EKONOMICKÁ UNIVERZITA V BRATISLAVE
NÁRODOHOSPODÁRSKA FAKULTA

KRYPTOMENY – ICH POTENCIÁLNY VPLYV NA SVETOVÉ EKONOMIKY

Diplomová práca

2019 **Martin Lindák**

EKONOMICKÁ UNIVERZITA V BRATISLAVE

NÁRODOHOSPODÁRSKA FAKULTA

KRYPTOMENY – ICH POTENCIÁLNY VPLYV NA SVETOVÉ EKONOMIKY

Diplomová práca

Študijný program:	Financie
Študijný odbor:	Financie, bankovníctvo a investovanie
Školiace pracovisko:	Katedra financií
Vedúci záverečnej práce:	Mgr. Marek Káčer, PhD.

Bratislava 2019 **Martin Lindák**

Čestné vyhlásenie

Čestne vyhlasujem, že diplomovú prácu som vypracoval samostatne a uviedol všetku použitú literatúru.

Dátum: .....

(podpis študenta)

Poďakovanie

Chcel by som sa poďakovať najmä vedúcemu mojej diplomovej práce Mgr. Marekovi Káčerovi, PhD. za profesionálnu pomoc, cenné rady, pripomienky a odborné vedenie pri vypracovaní tejto práce.

ABSTRAKT

LINDÁK, Martin: *Kryptomeny - ich potenciálny vplyv na svetové ekonomiky*. – Ekonomická univerzita v Bratislave. Národohospodárska fakulta; Katedra financií. – Vedúci záverečnej práce: Mgr. Marek Káčer, PhD. – Bratislava NHF EU, 2019, 61 s.

Cieľom diplomovej práce je teoreticky popísať, čo je kryptografia alebo inak nazývané, šifrovanie. Teoretická časť sa zaoberá históriou šifrovania od tých najjednoduchších foriem až po dnešné, elektronické formy šifrovania. Bližšie popísané je fungovanie prvej kryptomeny, Bitcoinu, jej blockchainu a taktiež jeho kľúčové vlastnosti. V rámci praktickej časti je vysvetlený priamy a nepriamy dopad kryptomien na súčasné ekonomiky, ako aj oblasti, kde by sa dala táto nová technológia v budúcnosti využiť, kde by mohla nahradiť súčasné systémy a zároveň riešiť napríklad spoločenské či ekonomické problémy. Na záver sa pozrieme na projekty, ktoré už na niektorých problémoch pracujú.

Kľúčové slová: kryptografia, šifrovanie, kryptomeny, blockchain, Bitcoin

ABSTRACT

LINDÁK, Martin: *Cryptocurrencies and their potential impact on society*. - University of Economics in Bratislava. Faculty of National Economy; Department of Finance, Thesis Supervisor: Mgr. Marek Káčer, PhD. – Bratislava: NHF EU, 2019, 61 p.

The aim of the diploma thesis is to describe theoretically what is cryptography or otherwise called encryption. The theoretical part deals with the history of encryption from the simplest forms to today's electronic forms of encryption. How the first cryptocurrency, Bitcoin works, its blockchain and its key properties. The practical part explains the direct and indirect impact of cryptocurrencies on current economies, as well as areas where this new technology could be used in the future, where it could replace existing systems while addressing social or economic problems. Finally, we look at projects that are already working on some issues.

Keywords: cryptocurrencies, encryption, blockchain, Bitcoin

OBSAH

ZOZNAM TABULIEK, GRAFOV A SCHÉM

ZOZNAM SKRATIEK A SYMBOLOV

AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
DES	Data Encryption Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
FBI	Federal Bureau of Investigation
GB	Gigabyte
GCHQ	Government Communications Headquarters
ICO	Initial Coin Offering
IDEA	International Data Encryption Algorithm
IPO	Initial Poblic Offering
NSA	National Security Agency
PGP	Pretty Good Privacy
RPOW	Reusable Proof of Work
SEC	U.S. Securities and Exchange Commission
USA	United States of America

ÚVOD

Kryptomeny sú fenoménom posledných desiatich rokov, odkedy vznikla prvá kryptomena Bitcoin. Čoraz viac sú kryptomeny diskutované v médiách a čoraz viac sa o nich diskutuje aj v súkromnom či verejnom sektore. Dôvodom tejto popularity je na jednej strane atraktívna investičná príležitosť, avšak na druhej strane, potenciálne využitie novej technológie blockchain, ktorá za kryptomenami stojí.

V diplomovej práci sa budeme venovať kryptomenám a technológii blockchain. Popíšeme si históriu tejto technológie a zároveň jej súčasný stav a potenciálne oblasti, kde by sa mohla v budúcnosti využiť. Najprv sa v diplomovej práci v rámci teoretickej časti pozrieme na krypto-technológie hlbšie. Popíšeme si hlavné piliere vzniku tejto novej technológie, pričom nazrieme do histórie šifrovania, ktoré je neoddeliteľnou súčasťou kryptomien ako základný pilier, ktorý tvorí ich špecifické vlastnosti. Pozrieme sa na predchodcov kryptomien, na projekty, ktoré neboli úspešné, avšak položili základ prvej kryptomene na svete. Neskôr si pre pochopenie opíšeme aj vznik a fungovanie prvej kryptomeny Bitcoin. V závere teoretickej časti by nám malo byť jasné, ako kryptomeny fungujú a aký veľký potenciál z hľadiska šifrovania predstavujú. V praktickej časti sú znázornené priame a nepriame dopady kryptomien na ekonomiky krajín. Najprv si vysvetlíme potenciál kryptomien, ich dopad na riešenie súčasných problémov v ekonomike či spoločnosti zameriame sa taktiež na konkrétne projekty a kryptomeny, ktorých vývoj prebieha.

Kryptomeny sú už v súčasnosti novým sektorom ekonomiky. Z médií o nich počujeme takmer denne. Po prečítaní diplomovej práce by malo byť čitateľovi jasné, ako kryptomeny fungujú, ako vznikli a ako sa k nim technologický progres dostal. Rovnako by mala diplomová práca čitateľovi poskytnúť obraz o tom, čo môžu kryptomeny a technológia blockchain zmeniť v budúcnosti.

1 Súčasný stav riešenej problematiky doma a v zahraničí

1.1 Počiatky šifrovania, ako počiatky kryptomien

V prvej polovici teoretickej časti si vysvetlíme dôležitosť a počiatky šifrovania alebo kryptografie, ktorá je základným pilierom kryptomien a tvorí ich dôležité vlastnosti. Málokto si v súčasnosti uvedomuje, že kryptomeny sú len evolúciou kryptografie či šifrovania, ktoré neraz hralo dôležitú úlohu vo vývoji dejín.

Kryptografia je vedný odbor, ktorý študuje metódy utajenia zrozumiteľného obsahu správ, na obsah, ktorý je nečitateľný alebo nezrozumiteľný takým spôsobom, že len príjemca správy je schopný utajenie odstrániť a správu prečítať.[1]

1.1.1 Stenografia

Počiatky kryptografie sa datujú niekde do 5. storočia pred našim letopočtom. Práve Herodotos, ako „otec histórie“ pripísal úspech boja Grékov proti Peržanom, tajným šifrám. Tie ochránili Grécko pred perzským panovníkom Xerxesom. Konkrétne Demaratus odoslal správu Grékom a plánoch Peržanov pomocou voskových tabuliek. Z nich zoškrabal vosk až na vrstvu dreva. Tam vyryl správu a následne tabuľky opäť zalial voskom. Na prvý pohľad nič zvláštne, avšak to stačilo na to, aby sa správa dostala adresátovi do Sparty.

Komunikácia skrytá pomocou ukrytej správy sa nazýva steganografia, podľa gréckych slov steganos (schovaný) a graphein (písať). Behom dvoch tisícročí sa rozvinuli rôzne formy steganografie vo rôznych častiach sveta. Číňania napríklad písali správy na hodváb, ktorý zbalili do guličky a následne zaliali voskom. Guličku následne posol prehltol.[2]

Bežnou formou utajenia bol aj neviditeľný atrament. Už po logickej úvahe prídeme na to, že steganografia ako forma šifrovania nie je najbezpečnejší systém šifrovania. Je ľahko odhaliteľný a pri jeho odhalení sa odhalí aj celá správa určená adresátovi.

---

[1] Jan Přikryl. *Jemný úvod do kryptografie*. s.2 [online]. [cit. 28.12.2018]. Dostupné na internete :< http://euler.fd.cvut.cz/predmety/y2kk/kzk-krypto-uvod.pdf >.

[2] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 20. ISBN 978-80-7363-850-4.

1.1.2 Transpozícia a substitúcia

Neskôr sa z tejto formy šifrovania vyvinula vyššie spomínaná kryptografia. Cieľom kryptografie nie je skryť existenciu správy, ale jej význam. Aby správu nebolo možné prečítať, odosielateľ a príjemca sa musia dohodnúť na pravidlách, ako bude správa šifrovaná, tak aby ktokoľvek iný kto ju prečíta, tak ju nebude vedieť odhaliť. V tomto kontexte sa kryptografia delí na dve vetvy. A to na transpozíciu a substitúciu.[3]

Pri transpozícii odosielateľ usporadúva písmená len v inom poradí ako sú v pôvodnom a zrozumiteľnom texte. So zvyšujúcim sa počtom slov v správe sa správa stáva bezpečnejšou, keďže v krátkom texte je vyššia pravdepodobnosť, že dokážeme uhádnuť správne poradie písmen a slov.

V súvislosti s transpozíciou vzniklo aj prvé šifrovacie vojenské zariadenie zo Sparty tzv. Scytale. Jedná sa o drevenú tyč, okolo ktorej sa obmotá pergamen, následne sa naň napíše správa a opäť sa odmotá a odošle. Bez drevenej tyče text nedáva zmysel, avšak so správnym priemerom inej drevenej tyče dáva text opäť zmysel. Pre lepšiu predstavu je Scytale uvedený na obrázku nižšie.

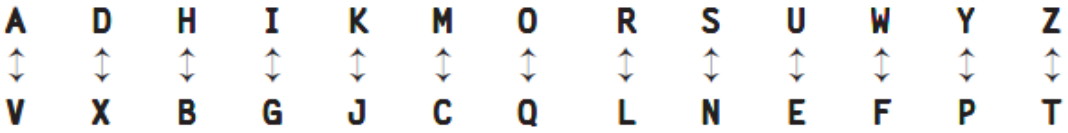
Obrázok 1: Príklad ako vyzeralo Scytale

Prameň: WIKIPEDIA.ORG. *Scytale*. [online]. [28.12.2018]. Dostupné na internete: < https://en.wikipedia.org/wiki/Scytale>.;

[3] Tamtiež, s. 21.

Alternatívou ku transpozičnej šifre je substitučná šifra. Jeden z prvých popisov substitučnej šifry sa objavuje v Kámasútre, ktorú napísal v 4. storočí nášho letopočtu bráhman Vátsjájana, pričom vychádzal z rukopisov o 800 rokov starších. V knihy sa odporúča ženám študovať okolo 64 umení, mieni nimi varenie, obliekanie, masáž atď. Medzi týmito umeniami je 45. umením na zozname tzv. mlecchita-vikalpa, umenie tajného písma, ktoré sa odporúča ženám, aby mohli utajiť svojho partnera. Princípom je párovanie písmen abecedy, tak aby sme vedeli ako boli písmená spárované a dal sa text dešifrovať.[4]

Obrázok 2: Princíp fungovania substitučnej šifry



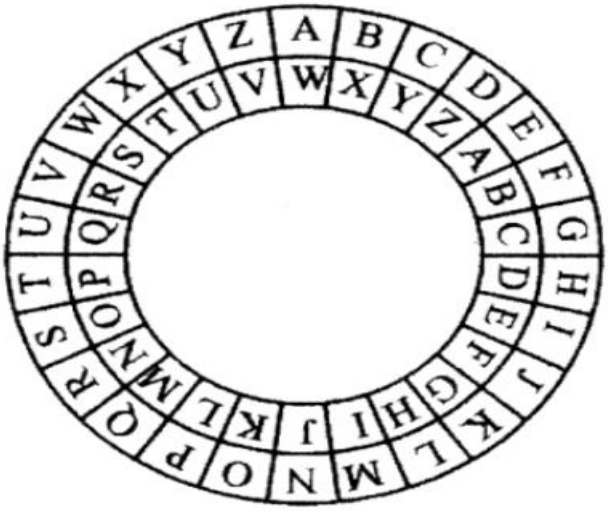
Prameň: SINGH. S. 2017. Kniha kódů a šifer. 3. vyd. Praha: nakladateľstvo Dokorán, s. r. o.; s. 23. ISBN 978-80-7363-850-4.

Využitie substitučnej šifry na vojenské účely sa objavilo v ére Gaiusa Juliusa Caesara. Z počiatku používal len jednoduché šifry a to v tom zmysle, že šifroval text len v inom jazyku, než bol jazyk nepriateľa. Až neskôr začal používať tzv. Caesarovu šifru, a to posunutie abecedy o 3 písmená. Neskôr sa z toho vyvinul aj ďalší šifrovací nástroj, ktorý pozostával z dvoch diskov, na ktorých bola abeceda. Pomocou nich ste mohli jednoducho zvoliť si posunutie, ktoré ste potrebovali a následne šifrovať text. Samozrejme tento kľúč k šifrovaniu/dešifrovaniu musel mať aj váš adresát. Treba zdôrazniť, že tento disk sa prvý krát objavil až v 15. storočí .[5]

[4] Tamtiež, s. 23.

[5]Ján Skalka, Cyril Klimeš, Gabriela Lovászová, Peter Švec, *Informatika na maturity a prijímacie skúšky*, Enigma, Nitra 2007, ISBN 978-80-89132-50-8. In*: História a princípy šifrovania*. [online]. [cit. 28.12.2018]. Dostupné na internete :<https://encyklopediapoznania.sk/clanok/444/historia-a-principy-sifrovania-scytale-cezarova-sifra-sifrovaci-disk-vigenerova-sifra-cardanova-sifra-vernamova-sifra-kluc-substitucne-a-transpozicne-sifry >.

Obrázok 3: Caesarova šifra



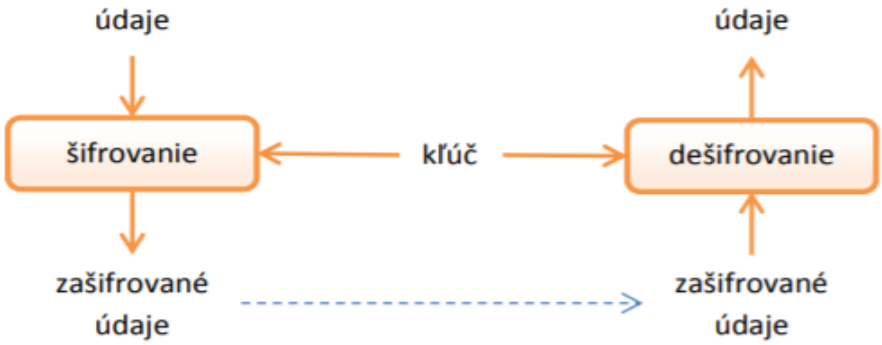
Prameň: Ján Skalka, Cyril Klimeš, Gabriela Lovászová, Peter Švec, *Informatika na maturity a prijímacie skúšky, Enigma*, Nitra 2007, ISBN 978-80-89132-50-8. In: *História a princípy šifrovania*. [online]. [cit. 28.12.2018]. Dostupné na internete :<https://encyklopediapoznania.sk/clanok/444/historia-a-principy-sifrovania-scytale-cezarova-sifra-sifrovaci-disk-vigenerova-sifra-cardanova-sifra-vernamova-sifra-kluc-substitucne-a-transpozicne-sifry >.

Substitučná šifra, je tzv. symetrická šifra, to znamená že: „V prípade, že šifrovací a dešifrovací kľúč sú rovnaké, hovoríme o symetrických šifrách.“[6]

To znamená, že odosielateľ a prijímateľ správy, musia vopred vedieť o kľúči, ktorý má text šifrovať/dešifrovať. A musia sa na tom vopred zhodnúť. Príkladom je Ceasarova šifra, kde ste museli vedieť, o koľko písmen v abecede sa šifra posunula.

[6] STANEK. M.. *Kryptológia.* s.3. [online]. [cit. 28.12.2018]. Dostupné na internete:< http://www.dcs.fmph.uniba.sk/~stanek/Kryptologia%20v1b.pdf >.

Obrázok 4: Symetrické šifrovanie



Prameň: STANEK. M.. *Kryptológia.* s.3. [online]. [cit. 28.12.2018]. Dostupné na internete:< http://www.dcs.fmph.uniba.sk/~stanek/Kryptologia%20v1b.pdf >.

V rámci kryptografie a tzv. kryptografov, treba brať do úvahy, že existovali aj ich oponenti, teda kryptoanalytici, ktorí sa zaoberali dešifrovaním a hľadaním šifrovacích kľúčov.

Kolískou kryptoanalýzy sa stala islamská civilizácia, keďže na kryptoanalýzu bolo potrebné vzdelanie v oblasti štatistiky, matematiky a lingvistiky. Prvá technika kryptoanalýzy bola objavená pravdepodobne v 9. storočí nášho letopočtu. Táto technika sa nazývala frekvenčná analýza a umožňovala kryptoanalytikom ešte dlhé storočia odhaľovať šifry kryptografov. Jej princíp spočíval v tom, že ste museli dôkladne poznať jazyk v ktorom bol pravdepodobne text písaný a následne ste pomocou frekvencie používania jednotlivých písmen, či slov a ich skladby vylučovacou metódou určovali pravdepodobné písmená v tom ktorom jazyku. [7]

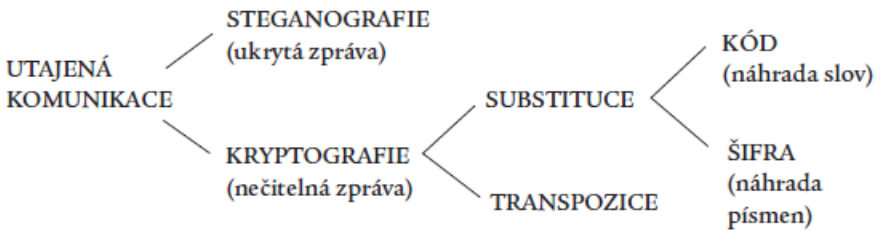
Neskôr to bol po dlhé storočia boj kryptografov a kryptoanalytikov, pričom vždy bola jedna skupina o krok popredu pred druhou. Ďalším vylepšením substitučnej šifry boli napr. kódy. Kódy sú: „Substitúcia na úrovní slov či fráz, zatiaľ čo šifra je substitúciou na úrovni písmen.“[8]

Pre lepší prehľad uvádzame schému:

[7] SINGH. S. 2017. *Kniha kódů a šifer. 3. vyd.* Praha: nakladateľstvo Dokorán, s. r. o.; s. 30-34. ISBN 978-80-7363-850-4.

[8] Tamtiež, s. 42.

Obrázok 5: Delenie utajenej komunikácie



Prameň: SINGH. S. 2017. Kniha kódů a šifer. 3. vyd. Praha: nakladateľstvo Dokorán, s. r. o.; s. 43. ISBN 978-80-7363-850-4.

Výhodou a zároveň nevýhodou kódov je, že sa musíte s prijímateľom správy dopredu dohodnúť, ako budú jednotlivé slová označené. To na jednej strane zvyšuje bezpečnosť, avšak na strane druhej robí proces náročnejším. V konečnom dôsledku budeme musieť mať nejakú šifrovaciu knihu. Tú vám, ale nemôže nikto ukradnúť, pretože by dokázal rozlúštiť vaše správy.

1.1.3 Polyalfabetická šifra

Doteraz sme písali o tzv. monoalfabetickej substitučnej šifre, ktorá dlhé storočia plnila svoj účel, avšak nebola dostatočne bezpečná a to spôsobilo niektoré prelomové udalosti v histórii, ako napríklad poprava škótskej kráľovnej Márie Stuartovej.[9]

V 16. storočí vynašli prvú polyalfabetickú šifru, ktorou je Vigenérova šifra pomenovaná po jej nálezcovi, ktorý sa volal Blaise de Vigenére. Polyalfabetická šifra je šifra, ktorá využíva viacero abecied pre jedno šifrovanie. Najväčší možný počet je 26 abecied, teda pre každé jedno písmeno. Pre predstavu uvádzame nižšie Vigenérov štvorec.

[9] Tamtiež, s. 57.

Obrázok 6: Vigenérov štvorec

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Prameň: SINGH. S. 2017. Kniha kódů a šifer. 3. vyd. Praha: nakladateľstvo Dokorán, s. r. o.; s. 120. ISBN 978-80-7363-850-4.

Na použitie šifry potrebujeme kľúč, teda nejaké slovo, od jeho dĺžky sa odvíja aj zložitosť šifry. Následne potrebujeme text, ktorý šifrujeme. V prípade kľúča **auto** si nájdeme jednotlivé abecedy podľa prvého písmena zľava, teda 26., 20., 19. a 14. riadok, a následne si medzi malými písmenami na vrchu štvorca nájdeme konkrétne písmená z textu ktorý šifrujeme. Následné do šifrovaného textu používame písmeno, ktoré sa nám prekrižuje z toho-ktorého riadku a stĺpca. Tu treba zdôrazniť, že slovo auto sa nám opakuje dookola, od začiatku šifrovaného textu až po koniec a ide postupne zľava doprava v šifrovanom texte a jeho písmenách.[10]

Šifra dlhšiu dobu mala široké uplatnenie, avšak nakoniec aj túto šifru prelomili a to aj napriek jej vylepšenia na zvýšenie bezpečnosti.

[10] Tamtiež, s. 56-62.

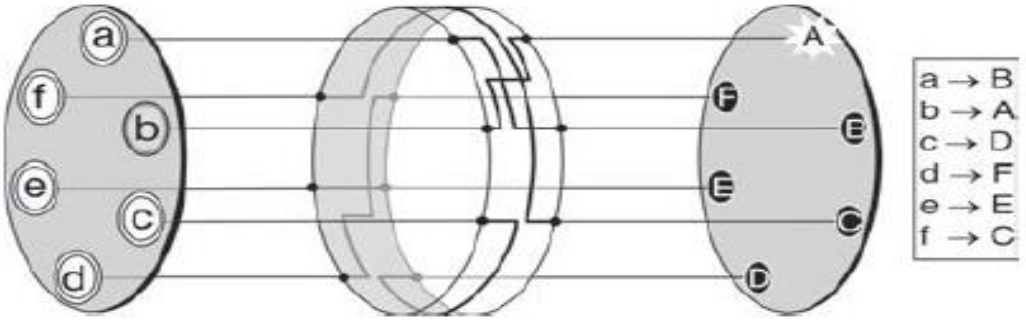
1.2 Mechanizácia šifrovania

Dôležitosť šifrovania sa zvýšila v dobe, keď sa vynašiel telegraf či rádio a boli správy ostatným viac dostupné. Čo si vyžadovalo mať kvalitné šifrovanie. To sa prejavilo najmä počas prvej svetovej vojny v rokoch 1914 až 1918, avšak vtedajší kryptografi nepriniesli nič prelomové a väčšinou sa jednalo len o šifry, ktoré kombinovali už prelomené šifry z minulosti. Vo výhode boli krajiny dohody, ktoré disponovali silnými kryptoanalytickými tímami a pomocou nich dokázali dešifrovať správy nepriateľov, a tak zefektívniť a skrátiť boje a celkovo vojnu.[11]

Prelom nastal až koncom prvej svetovej vojny, keď americkí vedci zistili ako používať Vigenérovu šifru efektívnejšie a položili tým základ pre vynález známy z druhej svetovej vojny, a to Enigmu. Vigenérova šifra mala jeden hlavný nedostatok, a to že používala kľúče (slová), ktoré dávali zmysel a preto sa aj ľahšie šifra dešifrovala. Americkí vedci začali používať náhodne generované slová, ktoré bolo oveľa ťažšie odhaliť, avšak museli ste vlastniť, tzv. kódovaciu knihu a rovnakú knihu musel mať aj adresát. Na základe knihy a konkrétnej strany či textu, ste šifrovaný text dešifrovali. [12]

Enigmu vymysleli nemeckí vynálezcovia Arthur Scherbius a Richard Ritter v roku 1918. Enigma sa skladá z troch prepojených častí: klávesnica, šifrovacia jednotka a signálna doska s lampičkami, tie signalizujú výstup z Enigmy, teda konkrétne zašifrované písmeno. Kľúčovou časťou stroja je tzv. scrambler, teda gumový kotúč, ktorý je pretkaný drôtmi, ktoré vedú signál. Tento kotúč prevádza drôtmi písmená z otvoreného textu na šifrované písmená. Pre jednoduchšie pochopenie prikladáme nižšie obrázok, ako to funguje. Na tomto obrázku je pre jednoduchosť zobrazená len 6 písmenová abeceda.

Obrázok 7: Zobrazenie scrambleru Enigmy



[11] Tamtiež, s. 104-116.
[12] Tamtiež, s. 116-124.

Prameň: SINGH. S. 2017. Kniha kódů a šifer. 3. vyd. Praha: nakladateľstvo Dokorán, s. r. o.; s. 128. ISBN 978-80-7363-850-4.

Prostredný kruh je práve scrambler, napravo je náš text, ktorý píšeme prostredníctvom klávesnice a ľavý kruh je výstup z Enigmy, teda zašifrovaný text. Kľúčovým prvkom je, že scrambler sa vždy po zadaní jedného písmena pootočí, avšak problémom je že má 6 šifrovacích abecied a po 6 otáčkach sa dostane na pôvodnú polohu. Táto pravidelnosť, ktorej sa chcú kryptografi vyhýbať sa riešila ďalším scramblerom, ktorý sa otočil len v prípade, keď prvý scrambler spravil jednu celú otáčku. To znamená, keď sa otočil šesťkrát v našom prípade. V prípade celej abecedy je to 26x26= 676 odlišných nastavení, ktoré Enigma mohla mať, pričom sa pridal ešte jeden ďalší scrambler. Celkovo bolo možných nastavení 17 576. V skutočnosti vynálezcovia ešte pridali možnosť meniť samotné scramblery medzi sebou a pridali aj tzv. prepojovaciu dosku, kde sa mohlo zameniť 6 párov písmen. Po zarátaní vylepšení, ktoré vynálezcovia spravili je to $10x10^{12}$ možných nastavení Enigmy, teda kľúčov. Keby kryptoanalytik skúšal každú minútu jedno nastavenie, potreboval by na preverenie každej možnosti približne vek vesmíru, ktorý sa odhaduje na približne 13 mld. rokov.[13][14]

Scherbius zahájil veľkovýrobu až v roku 1925, potom, čo začal predávať Enigmu samotnej nemeckej armáde, ktorá mala o ňu záujem. Neskôr sa uplatnila aj v komerčnom sektore medzi obchodníkmi.[15]

Enigma neostala dlho nerozlúštená a v 30. rokoch ju vďaka Francúzom, ktorí predali papiere o nastavení a fungovaní Enigmy, ktoré dostali od Nemca Hansa-Thila Schmidta, dešifrovali Poliaci. Dôvodom bolo, že francúzska špionáž nebola natoľko rozvinutá a netrúfla si na dešifrovanie Enigmy. V Poľsku sa za rozlúštenie zaslúžil úrad Biuro Szyfrów a konkrétne kryptograf Marian Rejewski. Ten rozlúštil Enigmu vďaka manuálu od Francúzov, a chybe, ktorú robili Nemci v odosielaní správ, čo mu znížilo počet možných nastavení Enigmy na 17 576. Na tento účel zostavil aj tzv. bomby, čo boli špeciálne zariadenia, ktoré počítali konkrétne usporiadanie scramblerov a ktorým to trvalo približne 2 hodiny. Tu treba

[13] Tamtiež, s. 127-135.

[14] TASR. *Podľa najnovších výskumov je vesmír starší o 80 miliónov rokov*. [online]. [cit. 28.12.2018]. Dostupné na internete: <http://skolskyservis.teraz.sk/zaujimavosti/vyskum-vesmir-vek-sonda-planck/2122-clanok.html >.

[15] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 140. ISBN 978-80-7363-850-4.

zdôrazniť, že Nemci každý deň menili nastavenie Enigmy, podľa kódovej knihy. To znamená, že na odhalenie nastavenia Enigmy mal 24 hodín. V prípade Enigmy, ktorú používali Nemci v 30. rokoch mal úrad celkovo šesť bômb, keďže možných variant usporiadania scramblerov bolo šesť. Neskôr pred začiatkom vojny Nemci pridali ďalšie dva scramblery. To znamená, že ich bolo dokopy 5 a z toho použili vždy tri. To znamenalo, že Marian Rejewski by potreboval celkovo 60 bômb, na to aby mohli počítať 17 576 nastavení. Na takýto počet bômb už Biuro Szyfrów nemalo rozpočet. Neskôr Nemci zvýšili aj počet párov písmen, ktoré sa mohli zmeniť zo 6 na 10. Výsledkom bolo, že Poliaci predali Enigmu spolu s manuálom a plánom konštrukcie bômb tesne pred začiatkom druhej svetovej vojny spojencom, teda Francúzsku a Veľkej Británii.[16]

Po predaní všetkých vecí sa dešifrovanie presunulo do Bletchley Parku v Buckinghamsire vo Veľkej Británii. Vedci si Enigmu v roku 1939 osvojili a mali aj vyššie finančné zdroje než poľské Biuro Szyfrow. Hneď po vyhlásení vojny Veľkou Britániou prišiel do Bletchley Parku mladý matematik Alan Turing, ktorý ešte predtým vo svojej stati O Vyčísliteľnosti[17] popísal tzv. univerzálny Turingov stroj. Jednalo sa v princípe o novodobý počítač, teda stroj, ktorý by bol schopný vykonávať zložité operácie a bol by programovateľný.

Alan Turing sa následne v Bletchley Parku začal venovať Rajewského odhaleniam v súvislosti s rozlúštením Enigmy. Rajewského postup zatiaľ na odhladovanie do určitej miery stačil. Napriek tomu, bolo potrebné nájsť financie a nový spôsob ako dešifrovať Enigmu na dennej báze. To sa Turingovi pomocou matematiky, logiky a niektorým chybám Nemcov, ktoré opakovali pri šifrovaní, podarilo. Aj za pomoci Britského premiéra Winstona Churchilla, ktorého kvôli financiám na tzv. bomby, priamo kontaktoval. Prvú bombu, ktorú Turing upravil, aby zvládala viac výpočtov za kratší čas, dodali do Bletchley Parku začiatkom roka 1940. Koncom roka 1942 bolo v Bletchley Parku už dostupných 49 bômb. V prípade dobrého nastavenia bômb, teda scramblerov a prepojovacích káblov, sa mohol nájsť kľúč do jednej hodiny. Napriek tomu dešifrovanie nebolo jednoduché, pretože bomby potrebovali obsluhu

[16] Tamtiež, s. 141-156.
[17] V angličtine On Computable Numbers

a rovnako hľadanie tzv. spojení/ťahákov, v šifrovaných textoch a až následne dokázali nájsť kľúč, teda nastavenie Enigmy v konkrétnom dni. [18]

Napriek tomu, to Alan Turing a jeho tím nemali jednoduché. Dôvodom bolo to, že Enigma mala vybudovanú pevnú sieť s odlišnosťami. Napríklad v Európe používali Nemci odlišné šifrovacie knihy ako v Afrike. Rovnako Luftwaffe, nemecké letectvo, alebo námorníctvo, teda Kriegsmarine mali odlišné nastavenie Enigmy. Kriegsmarine používalo 8 scramblerov a nie 5, čo znamenalo 6-krát viac možných usporiadaní, ktoré museli analytici v Bletchley parku preveriť. Rovnako operátori Kriegsmarine si dávali pozor na to, aby sa v ich šifrovaní nedal nájsť nejaký systém alebo ťahák, ktorý by ľuďom v Bletchley parku uľahčil prácu. To viedlo k tomu, že Spojenci strácali kontrolu v tzv. bitke o Atlantik a nemecké ponorky mali prevahu.

Spojenci sa rozhodli čo najskôr získať návod na nastavenie Enigmy alebo kódovú knihu, pripravili si plán na špionážnu akciu, avšak tá sa nakoniec neuskutočnila, keďže sa im medzitým podarilo ukoristiť dokumenty s nastavením Enigmy. Po tomto sa už darilo Bletchley parku pravidelne dešifrovať správy Kriegsmarine a zabraňovať útokom na spojenecké obchodné lode. Spojencom sa darilo skrývať ich odhalenie Enigmy rôznymi manévrami, tak dobre, že Nemci aj po vyšetrovaní jedného útoku spojencov došli k záveru, že tak presne mierený útok bol vecou náhody a nie dešifrovania Enigmy.

Bletchley parku sa podarilo dešifrovať aj Japonské a Talianske šifrovanie. Dešifrovanie komunikácie Nemecka, Talianska a Japonska malo meno operácia Ultra. Odhaduje sa, že činnosť Bletchley parku skrátila druhú svetovú vojnu o niekoľko rokov, keďže kryptoanalytici významné pomáhali pri všetkých väčších operáciách, či už v Afrike, pri vylodení v Taliansku alebo vylodení v Normandii. V každej z týchto operácií výrazne pomohli k víťazstvu. [19]

[18] SINGH. S. 2017. *Kniha kódů a šifer. 3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 156-174. ISBN 978-80-7363-850-4.

[19] SINGH. S. 2017. *Kniha kódů a šifer. 3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 175-181. ISBN 978-80-7363-850-4.

1.3 Vznik počítačov[20]

Počas druhej svetovej vojny existoval aj lepší šifrovací prístroj a šifra než Enigma. Bola ňou šifra Lorenz, ktorú používal Adolf Hitler pri komunikácii s jeho generálmi. Na túto šifru sa používal prístroj Lorenz SZ40, ktorý bol zložitejší než Enigma. Napriek tomu, že kryptoanalytici ako John Tiltman a Bill Tutte našli slabinu šifry, nemohli používať na dešifrovanie bomby, ktoré používali na dešifrovanie Enigmy. Dôvodom bolo to, že dešifrovanie šifry Lorenz si vyžadovalo viacero úkonov z viacero oblastí, a nebolo to len mechanickým dešifrovaním. Niekedy v priebehu vojny prišiel Max Newman, matematik z Bletchley parku, na spôsob ako automatizovať dešifrovanie šifry Lorenz. Primárne vychádzal z Turingovho konceptu univerzálneho prístroja, ktorý bol schopný riešiť rôzne problémy a v princípe bol prvým programovateľným počítačom. Koncept a postavenie finálneho prístroja pod menom Colossus bol vedením odmietnutý a až neskôr v roku 1943 ho do Bletchley parku priniesol Tommy Flowers, ktorý ho z vlastnej iniciatívy skladal 10 mesiacov.

Po vojne ho museli kvôli bezpečnosti zničiť spolu aj s konštrukčnými plánmi. Dnes poznáme tento prístroj pod menom ENIAC (Electronic Numerical Integrator and Calculator), ktorý v roku 1945 postavili J. Presper Eckert a John W. Mauchly z University of Pennsylvania.

Práca počítačov so šiframi sa veľmi podobá starým metódam, avšak napriek tomu má niekoľko rozdielov:

1. Mechanické šifrovacie stroje majú technické obmedzenia, čo sa týka šifrovania. Počítače môžu v princípe napodobniť šifrovacie stroje rôznej zložitosti.
2. Počítače sú rýchlejšie než mechanické šifrovacie stroje.
3. Počítač nepracuje so slovami, ale prevádza abecedu na binárne čísla (binary digits). Konkrétne, napríklad protokolom ASCII (American Standard Code for Information Interchange). ASCII priraďuje každému písmenu abecedy binárne číslo zložené zo 7 čísel (kombinácia jednotiek a núl). V konečnom dôsledku poskytuje 128 možných spôsobov, ako usporiadať 7 binárnych čísel (rozumej

[20] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 230-235. ISBN 978-80-7363-850-4.

jednotiek a núl. Neskôr bolo pridané ďalšie binárne číslo, čo rozšírilo počet možností na 256).

Šifrovanie bolo z počiatku len aplikáciou starších metód ako substitúcia či transpozícia. Dôvodom bolo aj to, že šifrovanie prostredníctvom počítačov bolo z počiatku obmedzené len na vlastníkov, medzi ktorých patrila najmä armáda a štát. Až behom 60. rokov ceny počítačov klesli a výkon a používanie počítačov vzrástlo.

1.4 Šifra DES[21]

S rozširovaním počítačov sa zväčšila aj potreba mať nejaký šifrovací štandard, keďže počítače a šifrovanie sa používali vo väčšine ekonomiky, či už v bankovom sektore, obchode alebo v iných oblastiach. Problémom bolo, že každá spoločnosť mala vlastný kľuč či šifrovanie. Prvým dlhodobo používaným štandardom bola šifra Lucifer, ktorá bola v roku 1976 oficiálne prijatá pod menom DES (Data Encryption Standard). Šifru navrhol nemecký emigrant Horst Feistel, ktorý po problémoch s National Securty Agency (NSA), ktorá doteraz zaisťuje bezpečnosť a priebeh vládnej a vojenskej komunikácie, vytvoril túto šifru v laboratóriu J.Watsona v IBM. Samotná šifra fungovala na princípe rozdeľovania - napríklad 128bitová správa sa rozdelila na bloky, ktoré sa samostatne šifrovali - a miešania. Samotné vlastnosti a podmienky šifrovania sa mohli meniť, keďže boli predmetom kľúča (bolo to číslo) na ktorom sa dohodli odosielateľ a príjemca. Neskôr vďaka vývoju bola reputácia šifry podlomená a nahradil ju nový štandard v roku 2002 tzv. AES (Advanced Encryption Standard).

Čo bolo stále problémom šifrovania v povojnovom období, bola distribúcia kľúčov. Rovnako ako počas druhej svetovej vojny museli Nemci distribuovať knihu kľúčov každej jednotke, ktorá mala Enigmu. Rovnako tak verejný aj súkromný sektor v období počítačov musel distribuovať kľúče fyzicky. To stálo obe sektory vysoké sumy peňazí, pričom museli dôverovať pár ľudom, ktorý boli zamestnaní v spoločnosti. Až v 70. rokoch 20. storočia prišli na to, ako vyriešiť problém distribúcie kľúčov, ktorý bol spojený so šifrovaním od začiatku používania.

[21] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 235-239. ISBN 978-80-7363-850-4.

1.5 Vyriešenie problému distribúcie kľúčov[22]

V roku 1974 sa stretli dvaja kryptografi, ktorí pracovali nezávisle od akejkoľvek korporácie alebo štátnej agentúry. Boli to Martin Hellman a Whitfield Diffie. Neskôr sa k nim pripojil aj Ralph Merkle. Táto trojica spoločne prišla na matematickú funkciu, kde nebolo potrebné, aby sa dvojica, ktorá si vymieňala kľúč stretla a dohodla sa na postupe. Dokonca sa mohli o tom spokojne baviť cez e-mail alebo telefón aj napriek tomu, že by ich niekto odpočúval. Po dvoch rokoch prišli na to, že odpoveďou na dlhotrvajúci problém bola modulárna aritmetika a jej vlastnosti ako jednosmernej funkcie, kde je náročné sa z vypočítaného čísla dostať na číslo pôvodné. Na rozdiel napríklad od bežne aritmetiky, kde vieme, že napríklad 3*3=9 a rovnako 9/3=3. Objav tejto trojice môžeme najjednoduchšie ilustrovať na priloženej tabuľke, kde vystupuje dvojica Alica a Bob a zároveň tretia strana, ktorá chce odhaliť ich šifru.

[22] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 239-252. ISBN 978-80-7363-850-4.

Obrázok 8: Ukážka fungovania jednosmernej funkcie

Kroky	**Alica**	**Bob**
Krok č.1	Alica zvolí napríklad číslo 3 a uchová si ho v tajnosti. Toto číslo označíme ako A.	Bob zvolí napríklad číslo 6 a uchová si ho v tajnosti. Toto číslo označíme ako B.
Krok č.2	Alica vloží 3 o jednosmernej funkcie a vypočíta výsledok $7^3 (\text{mod } 11) = 343 (\text{mod } 11) = 2$.	Bob vloží 6 o jednosmernej funkcie a vypočíta výsledok $7^6 (\text{mod } 11) = 117\,649 (\text{mod } 11) = 4$.
Krok č.3	Alica nazve tento výsledok ako Alfa a pošle ho Bobovi.	Alica nazve tento výsledok ako Beta a pošle ho Bobovi.
Výmena	V normálne situácii by bol práve toto ten moment, keď si Alica a Bob vymieňajú informácie. Tretia strana by mohla komunikáciu odpočúvať a zistiť utajované informácie. Napriek tomu, že tretia strana môže komunikáciu odpočúvať, tak systém neovplyvní. Tretia strana sa dozvie len čísla 2 a 4, avšak tie nie sú kľúčom, a tak nezáleží, či sa ich tretia strana dozvie	
Krok 4	Alica vezme Bobov výsledok a vypočíta: $4^3 (\text{mod } 11) = 9$	Bob vezme Alicin výsledok a vypočíta: $2^6 (\text{mod } 11) = 9$
Kľúč	Obaja dospeli k rovnakému číslu 9. A to je kľúčom.	

Prameň: SINGH. S. 2017. Kniha kódů a šifer. 3. vyd. Praha: nakladateľstvo Dokorán, s. r. o.; s. 251. ISBN 978-80-7363-850-4.

Po zverejnení v roku 1976 to bol veľkolepý objav, ktorý uznala široká verejnosť a aj kryptografická pôda. Problémom stále bolo, že v prípade, že dve strany boli v rôznych štátoch v rôznych časových pásmach, tak stále museli na seba čakať, kým sa druhá strana ozve alebo odpíše na e-mail. Preto sa naďalej hľadali praktickejšie riešenia tohto problému.

1.6 Asymetrické šifrovanie

V roku 1975 jeden z trojice Whitfield Diffie prišiel na to, ako tento problém vyriešiť. A prišiel na tzv. asymetrické šifrovanie, kde sa nebude používať jeden kľúč, ale naopak dva kľúče, a to verejný a súkromný kľúč. Presnejšie verejný kľúč niekoho budete môcť nájsť kdekoľvek, avšak súkromný si ponecháte len vy. Keď vám niekto bude chcieť odoslať správu, tak ju zašifruje vašim verejným kľúčom a následne si vy môžete dešifrovať túto správu vašim

súkromným kľúčom. Diffie to popísal teoreticky, avšak neprišiel na vhodnú matematickú funkciu. Rovnako prvý náčrt asymetrického šifrovania, ešte nevyriešil všetky problémy s tým súvisiace.

Na vhodnú funkciu prišla až iná trojica, konkrétne Ron Rivest, Leonard Adleman a Adi Shamir. Trojica v roku 1977 našla odpoveď na jednosmernú funkciu v teórii čísiel, a to konkrétne v prvočíslach. Zjednodušene môžeme vysvetliť šifrovanie takto:

1. Potrebujeme si zvoliť dostatočne veľké dve prvočísla A a B (čísla, ktoré sú deliteľné jednotkou a sebou samým, ako napríklad 3 alebo 5)
2. Následne ich vynásobíme medzi sebou a dostaneme číslo N, ktoré nám bude slúžiť ako verejný kľúč a môžeme ho kdekoľvek zdieľať. Používame ho v rámci jednosmernej funkcie, ktorá nám šifruje správu
3. A a B nám budú slúžiť ako súkromný kľúč, pretože nám umožňuje dešifrovať správu. Dôležité je poznamenať, že bez čísla A a B je pre tretiu stranu skoro nemožné sa dopátrať k týmto číslam, len z čísla N, a to pri dostatočne veľkých prvočíslach. Hovoríme pritom o číslach s niekoľkými desiatkami miest.

Celkovo je jednosmerná funkcia zložitejšia, avšak my sme sa len zamerali a vysvetlili si jej najdôležitejší aspekt, ku ktorému sa trojica dostala. Po prvých písmenách ich priezvisk dostala šifra meno RSA. [23]

Dôležité je spomenúť, že v podobnom čase objavila iná trojica rovnako šifrovanie verejným/súkromným kľúčom a šifrovanie založené na teórii čísel, konkrétne prvočísel, avšak nikto o tom až do roku 1997 nemohol vedieť, keďže trojica Clifford Cocks, James Ellis a Malcolm Williamson pracovali pre nadchádzajúcu inštitúciu Bletchley parku, Government Communication Headquaters (GCHQ). Ellis už v roku 1969 vedel, že šifrovanie verejným/súkromným kľúčom môže v kryptografii existovať, avšak nevedel, ktorá matematická funkcia by na to mohla slúžiť. Až neskôr mu Cocks a Williamson pomohli s matematikou a objavili prvočísla, ako vhodného kandidáta. V roku 1975, dva roky pred

[23] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 253-263. ISBN 978-80-7363-850-4.

objavením toho istého zo strany Adlemana, Shamira a Rivesta, mali celú teóriu okolo šifrovania verejným/súkromným kľúčom kompletnú, avšak verejnosť o nej nemohla vedieť. [24]

1.7 Vznik Cypherpunks[25]

Phil Zimmerman bol kryptografom, ktorý nepokračoval v dobre našliapnutej kariére v Silicon Valley, ale naopak stal sa z neho aktivista. Najskôr ako horlivý aktivista proti jadrovým zbraniam, počas zúriacej studenej vojny medzi Spojenými štátmi a Sovietskym zväzom. Neskôr si začal uvedomovať hodnotu kryptografie v demokratickom režime a úlohu bezpečnosti a súkromia medzi bežnými ľuďmi. Dôvodom bolo to, že dovtedy bola kryptografia z väčšej časti len záležitosťou vlád a ich armád, avšak v 80. a 90. rokoch 20. storočia sa začala dostávať aj medzi bežných ľudí.

V 80. rokoch začal Zimmerman pracovať na softvéri, ktorý by zrýchlil šifrovanie pomocou RSA. Zimmerman si uvedomoval, že problémom šifrovania pomocou verejného kľúča je to, že neviete overiť pravosť odoslanej správy od určitého človeka, pretože váš verejný kľúč je dostupný každému. Vymyslel systém, kde sa kombinuje symetrické a asymetrické šifrovanie spolu s RSA a inou šifrou IDEA (podobná šifra ako DES). Odosielateľ tak posiela druhej strane dve veci:

1. Správu zašifrovanú symetrickou šifrou IDEA
2. Kľúč k IDEA zašifrovaný asymetrickou šifrou RSA

Príjemca tak dostane správu, ktorá je zašifrovaná a rovnako má istotu, že je od konkrétneho človeka. Zo systému plynie aj výhoda, že je rýchlejší, pretože len malá časť informácií je zašifrovaná pomalšou asymetrickou šifrou RSA. Rovnako do softvéru zahrnul nástroj na vytváranie súkromného a verejného kľúča, ktorý prácu používateľom uľahčuje. Rovnako vymyslel digitálne podpisy. Výsledkom bol systém, ktorý dovtedajšie inovácie v oblasti kryptografie zabalil do jedného ľahko použiteľného produktu, ktorý nazval Pretty Good Privacy (PGP).

Zimmerman mal z počiatku problém s vládou USA a so spoločnosťou RSA Data Security, Inc., pretože, ona mala patent na šifru RSA. Zimmerman to ignoroval a v roku 1993

[24] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 263-274. ISBN 978-80-7363-850-4.

[25] SINGH. S. 2017. *Kniha kódů a šifer*. *3. vyd*. Praha: nakladateľstvo Dokorán, s. r. o.; s. 275-297. ISBN 978-80-7363-850-4.

požiadal kamaráta aby nahral softvér na internet ako verejne dostupný pre kohokoľvek. Tento krok vyvolal medzi kryptografmi a neskôr aj medzi laickou verejnosťou rozruch. Na jednej strane kvôli patentu zo strany RSA Data Security, Inc., na strane druhej bol predmetov vyšetrovania zo strany veľkej poroty, pretože FBI tvrdila, že vyváža zbrane, ktoré pomáhajú teroristom. Po troch rokoch v roku 1996 úrad amerického generálneho prokurátora stiahol žalobu a to aj vďaka verejnosti a ostatným kryptografom, ktorí stáli na Zimmermanovej strane.

Zimmerman bol súčasťou tzv. Cypherpunk, z ktorého vzišli aj ostatné inovácie v oblasti kryptografie a pravdepodobne aj Bitcoin a následne kryptomeny.

Cypherpunks bola malá skupina kryptografov, ktorí sa každý mesiac stretávali v San Franciscu od roku 1992. Ich cieľom bolo presadzovať súkromie a bezpečnosť vo vznikajúcej digitálnej dobe v spojení s používaním internetu. Vznikol aj tzv. Cypherpunks mailing list, ktorého súčasťou boli:

- Jacob Appelbaum: Vývojár prehliadača Tor, ktorý slúži na anonymné prehliadanie webu
- Julian Assange: Zakladateľ portálu WikiLeaks
- Dr Adam Back: Tvorca tzv. Hashcash, neskôr zakladateľ spoločnosti Blockstream, ktorá participuje na ďalšom vývoji Bitcoinu.
- Bram Cohen: Tvorca BitTorrent
- Hal Finney: Hlavný autor druhej verzie PGP, tvorca tzv. of Reusable Proof of Work
- Tim Hudson: Spoluautor SSLeay, predchodca to OpenSSL (certifikáty pre web)
- Paul Kocher: Co-author of SSL 3.0
- Moxie Marlinspike: Tvorca Open Whisper systému (vývojár Signal), jedná sa o vývoj aplikácie Signal, ktorá slúži na šifrovanú komunikáciu, či už prostredníctvom správ alebo hlasovo
- Steven Schear
- Bruce Schneier
- Zooko Wilcox-O'Hearn: vývojár DigiCash, Zakladateľ projektu Zcash (kryptomena)
- Philip Zimmermann: Tvorca prvej verzie PGP
- Wei Dai: Vytvoril koncept B-money, ktorý predchádzal Bitcoinu.

Prvým podstatným prvkom pre vznik Bitcoinu bol projekt DigiCash, ktorý vznikol ešte pred skupinou Cypherpunks. Tento projekt založil David Chaum v roku 1989. Jednalo sa o rovnomennú spoločnosť, kde Chaum vymyslel systém na posielanie elektronických peňazí: „Návrh elektronickej meny začal David Chaum realizovať v roku 1990 v Amsterdame založením spoločnosti DigiCash, kde zrealizoval a začal prevádzkovať elektronickú menu ecash s prvou elektronickou platbou uskutočnenou v roku 1994. Po počiatočných úspechoch sa použitie nikdy výraznejšie nerozšírilo, paradoxne pre pohodlné používanie kreditných kariet s absolútne protichodnými vlastnosťami, aké poskytovala Chaumova mena.“[26]

Ďalšou inováciou, ktorá pomohla vzniku Bitcoinu z dielne Cypherpunks bol Hashcash v roku 1997 od Adama Backa, ktorý bol založený na koncepte proof of work (ktorý si vysvetlíme nižšie) a slúžil proti nevyžiadaným e-mailom (spamom).[27]

Ďalším krokom k vzniku Bitcoinu bola práca od vývojára menom Wei Dai, ktorý navrhol koncept B-money. Jednalo sa o jeden z prvých konceptov decentralizovaných a anonymných peňazí. V tomto koncepte popísal systém proof of work (kde by mali niektorí používatelia potvrdzovať transakcie prebehnuté v systéme) a rovnako emitovanie digitálnej meny, ktorej množstvo by malo byť vopred dohodnuté a fungovať na základe nejakého algoritmu. [28][29]

Predposledným konceptom, ktorý ovplyvnil koncept Bitcoinu a vznikol pred ním bol koncept menom Reusable proof of work (RPOW), ktorý predstavil Hal Finney v roku 2004. Koncept bol podobný tomu, čo popisoval Hashcash, avšak tokeny v systéme sa mohli použiť opakovane a preniesť z jednej adresy na inú adresu.[30]

Posledným konceptom, ktorý predstavil Nick Szabo bol Bit Gold z roku 2005, ktorý sa doteraz označuje za predchodcu Bitcoinu, práve kvôli tomu, že sa Bitcoinu a jeho štruktúre najviac blíži. Nick Szabo v tomto koncepte v princípe spojil niekoľko predchádzajúcich konceptov, aby tak nastavil systém, ktorý je čisto decentralizovaný a jeho dôvera neleží na nejakej centrálnej autorite, ktorá by mohla systém ovplyvniť. V tomto koncepte napríklad

[26]GASPER, P. *Bitcoin: technologická a ideologická história*. Kratkespravy.sk [online]. [cit. 29.12.2018]. Dostupné na internete: < https://www.kratkespravy.sk/2017/12/bitcoin-historia/ >

[27]WIKIPEDIA. *Hashcash.* [online]. [cit. 29.12.2018]. Dostupné na internete: < https://en.wikipedia.org/wiki/Hashcash >

[28]WIKIPEDIA. *B-Money.* [online]. [cit. 29.12.2018]. Dostupné na internete: < https://en.bitcoin.it/wiki/B-money >

[29]GASPER, P. *Bitcoin: technologická a ideologická história*. Kratkespravy.sk [online]. [cit. 29.12.2018]. Dostupné na internete: < https://www.kratkespravy.sk/2017/12/bitcoin-historia/ >

[30] Tamtiež

vylepšil RPOW od Hala Finneyho a rozhodol sa, že najlepšie bude, keď sa bude tokeny a ich história, kde kedy boli poslané, reťaziť do tzv. blokov. [31]

1.7.1 Kryptomeny

Na podobnom systéme, ktorý sme popisovali vyššie, teda na systéme asymetrického šifrovania fungujú aj kryptomeny. Na účely tejto práce nebude potrebné rozpisovať podrobne, ako všetko v systéme kryptomien funguje, ale bude nám postačovať vysvetlenie základnej terminológie a logiky, na ktorej systém funguje.

V nasledujúcej časti budeme vysvetľovať kryptomenu Bitcoin, ktorá je prvou kryptomenou a zároveň aj najpopulárnejšou kryptomenou s najväčšou trhovou kapitalizáciou.[32] Koncept bol prvý krát diskutovaný v roku 1998 komunitou ľudí, ktorá bola súčasťou tzv. Cyberpunk mailing listu. Po desiatich rokoch v roku 2008 bol publikovaný The White Paper, kde bol celý koncept popísaný do detailov. Stojí za ním Satoshi Nakamoto, človek alebo skupina ľudí, keďže doteraz sa nezistilo kto stojí za týmto menom.[33]

Bitcoin je založený na dvoch základných kryptografických technológiách:[34]

1. Kryptografická hashovacia funkcia, presnejšie SHA-256 a RIPEMD-160
2. Kryptografia verejných kľúčov, presnejšie ECDSA - Elliptic Curve Digital Signature Algorithm

V sieti všetci medzi sebou komunikujú prostredníctvom správ, ktoré sa nazývajú transakcie. Zvyčajne obsahujú informácie o prevode Bitcoinov z jednej adresy na inú adresu. Vlastníctvo kryptomien je tvorené prostredníctvom digitálnych kľúčov, presnejšie páru verejného a súkromného kľúča a digitálneho podpisu. Súkromný kľúč je generovaný náhodne a užívatelia ho držia v bezpečí mimo dosah niekoho iného, keďže súkromný kľúč nám umožňuje narábať s kryptomenami. Používa sa pri potvrdzovaní transakcie spolu s digitálnym

[31] BITCOIN WIKI. *Nick Szabo*. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://en.bitcoinwiki.org/wiki/Nick_Szabo >

[32] COINMARKETCAP. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://coinmarketcap.com/ >.

[33] STANCEL, D. 2015. *Economic Consequences Of Cryptocurrencies And Associated Decentralized Systems.* Brno: Masaryk, Faculty of Economics and Administrations. s. 17.

[34] STANCEL, D. 2015. *Economic Consequences Of Cryptocurrencies And Associated Decentralized Systems.* Brno: Masaryk, Faculty of Economics and Administrations. s. 10.

podpisom, ktorý potvrdzuje vlastníctvo a pravdivosť odoslanej transakcie s príslušnou sumou bitcoinov. Verejný kľúč je generovaný jednosmernou hashovacou funkciou zo súkromného kľúča. Naopak verejný kľúč je prístupný a viditeľný každému v sieti, pretože prostredníctvom neho sa posielajú bitcoiny tomu ktorému účastníkovi v sieti.[35]

Adresa je jedinečná kombinácia 58 alfanumerických znakov, prostredníctvom ktorej sa posielajú bitcoiny. Následne tieto transakcie sú zabalené do tzv. blokov a navzájom poprepájané, čo vytvára reťaz blokov, teda blockchain.

V nasledujúcej časti si popíšeme pre pochopenie konkrétne fungovanie bitcoinu a jeho blockchainu, a to z pohľadu bežných používateľov a rovnako tzv. minerov, teda ťažiarov, ktorý zabezpečujú sieť.

Fungovanie bitcoinu na užívateľskej úrovni

Zapojenie do siete Bitcoinu a celkovo kryptomien je umožnené každému používateľovi. Používateľ si musí nainštalovať peňaženku do mobilu alebo počítača, ktorá mu vygeneruje pár súkromný a verejný kľúč. Následne mu môže niekto poslať bitcoiny s ktorými môže po potvrdení transakcie narábať. Ako sme spomínali vyššie, jeho verejný kľúč je kombinácia 58 alfanumerických znakov (v skutočnosti Satoshi Nakamoto vylúčil znaky, ktoré sa dajú ľahko zameniť ako Il a 0O)[36] a vyzerá napríklad takto:

1G5wNM3suB2KXkon8LN6MqJtzWyexMju7M

Verejný kľúč je vygenerovaný prostredníctvom jednosmernej hashovacej funkcie zo súkromného kľúča, ktorý by mal používateľ držať v tajnosti a nikomu ho neposkytovať. V prípade hashovania je dôležité zdôrazniť, že keď nejaký objem dát zahashujeme (v Bitcoine konkrétne hashovacia funkcia SHA256), tak to znamená, že nám vznikne odtlačok/podpis z týchto dát alebo informácií. Tento podpis/odtlačok je jedinečný a to znamená, že akokoľvek pozmeníme vstupné informácie, tak sa nám výsledný hash zmení.

V prípade, že používateľ pošle na inú adresu bitcoiny sa v sieti stane toto:[37]

1. Odosielateľ vytvorí transakciu
2. Zoberie dáta z transakcie (identifikátor a ďalšie informácie spojené s transakciou)

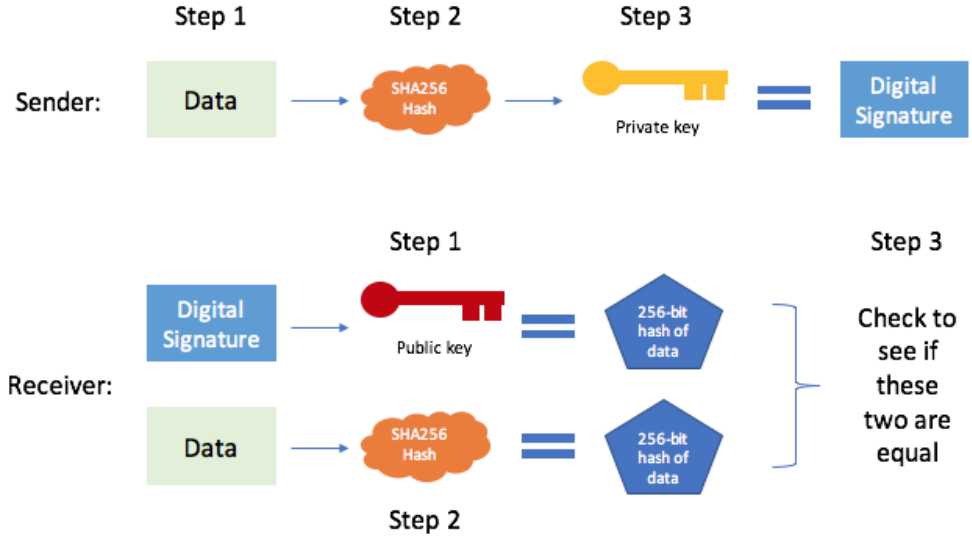
[35] Tamtiež. s.10.
[36] UNIVERSITY OF NICOSIA. *DFIN-511: Introduction to Digital Currencies.* s.13.
[37] UNIVERSITY OF NICOSIA. *DFIN-511: Introduction to Digital Currencies.* s.20.

3. Použije hashovaciu funkciu SHA256, pričom vznikne podpis/odtlačok
4. Podpis/odtlačok zašifruje svojim súkromným kľúčom
5. Odošle zašifrovaný odtlačok/podpis spolu s nezašifrovanými dátami do siete

Na prijímateľovej strane sa udeje toto:[38]

1. Zoberie podpis/odtlačok odosielateľa a použije jeho verejný kľúč na dešifrovanie, pričom mu ostane odtlačok/podpis
2. Zoberie dáta a použije rovnaký postup ako odosielateľ a to znamená, že použije hashovaciu funkciu SHA256, pričom mu vznikne odtlačok/podpis týchto dát
3. V poslednom kroku porovná ním hashované dáta a hashované dáta odoslané odosielateľom.
4. V prípade, že sa tieto odtlačky/podpisy zhodujú, tak to znamená, že nikto nepozmenil pôvodné dáta (v ktorých je zapísané kto komu a koľko bitcoinov posiela) a všetko čo tvrdí odosielateľ je pravda.

Obrázok 9: Postup pri odosielaní transakcie



Prameň: MARSHALL. B.. *How does a bitcoin transaction actually work.* [online]. [cit. 29.12.2018]. Dostupné na internete: < https://medium.com/@blairlmarshall/how-does-a-bitcoin-transaction-actually-work-1c44818c3996 >.

[38] UNIVERSITY OF NICOSIA. *DFIN-511: Introduction to Digital Currencies.* s.21.

Fungovanie Bitcoinu na úrovni minerov/ťažiarov

Fungovanie Bitcoinu na úrovni minerov je odlišné oproti používateľskej úrovni a to z toho dôvodu, že plnia v sieti inú, ale nemenej dôležitú úlohu. Zjednodušene povedané je úlohou minerov udržovať sieť v chode, emitovať nové množstvo bitcoinov do siete a zároveň potvrdzovať transakcie v sieti.

Mineri sú používatelia, ktorý majú nakúpene špeciálne zariadenia na riešenie matematických úloh v sieti, čím emitujú bitcoiny a potvrdzujú transakcie. Bitcoin je nastavený ta, že každých 10 minút sa generuje blok prebehnutých transakcií v sieti, o ktorý sa starajú mineri. Mineri v tom čase zoberú hash, teda odtlačok predchádzajúceho bloku, pridajú časový údaj do bloku a nepotvrdené transakcie v sieti, ktoré si vyberajú na základe poplatku, ktorý zadával odosielateľ pri tvorení transakcie. Blok má obmedzenú veľkosť, to znamená, že sa tam zmestí obmedzená množstvo transakcií a miner chce byť čo najziskovejší. Následne ku transakcii pridá náhodné číslo tzv. nonce a na celý súbor údajov použije hashovaciu funkciu.

Bitcoinová sieť je nastavená tak, že miner porovnáva výsledný hash s hashom generovaným sieťou. V tomto prípade sa musí v prípade hashov zhodovať počet núl na začiatku. V prípade, že sa počet núl nezhoduje, miner mení nonce a opäť použije hashovaciu funkciu až kým sa počet núl vo vzorovom hashy nebude zhodovať. V prípade, že sa nuly zhodujú, blok putuje do blockchainu ako potvrdený a miner dostane odmenu v podobe novo emitovaných bitcoinov a rovnako odmien, ktoré boli zadané v transakciách.

Vlastnosti Bitcoin blockchainu

- Vopred známe množstvo bitcoinov, presnejšie 21 miliónov. V súčasnosti je v obehu skoro 17,5 milióna bitcoinov.[39]
- Generovanie bloku každých 10 minút a s tým spojené emitovanie bitcoinov
- Emitovanie bitcoinov je nastavených v súčasnosti na každých 10 minút vo výške 12,5 bitcoinu. Odmena sa každé 4 roky delí na polovicu.
- Posledný bitcoin by sa mal vyťažiť v roku 2130, avšak jeden z posledných sa vyťaží približne v roku 2030

[39] COINMARKETCAP. [online]. [cit. 30.12.2018]. Dostupné na internete: < https://coinmarketcap.com/currencies/bitcoin/>.

- S narastajúcim výpočtovým výkonom siete (viac používateľov v sieti, alebo lepší výpočtový výkon zariadení). Rastie aj obtiažnosť siete, to znamená, že generovanie blokov je vždy nastavených na každých 10 minút.
- Náročnosť siete sa upravuje každé dva týždne.
- Najmenšia jednotka je tzv. Satoshi, čo je stomilióntina jedného bitcoinu
- Je to open-source projekt, to znamená, že jeho zdrojový kód je voľne dostupný na internete.[40]

Problém byzantských generálov

Pri tvorbe decentralizovaného systému tretej strany, narazíte na základný problém v systéme, ktorým je dôvera. Tento problém sa už rieši desaťročia, pretože je problémom v decentralizovaných systémoch prenášať informácie medzi účastníkmi bez toho, aby niekto v systéme nepodvádzal alebo neklamal. Tento problém sa inak nazýva aj problém byzantských generálov. Prvý krát bol tento problém popísaný v roku 1982 Marshallom Peasom, Robertom Shostakom a Leslie Lamportom.

Problém si môžeme predstaviť ako mesto ktoré oblieha armáda s niekoľkými divíziami, pričom tieto divízie komunikujú medzi sebou iba skrz poslov správ. Velitelia divízií sa musia zhodnúť na čase útoku na mesto. A z toho vzniká problém, či náhodou jeden z veliteľov nebude chcieť sabotovať útok a vyšle inej divízii nepravdivú správu. Preto generáli musia mať nejaký algoritmus, ktorý zaručí, že:

1. Lojálni generáli budú dôverovať algoritmu sa zhodnú na určitom pláne, pričom nebudú brať ohľad na zradcov.
2. Malé množstvo zradcov nemôže spôsobiť to, že lojálni generáli budú súhlasiť s ich plánom[41]

Tento problém rieši práve decentralizovaný systém Bitcoinu. Všetky transakcie v sieti sú potvrdzované tzv. uzlami (v angličtine Nodes) v sieti, ktoré na základe matematických princípov, ktoré sme spomenuli aj v predchádzajúcej kapitole, sa zhodujú na správnosti

[40]GitHub. *Bitcoin.* [online]. [cit. 30.12.2018]. Dostupné na internete: < https://github.com/bitcoin/bitcoin >.

[41] LAMPORT. L.- SHOSTAK. R. - MARSHALL. P. *The Byzantine Generals Problem. Journal ACM Transactions on Programming Languages and Systems (TOPLAS)* Vol. 4 Issue 3, 1982, s. 385. In: STANCEL, D.. 2015. *Economic Consequences Of Cryptocurrencies And Associated Decentralized Systems*. Brno: Masaryk, Faculty of Economics and Administrations.

a aktuálnom stave distribuovanej knihy, teda blockchainu. To znamená, že nikto nemá väčšinovú moc v blockchaine a preto sa Bitcoin nazýva virtuálna peer-to-peer mena. Ktokoľvek si môže stiahnuť Bitcoin core klienta a stiahnuť si celý blockchain (v súčasnosti 235 GB)[42] a začať fungovať ako uzol v sieti, ktorý zabezpečuje verifikáciu a správnosť prebehnutých transakcií.[43]

2 CIEĽ, METODIKA A METÓDY SKÚMANIA

Čiastkovým cieľom diplomovej práce je popísať ako kryptomeny a ich podkladová technológia blockchain funguje. Rovnako popísať ako technologický vývoj v oblasti šifrovania ku kryptomenám dospel. Hlavným cieľom je popísať potenciál kryptomien, aké môžu poskytnúť riešenia na súčasné spoločenské či ekonomické problémy. Zároveň si pritom popíšeme súčasné projekty, ktoré už teraz tieto riešenia poskytujú, alebo na nich pracujú.

Pre potreby diplomovej práce sme v rámci teoretickej časti čerpali najmä z kníh a webových zdrojov, ktoré sa problematike šifrovania venujú. V rámci praktickej časti sme čerpali hlavne z internetových zdrojov, rôznych dokumentov, prezentácií, či webových stránok samotných projektov. Dôvodom použitia týchto zdrojov bolo to, že kryptomeny sú stále mladým sektorom, ktorý sa neustále vyvíja. Odborná literatúra zaoberajúca sa kryptomenami, tak nie je natoľko dostupná ako v rámci iných tém.

V rámci diplomovej práce sme použili tzv. všeobecné metódy, teda metódy vedeckej abstrakcie, metódy analýzy a syntézy. Dôvodom prečo sme použili tieto metódy je, že kryptomeny existujú krátku dobu. Práve preto v diplomovej práci teoreticky popisujeme kryptomeny a s nimi spojené šifrovania a zároveň analyzujeme súčasné projekty, ich vývoj a potenciálny vplyv na ekonomiky krajín.

[42]BITINFOCHARTS. *Bitcoin.* [online]. [cit. 30.12.2018]. Dostupné na internete: < https://bitinfocharts.com/bitcoin/ >.

[43]STANCEL, D.. 2015. *Economic Consequences Of Cryptocurrencies And Associated Decentralized Systems.* Brno: Masaryk, Faculty of Economics and Administrations. s. 17.

3 VÝSLEDKY PRÁCE A DISKUSIA

V rámci praktickej časti načrtneme priamy dopad na ekonomiky a hospodárstva krajín, ktorý už prebieha. Napríklad vo forme kryptomenových búrz, platobných brán, kryptomenových debetných kariet. Rovnako aj vo forme bežných búrz, ktoré poskytujú derivátové nástroje, ktoré sú naviazané na kryptomeny. Následne prejdeme na nepriamy dopad na ekonomiky a hospodárstva krajín. V tejto časti sa najprv pozrieme na potenciálne oblasti využitia kryptomien a blockcainu. V ďalšej časti sa pozrieme na konkrétne projekty, ktoré sa týkajú napríklad decentralizovaného internetu, inteligentných zmlúv v rámci internetu vecí alebo právneho systému. Rovnako aj na projekt, ktorý by mohol niekedy v budúcnosti zrýchliť a zefektívniť systém vyrovnávania platieb medzi bankami.

3.1 Priamy dopad na ekonomiky, ktorý už prebieha

V tejto podkapitole sa pozrieme už na prebiehajúci dopad na ekonomiky, keďže kryptomeny prakticky vytvorili v ekonomike nový podsektor, ktorý patrí pod finančný sektor. Dôvodom je to, že keď chcete vlastniť kryptomeny, tak sa musíte ku nim nejako dostať a nikto vám ich nedá zadarmo, keďže sa obchodujú a sú trhovo ohodnotené. Samozrejme s týmito prevodmi vznikajú rôzne služby, ktoré sú na sektor naviazané.

3.1.1 Ťažba kryptomien

So vznikom prvej kryptomeny Bitcoin vznikla tiež hneď prvá ekonomická činnosť generujúca príjmy, a to tzv. mining alebo ťažba, ktorú sme si opísali v rámci teoretickej časti. Mineri sú v podstate rovnako podnikatelia. Investujú do zariadenia a do elektriny a ostatných položiek, aby mohli profitovať z ťažby tej-ktorej kryptomeny. Tu treba spomenúť, že viac ako polovicu nákladov tvorí elektrina a preto sa väčšina minerov koncentruje vo výhodných oblastiach, kde je nízka cena elektriny. Každá kryptomena má inak nastavený blockchain, tým myslíme náročnosť ťažby. Rovnako sa rôzni typ zariadenia, ktoré miner potrebuje na ťažbu a rovnako sú rôzne nastavené výšky odmien. Záleží aj od toho, koľko minerov už danú kryptomenu ťaží.

Napríklad Bitcoin sa v súčasnosti ťaží s tzv. ASIC (Application Specific Integrated Circuit) čipmi, čo sú špeciálne zariadenia vytvorení čisto na ťažbu bitcoinu a poskytujú najväčšiu efektivitu. Teda vysoký výpočtový výkon, hash rate, za čo najnižšiu cenu. Napriek

tomu, v súčasnosti ťaží bitcoin osamote len málokto. A to preto, že už existuje tzv. pool mining, čo je ťažba v skupine. To poskytuje oveľa väčší hash rate a teda aj pravdepodobnosť na vyťaženie bloku a odmeny, ktorá z toho plynie, a to vo forme emitovaných bitcoinov a rovnako poplatkov od používateľov, ktorí si posielali transakcie. Následne sa odmena rozpočíta pre celý pool a minerov v ňom, ktorí participovali. V súčasnosti v tejto oblasti je najviac minerov z Číny, keďže je tam lacná elektrina pri elektrárňach. Napriek tomu, je ťažné odhadovať presné čísla, pretože pooly sú väčšinou umiestnené v nejakom štáte, avšak pripojiť sa do nich môže prakticky ktokoľvek z kadekoľvek. Stačí že splní podmienky.[44]

Napriek tomu táto ekonomická činnosť nesie so sebou aj určité nevýhody a kritiku. Ťažba kryptomien a konkrétne napríklad bitcoinu spotrebuje veľké množstvo elektriny, keďže táto elektrina je potrebná na prevádzku zariadení, ktoré ťažia bitcoin a prípadne na chladenie týchto zariadení, keďže tieto zariadenia fungujú 24 hodín a 7 dní v týždni. V súčasnosti táto spotreba klesla od konca roka 2018, keďže v priebehu roka 2018 cena bitcoinu klesala. A tak sa niektorým minerom neoplatilo ťažiť a radšej pozastavili činnosť. Tým klesla náročnosť siete a tým pádom aj náklady minerov, ktorí ostali ťažiť. Spotreba elektriny bitcoinu sa odhaduje na približne 50 TWh za rok. To je napríklad spotreba vyššia než ročná spotreba elektriny v Portugalsku. A je to 75% spotreby Českej republiky.[45]

3.1.2 Kryptomenové burzy

Prvou vecou, ktorou každému napadne v prípade zámeny jednej meny za druhú menu, sú zmenárne alebo lepšie povedané burzy. V prípadne kryptomien je systém nastavený rovnako. Hneď od počiatkov začali vznikať kryptomenové burzy, kde ste si mohli zamieňať svoje kryptomeny. V priebehu tohto obdobia sa Mt.Gox dostávala pravidelne do problémov a to kvôli hackerom, ktorí napádali burzu. To je príčinou toho, že tieto typy búrz sú centralizované a to znamená, že nie sú tak odolné voči hackerským útokom ako napríklad samotné kryptomeny.

[44] TUWINER, J. *Bitcoin Mining Pools.* Buy Bitcoin Worldwide. [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.buybitcoinworldwide.com/mining/pools/ >

[45]DIGICONOMIST. *Bitcoin Energy Consumption Index.* [online]. [cit. 16.03.2019]. Dostupné na internete: <https://digiconomist.net/bitcoin-energy-consumption>

Mt.Gox

Prvou kryptomenovou burzou v histórii bola japonská burza Mt. Gox, ktorá vznikla v júli roku 2010. Bola prvou burzou, kde ste si mohli zamieňať kryptomenu za národnú menu, ako napríklad dolár. V období od roku 2010 do 2014 burza obchodovala 70% transakcií, ktoré sa udiali v rámci kryptomeny Bitcoin.[46]

Problémom burzy Mt.Gox bolo, že bola dlhé obdobie jedinou silnou burzou s výrazným monopolom, a tak bola na očiach hackerom, regulátorom a prakticky aj celému kryptomenovému svetu. Burza vo februári 2014 vydáva burza tlačovú správu, kde vyhlasuje bankrot a deklaruje, že jej chýba 850 tisíc bitcoinov, čo bolo v tom čase približne 800 miliónov dolárov. Neskôr majiteľ burzy Mark Karpelès vyhlásil, že na svojom cold wallet (kryptomenová peňaženka, ktorá je väčšinu času offline) našiel 200 tisíc bitcoinov. Toto vyhlásenie prinieslo nádej obchodníkom na burze, ktorí sa v priebehu rokov nemohli dostať k svojim bitcoinom. Neskôr sa ukázalo, že na burze fungoval aj robot Willy, ktorý obchodoval na burze tak, aby mohla burza zarobiť a vykrývať straty počas rokov kedy existovala.[47]

V súčasnosti sa rozhoduje o tom, komu bude strata z veriteľov a užívateľov vyplatená. Z 200 000 bitcoinov sa zatiaľ predal ekvivalent 312 miliónov dolárov a to v prvej polovici roka 2018. Používatelia burzy, ktorí prišli ešte počas fungovania burzy o prostriedky dostali možnosť žiadať odškodnenie. V súčasnosti sa rozhoduje o oprávnenosti žiadateľov a čaká sa na finálny verdikt. Úplné konečné rozhodnutie o vyrovnaní poškodených na burze bolo dané na 26. apríla 2019.

Burzu vlastní v súčasnosti Brock Pierce. Mark Karpelès bol zbavený všetkých obvinení. Mark bol v minulosti obvinený a hrozilo mu dva a pol roka vo väzení so štvorročnou podmienkou. Avšak 15.marca 2019 ho súd v Japonsku oslobodil.[48] [49]

---

[46] TĚTEK, J. *KRYPTO 15: TU MILIARDU DOLARŮ, PROSÍM PĚKNĚ, NECHCI*. [online]. [cit. 16.03.2019]. Dostupné na internete: <https://finmag.penize.cz/investice/335424-krypto-15-tu-miliardu-dolaru-prosim-pekne-nechci>.

[47] Tamtiež

[48] CNN. *Former Mt. Gox chief Mark Karpeles acquitted of most charges in major bitcoin case.* [online]. [cit. 16.03.2019]. Dostupné na internete: < https://edition.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html >.

[49] COINTELEGRAPH*: Mt. Gox Trustee May Have Crashed Bitcoin in 2018 by Dumping It on an Exchange, but There Is Still Hope.* [online]. [cit. 16.03.2019]. Dostupné na internete: < https://cointelegraph.com/news/mt-gox-trustee-may-have-crashed-bitcoin-in-2018-by-dumping-it-on-an-exchange-but-there-is-still-hope >.

Burzy v súčasnosti

Kryptomenové burzy v súčasnosti vyzerajú už úplne inak. Neexistuje v tomto sektore tak silný monopol, ako bol od roku 2010 do roku 2014. Rovnako sú v súčasnosti burzy bezpečnejšie a postupne sa prechádza na koncept decentralizovaných búrz, ktoré by mali byť výrazne odolnejšie voči útokom hackerov. Ďalším faktorom je rastúca regulácia búrz, ktorá by ich mala trestať za nesplnenie regulácií a obmedzovať v nelegálnej činnosti.

V súčasnosti podľa stránky coinmarketcap.com existuje 243 kryptomenových búrz.

„Veľká väčšina je centralizovaná, to znamená, že fungujú ako sprostredkovateľ, teda tretia strana medzi kupujúcim a predávajúcim. Burzy si za obchody a sprostredkovanie pýtajú poplatky, o ktorých si napíšeme neskôr. Na strane druhej existujú aj tzv. decentralizované burzy, ktoré fungujú ako platforma a svoje prostriedky posielate priamo druhej strane a nie cez „tretí účet“ na burze. Zatiaľ je takýchto búrz minimum (napr. Localbitcoins), napriek tomu mám za to, že množstvo decentralizovaných búrz bude rásť. Dôvodom je väčšinou negatívny postoj vlád ku kryptomenám a čoraz väčšia snaha regulovať kryptomeny ich.“[50]

„Väčšina existujúcich kryptobúrz sa vyznačuje zlým zákazníckym servisom či pochybnou vlastníckou štruktúrou a preto sa väčšinou neodporúča posielať prostriedky na tieto burzy. Ďalším problémom pri týchto burzách je likvidita, väčšinou sú to malé burzy, ktoré aj keď ponúkajú veľké množstvo obchodných párov (ktoré sú väčšinou spojené s bitcoinom) nedokážu promptne spĺňať požiadavky obchodníkov. To vytvára takzvaný spread, teda rozdiel medzi dopytovanou a ponúkanou cenou za danú kryptomenu. Spread je tak základným ukazovateľom likvidity konkrétneho menového páru. Po odčítaní nedôveryhodných búrz a tých, ktoré majú všeobecne nedostatočnú likviditu, nám ostane okolo 30 kryptobúrz. Aj medzi týmito burzami existuje silná konkurencie a to v poplatkoch, zalistovaných menových pároch, spoľahlivosti zákazníckej podpory, podmienkach v rámci overovania účtu, ale aj v možnosti pákového obchodovania.“[51]

Samozrejme burzy si účtujú za tieto služby nejaké poplatky, keďže ich primárnym cieľom na trhu je byť ziskový z ich podnikania. A tu sa dostávame aj k samotnému vplyvu na hospodárstvo, keďže vznikol nový sektor kryptomien a spoločností, ktoré s nimi podnikajú.

[50]LINDÁK, M. *Kryptoburzy*. Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/kryptoburzy >

[51] Tamtiež

„Poplatky si burza účtuje v rôznej výške a za rôzne služby. Najčastejším poplatkom, ktorý nájdete na drvivej väčšine kryptobúrz je tzv. maker/taker fee. V preklade je to poplatok za zrealizovanie transakcie, teda obchodu. Rovnako môže burza požadovať poplatky za výber z burzy, keď si vyberáte národnú menu alebo konkrétnu kryptomenu do svojej peňaženky. Tieto dva typy poplatkov sú najbežnejšie a nájdete ich na väčšine búrz. Ďalšími druhmi poplatkov sú špeciálne poplatky za nákup bitcoinu, ktoré účtuje napríklad CEZ.io. Rovnako sú vyššie poplatky pri platbe kartou, keďže táto platba prejde rýchlejšie.“[52]

Ako príklad ziskovosti takýchto búrz môžeme spomenúť súčasnú dvojku na trhu burzu Binance, ktorá mala v 1.štvrťroku 2018 čistý zisk vo výške 200 miliónov dolárov. Pre porovnanie napríklad nemecká najväčšia banka Deutsche bank mala v tomto období čistý zisk vo výške 146 miliónov dolárov. Deutsche bank zamestnáva okolo 100 000 ľudí a existuje už desiatky rokov. Binance v tom čase existovala len 8 mesiacov.[53]

Komerčné burzy poskytujúce deriváty finančného trhu napojené na kryptomeny

Kryptomeny sa s postupným rozvojom etablujú aj na bežných finančných trhoch a burzách. Dlhodobo sa rozhoduje o špecifickej forme finančného nástroja s názvom ETF, teda Exchange Traded Fund. Tie boli horúcou témou najmä v roku 2017 a 2018, keď niekoľko spoločností poslalo požiadavku regulátorovi v Spojených štátoch amerických, konkrétne Americkej komisii pre cenné papiere (SEC). Napriek tomu, sú tieto žiadosti doteraz neúspešné.[54]

Napriek tomu vznikajú iné finančné nástroje, napríklad v roku 2018 sa predpokladá, že zo všetkých hedgových fondov vytvorených v danom roku bolo 20% kryptomenových hedgových fondov, konkrétne naviazaných na Bitcoin.[55]

Jedným z ďalších a najčastejších finančných derivátov napojených na kryptomeny sú futures kontrakty. Dôvodom ich existencie je to, že tie spadajú pod iného regulátora:“ Druhou organizáciou je Commodity Futures Trading Commision (CFTC), jej úlohou je venovať sa burzovým či neburzovým derivátovým obchodom. Pod tohto regulátora spadajú všetci, čo

[52] Tamtiež

[53] WOLF, K. *Větší zisk než celá Deutsche Bank. To je krypto burza Binance*. Roklen24. [online]. [cit. 16.03.2019]. Dostupné na internete: < *https://roklen24.cz/a/SK2hF/vetsi-zisk-nez-cela-deutsche-bank-to-je-krypto-burza-binance* >

[54] LINDÁK, M. *Rok 2018 kapitalizácii kryptomien neprial, ale....* Openiazoch.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://openiazoch.zoznam.sk/cl/191397/Rok-kapitalizacii-kryptomien-neprial-ale >

[55] Tamtiež

spravujú nejaký typ derivátových služieb napojených na kryptomeny. Napríklad CBOE (Chicago Board Options Echange) s jej Bitcoin futures kontraktami alebo CME Group (Chicago Mercantile Exchange Group) s rovnakým produktom.“[56]

Kryptomeny sa čím ďalej tým viac etablujú aj v tejto oblasti, avšak stálym problémom je volatilita týchto aktív. Americká komisia pre burzy a cenné papiere, práve preto nechce schváliť ETF, keďže by to mohlo priniesť príliš vysokú volatilitu na trh.

3.1.3 Ostatné služby, poskytujúce zámenu kryptomien

Kryptoburzy, napriek tomu, že sú inštitúcie s najväčšími tržbami nie sú jediné, ktoré podnikajú vo sfére zámeny kryptomien za národné meny. V tejto časti sa pozrieme na poskytovateľov platobných brán a spoločnosti, ktoré poskytujú kryptomenové debetné karty.

Platobné brány a automaty

Spoločnosti, ktoré poskytujú platobné brány sú špecifické spoločnosti, ktoré poskytujú obchodom, ktoré majú záujem rozhranie. Kamenné obchody, avšak rovnako aj internetové obchody musia mať zmluvu s takouto spoločnosťou. Dôvodom je to, že väčšina týchto záujemcov účtuje v národnej mene, a teda chce mať platbu na svojom účte v eurách a naopak nechce mať napríklad bitcoiny vo svojej elektronickej peňaženke. Platobná brána im to presne zabezpečí. Väčšina platobných brán zvláda najčastejšie Bitcoin, Litecoin, Dash alebo Monero. Samozrejme tieto spoločnosti si za prevod a rovnako používanie platobnej brány účtujú poplatky, na čom oni majú v podstate založený podnikateľský plán.

Podobným spôsobom fungujú aj automaty na zámenu peňazí na kryptomeny. Poskytujú podobné portfólio kryptomien, ktoré môžete nakúpiť. Niekoľko takých automatov už je aj v Bratislave, Košiciach a ostatných väčších mestách. Podobne ako platobné brány zarábajú tieto spoločnosti, ktoré ich prevádzkujú na poplatkoch alebo spreade, čo znamená na mierne rozdielnej cene danej kryptomeny, oproti trhovej cene v tom momente. V týchto automatoch môžete platiť kartou alebo hotovosťou, avšak na Slovensku len do sumy 150 eur, keďže nad túto sumu už musíte poskytnúť osobné údaje. Následne vám stačí QR kód ktorý do automatu načítate, tento kód je identifikátor vašej peňaženky k danej kryptomene, ktorú

[56] LINDÁK, M. *Regulácia kryptomien vo svete a na Slovensku.* Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/regulacia-kryptomien >

nakupujete. Dôležité je poznamenať, že určitá časť automatov fungujú obojsmerne. To znamená, že môžete nakupovať, ale aj predávať kryptomeny.

Kryptomenové debetné karty

Kryptomenové debetné karty fungujú ako obyčajné bankové debetné karty, ktoré väčšina ľudí denne používa.

„Druhou možnosťou ako platiť kryptomenami sú špeciálne debetné platobné karty. Existuje niekoľko spoločností, ktoré umožňujú si „nabiť" kartu kryptomenou, ktorú vydavateľ karty podporuje. Následne sa pri samotnej platbe daná čiastka zamení na burze a obchodníkovi zaplatíte v danej národnej mene. Pri využití tejto možnosti je potrebné počítať s poplatkami, keďže ide väčšinou hlavný biznis vydavateľa karty.

Okrem poplatkov sa sleduje, či karta podporuje anonymitu alebo musíte dodať svoju totožnosť pri registrácii. Rovnako sú dôležité poplatky pri výbere z bankomatu, denné limity, či cena karty a ročný poplatok spoločnosti za správu. Rovnako je dôležité v akých krajinách môžete vyberať z bankového automatu peniaze a rovnako v akej mene.

Z pohľadu obchodníka to neznamená nič nové, pretože jemu prídu peniaze priamo v národnej mene a on si ani nevšimne, že niekto platil kryptomenou."[57]

Problémom týchto kariet je stále to, že celkovo sektor kryptomien je stále do veľkej miery neregulovaný alebo legislatívne prostredie je nejasné a rozdielne medzi jednotlivými štátmi Európskej únie (EÚ), ale aj ostatných štátov mimo EÚ.

„Na pôde Európskej únie v súčasnosti neexistuje jednotný postoj k regulácii kryptomien, ktorý by sa vyžadoval od každého štátu, to znamená, že každý štát definuje kryptomeny vo svojej legislatíve rozdielne. Najviac sa štáty zhodujú v tom, že kryptomeny neodporúčajú používať a že ich nepovažujú za skutočné peniaze či menu, keďže oficiálnou menou je euro. A rovnako na dani z pridanej hodnoty (DPH) v spojení s kryptomenami, keďže o tej rozhodol Európsky súdny dvor. Napriek tomu s rastúcim využitím kryptomien aj táto otázke nie je uzavretá."[58]

[57]LINDÁK, M. *Kryptoburzy*. Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/platenie-bitcoinom-kryptomenami >

[58]LINDÁK, M. *Kryptoburzy*. Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/regulacia-kryptomien >

Preto je prostredie podnikanie s kryptomenovými debetnými kartami rizikové. To sa potvrdilo aj začiatkom roka 2018, keď vydavatelia kariet ako Visa či Mastercard oznámili zákaz činnosti spoločnosti Wave Crest.

„Nad budúcnosťou kryptokariet je však veľa otáznikov. Dôvodom je najmä ich regulácia. Najmä v Európe v januári zatriasli trhmi oznámenia kartových spoločností, ako Visa či Mastercard. Obe oznámili zákaz činnosti WaveCrest, ktorá väčšine spoločností poskytuje kryptokarty. Medzi tieto spoločnosti patrila Bitwala, Xapo, Wirex, TenX a Cryptopay. Napriek zákazu sa už objavili nové spoločnosti alebo zasiahnuté spoločnosti zmenili politiku a stále je možnosť pre používateľov používať bitcoinové debetné karty.“[59]

To už nie je úplne aktuálne, keďže článok pochádza z mája roka 2018. Napriek tomu, zákaz a negatívny postoj voči spoločnostiam pretrváva a v nasledujúcej tabuľke ukazuje spoločnosti, ktoré fungujú a poskytujú služby v tejto oblasti aj v spojitosti s kryptomenami.

[59]LINDÁK, M. *Kryptoburzy*. Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/platenie-bitcoinom-kryptomenami >

Tabuľka 1: Spoločnosti poskytujúce kryptomenové debetné karty

Názov	Mena	Cena karty	Poplatky	Potreba osobných údajov pri registrácii	Podporované krajiny	Výber z ATM	Denný limit výberu z bankomatu
Bitnovo	BTC, EUR, BCH	20€	-	Nie	EHP	1 €	500 €
Revolut	GBP, EUR, USD, spolu s LTC,BTC a ETH, avšak tie sa nedajú posielať mimo Revolut peňaženky	6€	Zadarmo/premium 8€ za mesiac	Nie	EHP	200€ mesačne zdarma/potom 2% z výberu	200€ mesačne zdarma/potom 2% z výberu
Wirex	USD, EUR, GBP, BTC, LTC, XRP, ETH, WLO	Zdarma, potom mesačne 1,2€	Zadarmo	Nie	EHP	2€	250€ na deň

Prameň: Vlastné spracovanie podľa údajov jednotlivých spoločností.

Prienik kryptomien aj do kartového sveta je zatiaľ v rámci finančných inovácií otázny, keďže kryptomeny stále nie sú jednotne regulované, tak ako sme spomínali vyššie. To spôsobuje to, že spoločnosti sa do tohto podnikania radšej nepúšťajú po predchádzajúcej skúsenosti a radšej majú hlavné podnikanie v bežných platobných kartách a službách, ktoré následne čiastočne prepoja s kryptomenami.

3.2 Nepriamy dopad na ekonomiky

V nasledujúcej časti sa pozrieme na potenciálne oblasti využitia, kde by kryptomeny alebo blockchain mohli nájsť uplatnenie a v tom prípade šetriť náklady alebo priniesť niečo

inovatívne. Samozrejme veľa projektov je zatiaľ v rovine úvah alebo začiatkov. Napriek tomu sa už nájdu aj úspešné lastovičky.

3.2.1 Potenciálne oblasti využitia kryptomien a blockchainu

Decentralizovaná peer-to-peer databáza má široké využitie v praktickom živote či už bežného človeka, podnikateľa alebo verejnej správy. A to nie len v zmysle meny. Tu treba zdôrazniť, že nasledujúce oblasti využitia sa nepripisujú len Bitcoinu, ale hlavne kryptomenám a technológii blockchain všeobecne. Dôvodom je to, že Bitcoin v súčasnosti nie je technologicky nastavený na to, aby dokázal naplniť všetky nižšie spomínané oblasti. Medzi potenciálne oblasti využitia patrí:

1. **Finančný clearing** – „Jednou z možností využívania kryptosystémov vo finančnom svete, nad ktorou sa intenzívne uvažuje, je ich využitie na potreby zúčtovania svetového obchodovania. Náhrada dnes už „staromódneho“ mechanizmu SWIFT.“[60] Na takomto riešení pracuje tím za kryptomenou Ripple. Cieľom Ripple Labs je spolupracovať s nadnárodnými bankami a zrýchliť a zlacnieť cezhraničné prevody.[61]
2. **Finančné služby** – „Kryptosystém Bitcoin je pre súčasné obchodovanie titulov na burzách relatívne pomalým systémom. Overovanie transakcie každých 10 minút nie je dostatočné pre dnešný systém vysokofrekvenčného obchodovania, ktoré prebieha v milisekundách. Avšak už dnes uvažujú viacerí nad vznikom tzv. side chains, samostatne fungujúcich registrov, ktoré by neboli obmedzované relatívne pomalou infraštruktúrou bitcoinu. Umožňovali by rôzne druhy obchodovania s tým, že bitcoin – ako najdôveryhodnejší systém – by sa používal len na clearing medzi obchodníkmi, kde je 10 minútová frekvencia dostatočná.“[62]
3. **Blockchain na internet vecí** – Internet vecí si vyžaduje silnú infraštruktúru, ktorá nebude napadnuteľná. Predstavte si, že máte

[60]POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.5.

[61] LINDÁK, M. *Súperenie Bitcoinu, či 700-percentný rast meny Ripple*. Hospodárske noviny[online]. [cit. 16.03.2019]. Dostupné na internete: <https://finweb.hnonline.sk/komentare-a-analyzy/941934-superenie-bitcoinu-ci-700-percentny-rast-meny-ripple-komentar-dna >

[62] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.6.

inteligentné zariadenia po celom dome, na diaľku môžete sledovať vlhkosť vzduchu, teplotu, spotrebu elektriny, či vašu chladničku, či tam máte dostatok potravín. Všetky tieto zariadenia by museli vysielať dáta na internet a následne do vášho telefónu. Na to potrebujete bezpečný prenos, a uloženie dát, ktoré by nemohol nikto napadnúť.

4. **Upisovanie akcií na blockchaine** – „V súčasnosti je značne náročné zrealizovať úpis akcií alebo akýchkoľvek iných inštrumentov na burze. Nie je to samozrejme nemožné, avšak úkon je často finančne i procesne náročný. Nie však vo svete kryptosystémov. Úpis akcií, majetkový záznam k nim a ich obchodovanie na decentralizovaných trhoviskách je pravdepodobne jedna z ďalších oblastí, v ktorej budú kryptosystémy už čoskoro využívané.“[63]
5. **Decentralizované internet či úložisko dát** – „Každý sa už určite stretol s informáciami o tom, že niektorým spoločnostiam unikli osobné dáta klientov. Pri využívaní decentralizovaných aplikácií sa to už stať nemôže. Niektoré projekty uvažujú dokonca tak ďaleko, že dáta sa budú nielen bezpečne ukladať (automatické kryptovanie), a omnoho rýchlejšie vyvolávať zo siete, ale bezpečnosť internetu sa posunie na úplne novú úroveň, čo je využiteľné pri zabezpečovaní webových stránok, elektronickej komunikácie vo finančnom systéme, či samotnej elektronickej komunikácii. Tieto a podobné vlastnosti sú cieľom napr. projektu MaideSafeNet.“[64]
6. **Verejné obstarávanie** – práve verejné obstarávanie a transparentnosť či korupcia sú najdiskutovanejšími témami, keď sa spomenie verejná správa. „Verejné tendre organizované vládnymi agentúrami môžu byť transparentnejšie, zautomatizované a samo vynútiteľné použitím tzv. smart kontraktov (inteligentných kontraktov), ktoré by mali na starosť celý proces. Transparentnosť by bola dosiahnutá aj samotným faktom, že pri zverejňovaní verejných kontraktov by bola využívaná technológia blockchainu (Bitcoinu alebo jeho špecializovaného derivátu). Týmto

[63] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016 s.6.
[64] Tamtiež

spôsobom by si každý vedel overiť, či tender vyhrala naozaj najlepšia ponuka. Zároveň nie je nevyhnutné zverejniť identitu všetkých zúčastnených, pokiaľ to nie je žiaduce. Všetky ponuky môžu byť pseudo-anonymné, nakoľko adresy v blockchaine nemusia mať zverejnenú reálnu identitu, ktorá za nimi stojí. Napriek tom by ktorýkoľvek z účastníkov tendra mohol poskytnúť nepochybný dôkaz prepojenia jeho reálnej a virtuálnej identity prostredníctvom digitálneho podpisu.

Automatizácia obstarávania by sa dala zvýšiť až do takej miery, kedy smart kontrakt automaticky vyberie najvýhodnejšiu ponuku (napr. najmenej nákladnú) po vypršaní doby určenej na prijímanie ponúk. Následne ďalší, podmienený (escrow) kontrakt môže ošetriť vyplatenie odmeny až po splnení podmienok ukotvených v predchádzajúcom kontrakte. Odmena sa uvoľní po tom, čo dostane input od poverenej autority (či autorít). V prípade, ak by dodávateľ nedodal dohodnuté služby alebo tovary, finančné prostriedky by boli automaticky vrátené naspäť zadávateľovi verejného obstarávania. V prípade splnenia služby či dodania tovaru by uchádzač mohol automaticky získavať i referencie, ktoré by mohli byť následne využívané v ďalších verejných obstarávaniach (napr. v zmysle § 34 súčasného zákona č.343/2015 Z. z. o verejnom obstarávaní).

V rámci takéhoto fungovania verejného obstarávania by mohli mať uchádzači rovnako uľahčené napr. preukazovanie splnenia ostaných podmienok (napr. v zmysle §26), kedy by systém plnenie podmienok kontroloval a automaticky pod..“[65]

7. **Notárske zápisy –** „Prevod majetku. Vlastnícke tituly. Potvrdenia. Dohody. Závete. Pre realizáciu týchto druhov záznamov môže byť využívaná technológia blockchainu. Výsledkom je bezpečný záznam bez možnosti jeho zmeny a tým pádom s maximálnou mierou zabezpečenia autenticity, či s dostatočnou mierou transparentnosti. Notársky zaznamenané dáta na základe kryptosystémov môžu byť následne využívané pre ďalšie úkony a

[65] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.7.

ich aplikáciu pri automatizácii platieb, prevode majetku, či automatizácii úkonov bez zásahu človeka. Príkladom môže byť automatické naplnenie podmienok závetu, prevod vlastníctva majetku na základe vopred definovaných podmienok plnenia (napr. realizácia platby za kupovaný majetok), či automatické naplnenie sankcií pri neplnení zmluvných vzťahov, a pod..“[66]

8. **Registre –** „Využitie blockchain technológie si môžeme predstaviť aj pri vytváraní a používaní akýchkoľvek druhov verejných registrov. Používanie údajov bude zodpovedať kritériám nemeniteľnosti, zaručenej autenticity a nenapadnuteľnosti, zároveň však s poskytnutím dostatočnej miery súkromia i transparentnosti. Dané údaje budú zároveň kedykoľvek prístupné akýmkoľvek elektronickým zariadením. To rieši mnohé problémy, ktoré dnes so sebou nesú súčasné IT riešenia.“[67]

3.2.2 Potenciálne alebo fungujúce projekty v rámci využitia kryptomien či blockchainu

Finančný clearing

Keď chceme hovoriť o finančnom clearingu, tak musíme jednoznačne hovoriť o zatiaľ najrozvinutejšom projekte z oblasti kryptomien, o projekte Ripple. Ripple (XRP) je konkrétne názov kryptomeny v tomto projekte. Projekt vznikol v roku 2012, ktorého cieľom bolo od začiatku internetové platby lacnejšími, a to v prípade zmeny či spracovania transakcie. Rovnako je cieľom skrátiť časové obdobie medzi odoslaním a prijatím transakcie. V princípe tak Ripple funguje ako premosťovacia mena medzi národnými menami.

Množstvo ľudí z komunity kryptomien nepripisuje Ripplu veľkú hodnotu, a to z dôvodu, že nie je typickou kryptomenou. A to preto, že napríklad Ripple má vopred už emitované množstvo tokenov (XRP) a neťaží sa podobne ako napríklad pri Bitcoine. Rovnako o potvrdzovanie transakcií sa stará okrem finančných domov, hlavne jeho materská spoločnosť Ripple Labs. A to je skôr centralizovaný systém než decentralizovaný.

[66] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.7-8.

[67] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.8.

Na obranu Ripple Labs, ale treba spomenúť, že síce spoločnosť vlastní 60% emitovaných tokenov, avšak postupne ich predáva prostredníctvom smart kontraktu (inteligentnej zmluvy), kedy sa určité množstvo po určitom čase uvoľňuje na trh.

V súčasnosti Ripple Labs spolupracuje s viac ako 200 bankami a finančnými inštitúciami. Medzi jeho hlavné výhody patrí rýchlosť transakcie, jej cena, ktorá je nízka a rovnako to, že banky nemusia držať veľké prostriedky v rámci settlementu a tzv. nostro účtov, kde údajne banky držali celosvetovo v roku 2016 päť biliónov dolárov.[68]

Inteligentné zmluvy

Inteligentné zmluvy sú jedným z najrevolučnejších prvkov kryptomien. Inteligentné zmluvy alebo Smart Contracts sú špeciálne nakódované malé programy. Sú to vopred nakódované kontrakty, kde v prípade splnenia/nesplnenia podmienok prebehne určitá transakcia alebo výmena. Zjednodušene si to môžeme prirovnať ku automatu na kávu, rovnako keď splníme určité podmienky, teda hodíme mincu a stlačíme tlačidlo, tak nám vyhodí pohár a nasype napr. čokoládu, ktorú zaleje horúcou vodou a následne zapípa, aby sme si mohli čokoládu zobrať. Podobne fungujú aj inteligentné zmluvy.

Ako platforma pre tieto zmluvy a kontrakty slúži trhová dvojka, kryptomena Ethereum. Ona poskytuje blockchain, na ktorom sa dajú vytvárať inteligentné zmluvy. Zatiaľ najznámejším príkladom využitia inteligentných zmlúv na blockchaine Etherea bolo tzv. ICO, teda Initial Coin Offering. ICO je špecifickým nástrojom, ktorý sa v určitých veciach podobá na Initial Public Offering (IPO), keď veľké spoločnosti prídu na burzu a začnú verejne predávať akcie. Napriek tomu tu je niekoľko odlišností.

ICO je špecifickým nástrojom na získavanie prostriedkov na rozbeh projektu. Väčšinou začínajúce spoločnosti či projekty prídu s ICO, kde ponúknu určité množstvo tokenov za určitú cenu a investori majú možnosť prostredníctvom Etherea, tokenu kryptomeny Ethereum, nakúpiť ľubovoľné množstvo tokenov daného projektu, prostredníctvom ktorých prispejú na rozvoj projektu. ICO si získalo rýchlo popularitu, pretože do neho mohol vstúpiť ktokoľvek, kto mál počítač a pár eur, ktoré bol ochotný zameniť za kryptomeny. Aj preto bolo

[68]SILKJAER, T. *14 Common Misunderstandings About Ripple And XRP*. Forbes[online]. [cit. 16.03.2019]. Dostupné na internete:< https://www.forbes.com/sites/thomassilkjaer/2019/03/07/14-common-misunderstandings-about-ripple-and-xrp/amp/?__twitter_impression=true&fbclid=IwAR3J4DANblc--zl4a271AEKgcZZ8aLPYzdQmG6nS0LjMSXpUurIPgLEMygQ>

veľké množstvo projektov podvodmi, ktoré v konečnom dôsledku sa nikam nedostali. V roku 2016 sa prostredníctvom ICO vyzbieralo približne 100 miliónov dolárov. V roku 2017 to bolo 6 miliárd dolárov a v roku 2018 až 20 miliárd dolárov. [69]

V súčasnosti sa skôr hovorí o prepracovanejších ICO, kde by inteligentné zmluvy uvoľňovali prostriedky pre vývojárov postupne, podľa toho či by spĺňali vytýčené ciele v projekte.

Ďalšími potenciálnymi oblasťami využitia inteligentných zmlúv je napr. právo, kde sa hovorí o projekte Kleros.[70] Ten využíva inteligentné zmluvy na zlepšenie arbitrážnych rozhodnutí. Napríklad, keby zákazník chcel od remeselníka vyrobiť stoličku. Všetko sa zapíše do inteligentnej zmluvy, v prípade spokojnosti zákazníka sa odomknú prostriedky v inteligentnej zmluve a pošlú sa remeselníkovi. V prípade nespokojnosti, rozhoduje o kvalite produktu a splnení/nesplnení podmienok zadaných v inteligentnej zmluve anonymný tribunál, zložený z používateľov siete. Tí sú motivovaní finančnou odmenou rozhodnúť spravodlivo.

Inteligentné zmluvy môžete využiť napríklad aj pri správe rôznych registrov, alebo manažovaní zásob v skladoch v rámci veľkých spoločností. Podobne ich môžete použiť aj napríklad pri schvaľovaní hypotéky, kde by smart kontrakt zobral dáta o vašej bonite, hodnote nehnuteľností a ostatných faktorov, na základe ktorých by vám poskytol alebo neposkytol požadovanú sumu.

Registre

Projektom, o ktorom sa najviac hovorí v tejto oblasti je projekt, kryptomena Factom.

„Projekt Factom existuje od septembra 2015 a je zameraný na tvorbu a správu registrov, či databáz. Názov Factom pochádza z latinského slova Factum, ktoré v preklade znamená: „čo je uvedené, je skutočné.“ Factom je kryptosystém, ktorý využíva blockchain Bitcoinu a nedávno i Etheru (iná kryptomena) pre bezpečné ukladanie záznamov alebo dát. Zápis dát môže realizovať verejná alebo súkromná inštitúcia. Dáta zapísané do systému

[69]LINDÁK, M. *Rok 2018 kapitalizácii kryptomien neprial, ale....* Openiazoch.sk [online]. [cit. 17.03.2019]. Dostupné na internete: < https://openiazoch.zoznam.sk/cl/191397/Rok-kapitalizacii-kryptomien-neprial-ale >

[70] KLEROS. Dostupné na internete [online]. [cit. 17.03.2019]. < https://kleros.io/ >

Factom sú nezmazateľné a nemenné. Dáta nie sú ohrozené žiadnou treťou stranou napr. v podobe útočníka (hackera) a sú dôveryhodné.“[71]

Samozrejme, keďže Factom je kryptomenou, tak nesie so sebou špecifiká, ktoré sú odlišné od bežných cloudových služieb. „V prípade kryptosystému Factom musí verejná inštitúcia pri tvorbe databázy postupovať nasledovne. Po prvé musí nakúpiť menu Factomu – tzv. factoidy. Factoid môžeme prirovnať k bitcoinu, čiže ho môžeme chápať ako finančnú jednotku – token systému. Nakúpené factoidy drží v zabezpečenej elektronickej peňaženke. Následne za factoidy nakupuje práva na ukladanie dát do systému. Týmito právami sú tzv. entry kredity.“[72]

Tu treba spomenúť, že systém Factom je drahší než bežné cloudové riešenia, avšak naopak mal by byť bezpečnejší. Napriek tomu nikto nevie, či raz cloudové riešenia v cene neprekoná a nebude lacnejší.

V súčasnosti vývoj Factom projektu stále prebieha, avšak niektoré jeho prvky už fungujú. Na webe majú spomenuté riešenia v rámci autentifikácie dokumentov alebo produktov, rovnako riešenie pre banky a hypotekárny biznis alebo pre autentifikáciu zariadení v rámci internetu vecí. Na prevádzku a vývoj využíva príspevky od investorov, napríklad aj z Bill & Melinda Gates Foundation.[73]

Internet vecí

Oblasťou, kde sa rovnako môže presadiť technológia blockchain je internet vecí, ktorý sme spomínali vyššie. V tejto oblasti je najznámejším projektom IOTA. Projekt bol vytvorený v roku 2015, pričom o rok neskôr bol systém kompletný a boli vychytané všetky najväčšie chyby. Prostriedky na vývoj získali čiastočne prostredníctvom ICO. Špecifikom projektu je, že tokeny tzv. MIOTY sa neťažia a ich množstvo v obehu je vopred známe na úrovni 2 779 530 283. Blockchain je špecifický, pretože tu nefunguje ťažba. Presnejšie sa nazýva Tangle. Tangle funguje tak, že keď zariadenie internetu vecí vyšle transakciu do siete, najprv musí potvrdiť dve iné neznáme transakcie, ktoré boli v sieti skôr, až následne môže byť jeho transakcia potvrdená. Týmto sa autori chceli vyhnúť problémom napr. Bitcoinu, pri ktorom pri

[71] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.8.

[72] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016. s.8.

[73] KHATWANI, S. *A Comprehensive Beginner's Guide to Factom Cryptocurrency*. Coinsutra. [online]. [cit. 17.03.2019]. < https://coinsutra.com/factom-cryptocurrency-fct >

veľkom množstve transakcií sieť nestíha. A rovnako sa dostali k tomu, že čím bude viac zariadení zapojených v sieti, tak tým bude sieť bezpečnejšia a robustnejšia. Tu treba zdôrazniť, že pri IOTE neexistujú poplatky za transakciu, ako je to napríklad pri ostatných kryptomenách. Zároveň sa v rámci projektu pokračuje na rozvoji a ponuke ďalších riešení, ktoré vyriešia bezpečnosť a rýchlosť transakcií.[74]

IOTA má veľký potenciál do budúcnosti, keďže čím ďalej tým viac sa hovorí o zdieľanej ekonomike, internete vecí, priemysle 4.0, či automatizácii. Preto vývojári projektu už nadviazali partnerstvá aj s väčšími spoločnosťami.

IOTA v súčasnosti spolupracuje s Microsoftom na monetizácii dát, ktoré by sa prostredníctvom internetu vecí vyzbierali. Tieto dáta sú cenné pre rôzne spoločnosti alebo výskumníkov z tej ktorej oblasti. Ďalším partnerom je Volkswagen, ktorý pracuje aj na zlepšovaní výrobných procesov, či prenášaní dát rovno do áut bez nutnosti priameho pripojenia. Jedným z partnerov je aj spoločnosť Bosch, ktorá je najväčším dodávateľom automobilových komponentov a rovnako vyvíja a predáva rôznu elektroniku. Jej cieľom je rozvíjať internet vecí a zabezpečiť, aby tieto informácie boli bezpečne prenášané. Na to by im mohla slúžiť v budúcnosti IOTA.[75]

Finančné trhy

Finančné trhy môžeme vnímať z dvoch stránok. Z jednej strany sem patria aj kryptomenové burzy, ktoré sme spomínali vyššie a s nimi naviazané služby napojené na kryptomeny, teda kryptomenové debetné karty či platobné brány. Rovnako tak aj spomínané bežné burzy, ktoré poskytujú deriváty naviazané na kryptomeny.

Druhou stránkou je využitie blockchainu na finančných trhoch, presnejšie technológie, ktorá by bola efektívnejšou platformou, než je tomu v súčasnosti a zároveň by poskytovala dostatočnú bezpečnosť za prijateľnú cenu. Napriek tomu je stále problémom to, ako navrhnúť tento systém, keďže napríklad v prípade Bitcoinu sa mineri starajú o to, aby bola sieť zabezpečená a všetko prebiehalo správne. Rovnako je problémom aj súčasný stav regulácie, ktorá je najmä v prípade finančných trhov a vysporiadania obchodov náročná. Napriek týmto faktom je už niekoľko finančných inštitúcií či búrz, ktoré skúmajú potenciálne riešenia.

[74]DALIBOR. *IOTA (MIOTA).* Kryptomagazin [online]. [cit. 17.03.2019]. < https://kryptomagazin.sk/co-je-kryptomena-iota-a-ako-funguje-tangle >

[75]GRANT, E. *List And Guide Of IOTA Partnerships.* Use The Bitcoin. [online]. [cit. 17.03.2019]. < https://usethebitcoin.com/list-guide-iota-partnerships/ >

Prvou lastovičkou bola burza Nasdaq, ktorá v roku 2015 so svojou technológiou Nasdaq Linq Blockchain Ledger, na ktorom testuje obchodovanie súkromných cenných papierov. V máji roku 2018 oznámil Nasdaq partnerstvo s Citi. Spolu by chceli na blockchain zapisovať platobné inštrukcie a transakcie. Austrálska burza rovnako v roku 2015 oznámila zámer, že by chcela nahradiť Clearing House Electronic Subregister System, čo je elektronický systém na evidenciu a prevod cenných papierov medzi obchodníkmi. Austrálska burza má v úmysle využiť technológiu blockchain. Podobne aj Deutsche Börse spolu s Liquidity Alliance pracuje na vývoji blockchain riešenia, pre cezhraničné transfery cenných papierov. Okrem týchto búrz existuje množstvo ostatných búrz, ako Londýnska, Luxemburská alebo Kórejská burza cenných papierov, ktoré investovali alebo sa podieľajú na vývoji blockchain technológie, ktorá by im zjednodušila činnosti spojené s obchodovaním.

Decentralizovaný internet

Jedným z najznámejších projektov z tejto oblasti je neštandardný kryptomenový projekt Safe network. Samotný projekt vznikol ešte skôr než Bitcoin, a to v roku 2006, avšak vtedy ešte tokeny s názvom Maid Safe coin neexistovali. V konečnom dôsledku Safe Network nebol kryptomenou.

„Je potrebné zdôrazniť, že projekt MaidSafe nie je štandardnou kryptomenou, pretože SAFE Network nemá fungovať na blockchaine. Rovnako tak tu nie sú mineri, ale tzv. farmári, ktorí poskytujú svoje miesto na disku, výpočtový výkon alebo dátové pripojenie pre ostatných, a za to dostávajú token systému, safecoin. Tento systém sa nazýva Proof of Resource a umožňuje sieti overovať akcie a služby pomocou matematicky známeho mechanizmu.

Ak budete chcieť niečo uložiť do SAFE Network, vaše dáta sa rozdelia na menšie časti, zašifrujú sa (self-encryption) a rozdajú rôznym farmárom. Tí nebudú mať k dátam prístup a ani nebudú vedieť, od koho sú, rovnako ako vy nebudete vedieť, kde sa vaše dáta nachádzajú. V systéme nebude existovať rovnaká verzia dát od dvoch používateľov. To znamená, že dáta od druhého používateľa, ktoré sa nahrajú do SAFE Network a budú rovnaké, sa automaticky vymažú. Napriek tomu budú existovať kópie dát, ktoré boli rozdelené, zašifrované a rozoslané viacerým používateľom. Dôvodom je prístupnosť údajov, aby sa k nim majiteľ dostal v prípade napr. vypnutého počítača farmára.“[76]

[76]LINDÁK, M. *SAFE Network (VŠETKO, ČO CHCETE VEDIEŤ) – Projekt sľubujúci decentralizovaný internet.* Alza. [online]. [cit. 17.03.2019]. < https://www.alza.sk/safe-network >

Systém tak bude tvoriť alternatívu k dnešnej verzii internetu, ktorý neexistuje len tak vo vzduchu, ale v dátových centrách s veľkou spotrebou elektriny na chladenie či prevádzku. Rovnako je problémom, že tieto dátové centrá sú centralizované.

MaidSafe coin je v podstate tokenom, ktorý z projektu ako jediný je súčasťou blockchainu a spoločnosť prostredníctvom neho v minulosti získala prostriedky na vývoj. To znamená, že prebehlo vyššie spomínané ICO. V budúcnosti sa počíta s vytvorením ďalšieho tokenu s názvom Safe coin, ktorý by mal fungovať čisto len v rámci systému a mal by sa dať zamieňať len sa MaidSafe coin v pomere 1:1. Tento token bude slúžiť na odmeňovanie vývojárov, farmárov alebo majiteľov aplikácií, ktorí pre ich webový prehliadať niečo vytvoria. SAFE Network by mal byť vo finále internetom 2.0.

3.3 Zhrnutie práce a odporúčania

Na základe spracovanej literatúry, elektronických zdrojov, či tzv. white paperov jednotlivých projektov sme popísali, aký priamy a nepriamy dopad majú alebo môžu mať kryptomeny.

V rámci priameho dopadu kryptomien sme si popísali, ako fungujú kryptomenové burzy, platobné brány, mining alebo kryptomenové debetné karty. Popísali sme si, ako fungujú ich biznis modely a na čom dané spoločnosti poskytujúce spomínané služby zarábajú.

V rámci nepriameho dopadu sme si najprv popísali rôzne potenciálne oblasti využitia kryptomien a technológie blockchain. A to v oblastiach, kde môžu zlepšiť fungovanie a riešiť rôzne spoločenské či ekonomické problémy. Potenciálnymi oblasťami využitia sú rôzne registre, kde by ste mohli zahrnúť napríklad obchodný register, či živnostenský register. Blockchain môžete použiť aj na zapisovanie akcií na burze, či obchodovanie nejakých titulov. Ďalšou potenciálnou oblasťou je internet vecí, kde by fungoval ako podkladová platforma. Rovnako je možné použiť blockchain aj na verejné obstarávania, ktoré sú vo verejnej správe často zmanipulované. V závere tejto časti sme si spomenuli konkrétne projekty, ktoré zo spomínaných oblastí už pracujú na riešení. Medzi projektami sme spomenuli napríklad Kleros, ktorý sa venuje právnemu systému alebo spoločnosť Factom, ktorá rieši spomínané registre. Ďalším zaujímavým projektom, ktorý sme si predstavili je napríklad Safe Network, ktorého cieľom je vytvoriť decentralizovaný internet.

ZÁVER

Cieľom diplomovej práce bolo pozrieť sa na nový fenomén posledných rokov, na kryptomeny a ich potenciálny vplyv na svetové ekonomiky. Aký majú v súčasnosti dopad na trhy a ekonomiky a rovnako, aký ešte môžu mať potenciálny dopad v budúcnosti.

V rámci teoretickej časti sme si popísali fakty spojené s kryptomenami. Začali sme od úplného začiatku kryptomien. Presnejšie od šifrovania, ktoré je základom kryptomien, a ktoré existuje v komunikácii už stovky rokov. Popísali sme tie najjednoduchšie formy šifrovania a postupne sme sa dostali až k počítačom a elektronickému šifrovaniu. V závere sme popísali ako funguje asymetrická kryptografia a hashovacie funkcie. Následne sme túto teóriu prepojili na prvú kryptomenu, Bitcoin. Opísali sme pozadie jeho vzniku a rovnako fungovanie v rámci technológie blockchain.

V praktickej časti sme sa pozreli na priamy dopad kryptomien na ekonomiky krajín. V rámci nepriameho dopadu sme načrtli potenciálne oblasti, kde by mohli mať kryptomeny a technológia blockchain uplatnenie. Teoreticky existuje množstvo oblastí, kde by mohol blockchain šetriť náklady a automatizovať alebo zefektívniť už zabehnuté procesy. Či už je to oblasť rôznych registrov, finančných trhov a búrz alebo oblasť vymáhania spravodlivosti. Následne sme si ukázali priamy dopad kryptomien a s tým spojeného podnikania, do ktorého patria rôzne burzy alebo platobné brány ale aj konkrétne projekty a oblasti, kde už sa vyvíjajú riešenia, kvôli zefektívneniu súčasných procesov.

Kryptomeny majú na ekonomiky krajín priamy dopad už teraz, a to vo forme rôznych biznis modelov. Napríklad kryptomenových búrz, platobných brán, či kryptomenových debetných kariet. Z môjho pohľadu bude v budúcnosti kľúčové, ako sa štáty postavia ku kryptomenám. Napriek tomu, že kryptomeny dokážu fungovať nezávisle od akejkoľvek autority, stále existujú nejaké premostenia, kde sa stretáva digitálny svet kryptomien s reálnym svetom. Takýmto bodom sú napríklad kryptomenové burzy. V súčasnosti je problémom, že napríklad na pôde Európskej únie neexistuje jednotný postoj ku kryptomenám a jednotná regulácia. Je pravdou, že príliš obmedzujúca regulácia môže škodiť, avšak v tomto prípade by aspoň jednotnejšia úprava pomohla, keďže podnikatelia v tejto oblasti by vedeli lepšie plánovať svoje podnikanie.

BIBLIOGRAFICKÉ ODKAZY

Knihy a monografie

SINGH. S. 2017. *Kniha kódů a šifer*. 3. vyd. Praha: nakladateľstvo Dokorán, s. r. o.; 382. ISBN 978-80-7363-850-4.

Ján Skalka, Cyril Klimeš, Gabriela Lovászová, Peter Švec, *Informatika na maturity a prijímacie skúšky*, Enigma, Nitra 2007, ISBN 978-80-89132-50-8

STANCEL, D. 2015. *Economic Consequences Of Cryptocurrencies And Associated Decentralized Systems*. Brno: Masaryk, Faculty of Economics and Administrations.

LAMPORT. L.- SHOSTAK. R. - MARSHALL. P. *The Byzantine Generals Problem*. Journal ACM Transactions on Programming Languages and Systems (TOPLAS) Vol. 4 Issue 3, 1982,

Elektronické dokumenty

STANEK. M.. Kryptológia. [online]. [cit. 28.12.2018]. Dostupné na internete:< http://www.dcs.fmph.uniba.sk/~stanek/Kryptologia%20v1b.pdf>.

Jan Přikryl. *Jemný úvod do kryptografie*. [online]. [cit. 28.12.2018]. Dostupné na internete :< http://euler.fd.cvut.cz/predmety/y2kk/kzk-krypto-uvod.pdf >

TASR. *Podľa najnovších výskumov je vesmír starší o 80 miliónov rokov*. [online]. [cit. 28.12.2018]. Dostupné na internete: < http://skolskyservis.teraz.sk/zaujimavosti/vyskum-vesmir-vek-sonda-planck/2122-clanok.html>

GASPER, P. *Bitcoin: technologická a ideologická história*. Kratkespravy.sk [online]. [cit. 29.12.2018]. Dostupné na internete: < https://www.kratkespravy.sk/2017/12/bitcoin-historia/ >

WIKIPEDIA. *Hashcash*. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://en.wikipedia.org/wiki/Hashcash >

WIKIPEDIA. *B-Money*. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://en.bitcoin.it/wiki/B-money >

BITCOIN WIKI. *Nick Szabo*. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://en.bitcoinwiki.org/wiki/Nick_Szabo >

COINMARKETCAP. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://coinmarketcap.com/ >.

UNIVERSITY OF NICOSIA. DFIN-511: Introduction to Digital Currencies.

MARSHALL. B.. *How does a bitcoin transaction actually work*. [online]. [cit. 29.12.2018]. Dostupné na internete: < https://medium.com/@blairlmarshall/how-does-a-bitcoin-transaction-actually-work-1c44818c3996>.

GitHub. *Bitcoin*. [online]. [cit. 30.12.2018]. Dostupné na internete: < https://github.com/bitcoin/bitcoin >.

BITINFOCHARTS. *Bitcoin.* [online]. [cit. 30.12.2018]. Dostupné na internete: < https://bitinfocharts.com/bitcoin/ >.

TUWINER, J. *Bitcoin Mining Pools. Buy Bitcoin Worldwide.* [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.buybitcoinworldwide.com/mining/pools/ >

CNN. *Former Mt. Gox chief Mark Karpeles acquitted of most charges in major bitcoin case.* [online]. [cit. 16.03.2019]. Dostupné na internete: < https://edition.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html >.

COINTELEGRAPH*: Mt. Gox Trustee May Have Crashed Bitcoin in 2018 by Dumping It on an Exchange, but There Is Still Hope*. [online]. [cit. 16.03.2019]. Dostupné na internete: < https://cointelegraph.com/news/mt-gox-trustee-may-have-crashed-bitcoin-in-2018-by-dumping-it-on-an-exchange-but-there-is-still-hope >.

LINDÁK, M. *Kryptoburzy*. Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/kryptoburzy >

WOLF, K. *Větší zisk než celá Deutsche Bank. To je krypto burza Binance.* Roklen24. [online]. [cit. 16.03.2019]. Dostupné na internete: < https://roklen24.cz/a/SK2hF/vetsi-zisk-nez-cela-deutsche-bank-to-je-krypto-burza-binance >

LINDÁK, M. *Rok 2018 kapitalizácii kryptomien neprial, ale....* Openiazoch.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://openiazoch.zoznam.sk/cl/191397/Rok-kapitalizacii-kryptomien-neprial-ale >

LINDÁK, M. *Regulácia kryptomien vo svete a na Slovensku*. Podnikajte.sk [online]. [cit. 16.03.2019]. Dostupné na internete: < https://www.podnikajte.sk/financny-manazment/regulacia-kryptomien >

POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. *Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore*. NADÁCIA F.A. HAYEKA 2016.

SILKJAER, T. *14 Common Misunderstandings About Ripple And XRP*. Forbes[online]. [cit. 16.03.2019]. Dostupné na internete:< https://www.forbes.com/sites/thomassilkjaer/2019/03/07/14-common-misunderstandings-about-ripple-and-xrp/amp/?__twitter_impression=true&fbclid=IwAR3J4DANblc--zl4a271AEKgcZZ8aLPYzdQmG6nS0LjMSXpUurIPgLEMygQ >

KLEROS. Dostupné na internete [online]. [cit. 17.03.2019]. < https://kleros.io/ >

KHATWANI, S. *A Comprehensive Beginner's Guide to Factom Cryptocurrency*. Coinsutra. [online]. [cit. 17.03.2019]. < https://coinsutra.com/factom-cryptocurrency-fct >

DALIBOR. *IOTA (MIOTA)*. Kryptomagazin [online]. [cit. 17.03.2019]. < https://kryptomagazin.sk/co-je-kryptomena-iota-a-ako-funguje-tangle >

GRANT, E. *List And Guide Of IOTA Partnerships.* Use The Bitcoin. [online]. [cit. 17.03.2019]. < https://usethebitcoin.com/list-guide-iota-partnerships/ >

LINDÁK, M. *SAFE Network (VŠETKO, ČO CHCETE VEDIEŤ)* – Projekt sľubujúci decentralizovaný internet. Alza. [online]. [cit. 17.03.2019]. < https://www.alza.sk/safe-network >