand's Democrat Party holds election with blockchain. In: *Computerweekly* [online]. Computerweekly, 2018 [cit. 2022-11-08]. Dostupné z: https://www.computerweekly.com/news/252452435/Thailands-Democrat-Party-holds-election-with-blockchain

[59] SELSKY, ANDREW. 2 Oregon counties offer vote-by-mobile to overseas voters. In: *Apnews* [online]. Apnews, 2019 [cit. 2022-11-08]. Dostupné z: https://apnews.com/article/8ce0fbc400514f55839fa84fb364d7f4

[60] DE, Nikhilesh. City of Denver to Pilot Blockchain Voting App in Coming Elections. In: *Coindesk* [online]. Coindesk, 2019 [cit. 2022-11-08]. Dostupné z: https://www.coindesk.com/markets/2019/03/07/city-of-denver-to-pilot-blockchain-voting-app-in-coming-elections/

[61] PRESSGROVE, Jed. Utah County Makes History With Presidential Blockchain Vote. In: *Govtech* [online]. Govtech, 2020 [cit. 2022-11-08]. Dostupné z: https://www.govtech.com/products/utah-county-makes-history-with-presidential-blockchain-vote.html

[62] Switzerland's first municipal blockchain vote hailed a success. In: *Swissinfo* [online]. Swissinfo, 2018 [cit. 2022-11-08]. Dostupné z: https://www.swissinfo.ch/eng/crypto-valley-_-switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928

[63] BAYTAş, Mehmet, Aykut COşKUN, Asim YANTAç a Morten FJELD. Towards Materials for Computational Heirlooms. In: *Proceedings of the 2018 Designing Interactive Systems Conference* [online]. New York, NY, USA: ACM, 2018, s. 703-717 [cit. 2022-05-16]. ISBN 9781450351980. Dostupné z: doi:10.1145/3196709.3196778

[64] FENG, Qi, Debiao HE, Sherali ZEADALLY, Muhammad KHAN a Neeraj KUMAR. A survey on privacy protection in blockchain system. In: *Journal of Network and Computer Applications* [online]. 2019, , s. 45-58 [cit. 2022-05-16]. ISSN 10848045. Dostupné z: doi:10.1016/j.jnca.2018.10.020

[65] KRAUSE, Solvej, Harish NATARAJAN a Helen GRADSTEIN. *Distributed Ledger Technology (DLT) and blockchain (English)* [online]. FinTech note, no. 1. Washington, D.C.: Worl Bank Group, 2017 [cit. 2022-05-26]. Dostupné z: http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain