**МЕЃУНАРОДЕН СЛАВЈАНСКИ УНИВЕРЗИТЕТ**

**Гаврило Романович Державин**

**Факултет за технички науки и информатика**




# Втора генерација крипто валути, (Proof-of -Stake), консензус протокол и паметни договори

*-Магистерски труд-*

**Ментор:**

Проф. д-р Орце Симов

**Студент:**

Сашко Митковски М238010

**Свети Николе, 2025**

# Содржина:


Вовед ... 4

1.Криптовалути ... 7

1.1.Дефиниција на криптовалути ... 7

1.2.Историски развој на криптовалутите ... 10

1.3. Предности и недостатоци на користењето криптовалути ... 16

1.4. Извор на криптовалути ... 17

1.5. Целта на криптовалутите ... 18

1.6. Криптовалутите како инвестициски објект ... 19

1.7. Делење на криптовалутите по генерација ... 20

1.8. Прва генерација Биткоин ... 20

1.9.Конкуренти на пазарот на криптовалути ... 23

1.10.Сајбер безбедноста и криптовалутите ... 25

1.11.Споредба на пазарите на криптовалути и традиционалните пазари на капитал ... 27

1.12.Предности и недостатоци на инвестирање на пазарот на криптовалути ... 29

1.13.Криптовалутите во иднина ... 33

2. Платформи за криптовалути од втора генерација ... 35

2.1.Етереум ... 36

2.2.Историја ... 37

2.3. Рударење на Ethereum ... 38

2.4.Карактеристики ... 39

2.5. Употреба и потенцијал ... 41

3. Што се децентрализирани апликации ... 42

-Развој на DApp: моменталната слика ... 43

-Колку токени се поврзани со Ethereum? ... 43

Операција ... 47

Карактеристики ... 48

Трендови ... 49

4. Механизми за консензус ... 50

4. 1. Доказ за работа (Proof-of-Work) ... 51

4.2. Доказ за удел (Proof-of -Stake) ... 52

4.3. Доказ за изминато време (Proof-of –Elapsed-Time) ... 53

4.4. Доказ за авторитет (PoA) (Proof-of-Authority) ... 54
4.5. Доказ за важност (PoI) ( Proof-of-Importance) ... 55
4.6. Доказ за капацитет (Proof-of-Capacity) ... 56
4.7. Доказ за согорување (Proof-of-Burn) ... 57
4.8. Споредба на механизми за консензус ... 58
5. Паметни договори ... 60
5.1. Создавање паметни договори ... 64
5. 2. Извршување паметни договори ... 64
5.3. Интеграција на паметни договори ... 64
5.4. Правен статус на паметните договори ... 66
5.5. Финализирање на паметниот договор ... 67
5.6. Како функционираат паметните договори ... 67
5.7. Безбедност на паметните договори ... 68
5.8. Децентрализиран систем ... 70
5.9. Улога во реалниот свет ... 71
5.10. Предности и недостатоци на паметните договори ... 72
5.11. Безбедносни проблеми ... 73
5.12. Разлика од паметните правни договори ... 74
6. Програмски јазик Solidity ... 74
6.1. Намена и основни карактеристики ... 75
7. Блокчејн технологија ... 75
7.1. Структура на блокчејн ... 76
7.2. Основни видови блокчејни ... 79
7.3. Како функционира блокчејнот ... 81
7.4. Ограничувања на блокчејнот ... 83
Заклучок ... 85
Користена литература ... 88

## Вовед

Криптовалутите доживеаа експоненцијален раст во 2018 година, привлекувајќи многу инвеститори кои се надеваат на обновен раст и брза краткорочна добивка. Втората генерација криптовалути доаѓа како надградба на првата генерација. Криптовалутите што овозможуваат лесна конструкција на паметни договори и децентрализирани апликации се нарекуваат криптовалути од втора генерација. Целта е да се користи блокчејн технологијата во некои други можности што одат надвор од опсегот на дигиталните валути. Гледајќи само од аспект на дигиталните валути, целта беше да се подобри скалабилноста, или да се зголемат и забрзаат трансакциите. Најпознатиот претставник на втората генерација криптовалути е Ethereum. Оваа платформа воведува децентрализирани апликации и таканаречени паметни договори, технологии што ги прават трансакциите побрзи и побезбедни. Ethereum е криптовалута од втора генерација, воведена во 2015 година. Нејзин творец е руско-канадскиот програмер Виталик Бутерин, кој се откажал од колеџ за целосно да се посвети на развојот на етереум, верувајќи дека блокчејн технологијата ќе го промени светот. Тој не се сомневал во моќта на блокчејн и сите негови придобивки, туку видел дека главната книга (список на сите трансакции на мрежата на Биткоин) има многу поголем потенцијал отколку само складирање на трансакции. Тој верувал дека блокчејн може да реши проблеми што се јавуваат во деловните и животните ситуации. Тој исто така сфати дека му е потребен послободен блокчејн што ќе им овозможи на потенцијалните програмери да градат апликации користејќи блокчејн технологија, бидејќи сегашниот дизајн на блокчејнот на Биткоин не нуди многу простор за развој. Тој го спореди велејќи дека мрежата на Биткоин е како калкулатор, а Етереум е како паметен телефон. Тој исто така ја основа Фондацијата Етереум, која е група програмери и аналитичари кои работат на проширување на мрежата и основната технологија.[1]

Етереум е децентрализирана блокчејн платформа за градење апликации, додека Етереум е криптовалутата што се користи на оваа платформа. Може да се користи за секаков вид трансакција или договор. Во пракса, се користи за секаков вид активност што има економски или управувачки аспект. Со пониски трошоци од алтернативните компании што вршат трансакции (Paypal, Skrill и слично), Етереум е децентрализиран, без измами, брз, безбеден и отпорен на цензура.

[1] https://www.cryptonewsz.com/why-did-buterin-create-ethereum/23077/, 2019.

Додека блокчејнот на Биткоин се користи за трансакциски дејства, блокчејнот на Етереум се користи и за трансакциски дејства, но исто така и за креирање на dApps и паметни договори. За да креира децентрализирани апликации и „договорни“ паметни договори, Етереум го лансираше својот програмски јазик наречен Turing-complete, кој креира апликации и договори и каде што корисниците креираат свои произволни правила за да постават некои од нивните услови или правила „едноставно со пишување логика во неколку редови код“.[2]

Паметен договор е термин што се користи за компјутерска програма за олеснување на размена на нешто како што се пари, акции, недвижен имот или нешто друго што претставува размена на вредност. На пример, сакаме да му платиме на Марк да ни печати визит-картички, а тоа чини 5 биткоини. Сепак, не можеме да бидеме апсолутно сигурни дека ќе го добиеме она за што сме платиле. Затоа, во наш интерес е да склучиме договор што би ни овозможил да бидеме сигурни дека ќе добиеме визит-картички откако ќе платиме. Овие паметни договори ги поставуваат условите за да се случи некоја активност и се исто така одговорни за извршување на договорените правила и обврски. Паметните договори се автоматски извршени линии на код што се складираат на блокчејнот и содржат однапред одредени правила. Кога правилата се исполнети, овој код е решен и се обезбедува излез. Наједноставно кажано, ова се програми што се извршуваат во формат креиран од авторот или според правилата поставени од сопственикот. Паметните договори имаат најголема цел во склучувањето деловни соработки со согласност на двете страни. Тие се исполнети со апсолутно детални услови што ги потврдуваат страните вклучени во договорот. Ова го намалува ризикот од измама и кражба, а бидејќи не е вклучена трета страна, трошоците се намалуваат.[3]

Етереум е децентрализиран систем за креирање апликација. Сето ова бара многу компјутерска моќ и електрична енергија, а тоа се сите трошоци. За да ги покрие овие трошоци, Етереум го издава Етер, решение за проблемот со плаќањето. Се третира како дигитална криптовалута, но фундаментално се смета за „гориво“ за апликации на децентрализираната мрежа на Етереум. Исто така, рударите го добиваат како награда

[2] http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, str. 13., 2019.

[3] https://hackernoon.com/everything-you-need-to-know-about-smart-contracts-a-beginners-guide-c13cc138378a, 2019.

за разни активности што бараат рударење на мрежата на Етереум, но е малку поинакво од рударењето на мрежата на Биткоин. Употребата на етер зависи од компјутерската моќ на околината и времето потребно за обработка на одредена трансакција или постапка. Колку е покомплицирана активноста, толку се поголеми наградите.[4]

Етерот е исто така блокчејн систем каде што трансакциите се евидентираат во блокови и се јавно достапни. Како и во случајот со Биткоинот, Етерот може да се купи преку онлајн берзи или берзи. Има ограничена годишна понуда на крипто пазарот од 18 милиони етери годишно. Во крипто светот, Етерот се нарекува кралица на криптовалутите бидејќи е втор по големина по пазарна капитализација.

[4] https://www.investopedia.com/terms/e/ether-cryptocurrency.asp, 2019.

# 1.Криптовалути

Криптовалутите се дигитална валута, создадена врз основа на знаење од криптографијата, математичка дисциплина која се занимава со шифрирање. Нивната главна цел е да се натпреваруваат со државните пари. Нивниот најуспешен претставник е несомнено Биткоинот, кој својата вредност ја стекна главно благодарение на новата блокчејн технологија. Криптовалутите се нов изум на раскрсницата на неколку различни дисциплини - тие комбинираат знаење од монетарната теорија, софтвер со отворен код, дистрибуирани мрежи, криптографија и многу, многу други. Ова е возбудлива област што воопшто не постоеше пред неколку години. Сепак, во краткиот период од своето постоење, криптовалутите станаа предмет на општа дебата, со нивните гласни поддржувачи и често дури и погласни противници или критичари.[5]

## 1.1.Дефиниција на криптовалути

Иако ова може да изгледа малку веројатно, дефиницијата за криптовалути е доста сложена и може значително да се разликува меѓу авторите. Ова главно се должи на фактот што бројот на криптовалути се зголемува со текот на времето и поединечните валути често се разликуваат повеќе или помалку во нивните карактеристики. На пример, Европската банкарска управа излезе со дефиниција во 2014 година дека криптовалутата е виртуелна валута, односно дигитална форма на вредност што не е издадена или контролирана од која било централна банка или друг државен орган и со посредство на нејзиното тргување, складирање и пренос е исклучиво електронски. Иако оваа дефиниција може да изгледа точна, таа е премногу широка и вклучува средства различни од криптовалутите, како што се валутите издадени од компанијата како централна власт, вклучувајќи ги Egold, Liberty Reserve и Linden долари. Затоа, дефиницијата мора да биде поширока и поконкретна, така што само криптовалутите и ништо друго да минуваат низ имагинарното сито. На пример, други автори ја класифицираат криптовалутата и под електронски генерирана и складирана валута, а потоа ја дефинираат криптовалутата како вид на дигитална валута која се потпира на

[5] Vigna, P., & Casey, M. J. (2015). Cryptocurrency: how Bitcoin and digital money are challenging the global economic order. *(No Title)*.

криптографија за поврзување на дигитални потписи на peer-to-peer мрежа и децентрализација.

Друга дефиниција ја опишува криптовалутата како систем кој ги исполнува следните 6 услови:

- На системот не му е потребна централна власт. Дистрибуирано постигнува договор за неговата состојба.
- Системот ги следи единиците и сопственоста на криптовалутата.
- Сопственоста може да се докаже само криптографски.
- Системот дефинира дали може да се создадат нови единици. Ако е така, тој дефинира како и кој ќе стане нивен сопственик.
- Системот ви овозможува да вршите трансакции во кои се менува сопственикот на единицата за криптовалути. Само потврден сопственик може да издаде налог за трансакција.
- Ако две различни трансакции се внесени од една единица, системот извршува само една од нив.

Овие услови се меѓусебно поврзани. Сепак, најважниот услов е оној кој стои зад формирањето на криптовалутите. Меѓутоа, децентрализацијата на валутата има свој степен и е предмет на сите следни услови. Колку е подецентрализирана криптовалутата, толку е помал ризикот ентитетот да може да прекрши некој од другите услови. Покрај тоа, самото отсуство на централна власт ја одредува вредноста на криптовалутите, што е главно поврзано со нејзината репутација. Затоа, загрозувањето на оваа основна состојба може да доведе до значителен пад на вредноста на валутата. Оваа состојба е исто така директно поврзана со последната состојба. Без централна власт која може да ја контролира валидноста на плаќањата, во светот на дигиталните валути се јавува таканаречениот проблем со двојното трошење. Ова е измама која се раѓа кога имателот на дадена валута се обидува двапати да плати со иста „монета“. Биткоинот излезе со нова блокчејн технологија за да го реши овој проблем. Токму ова откритие им даде вредност на криптовалутите.

Криптовалутите претставуваат:

- Слободни пари!;
- Виртуелна валута;
- Peer-to-Peer (P2P) конекција (размената на пари функционира од компјутер на компјутер без потреба од каква било институција);
- Анонимни;
- Нема курсна разлика;
- Нема централна банка, па поради тоа не може да се влијае на валутата;
- Не се зависни ниту од еврото ниту од доларот;
- Можатда се искористат ценовните флуктуации (случај со сите валути);
- Секој може да купи, да продаде и да плати со крипто-валута;
- Сигурниот начин на плаќање се должи на екстремно јакиот метод на енкрипција;
- Нема земја штостои зад оваа валута – па така е ослободена од државно влијание;
- Оваа валута не може да биде „злоупотребена“за политички цели;
- Исто како што има различни валути во светот, така има и различни крипто-валути;
- Не е можна кражба, поради тоа што немаме физичко складирање. Доволен е компјутер. Со оглед на тоа што оваа валута се генерира рандом, не може лесно да се „симне“ (нема кражба на податоци);
- Трансферот се реализира за неколку секунди, 24/7. Нема празници, нема викенди;
- Зад криптовалутите стои крипто-код, поради тоа е ограничена нивната понуда. Не е лесно повторно да се отпечати, како кај хартиените пари. Поради тоа не се предмет на инфлација. Има ограничена достапност, исто како златото и среброто. Затоа штопонудата и побарувачката ја одредува цената на валутата, се очекува пораст на нејзината вредност

Ризици на крипто-валутата се:

- Перформансите зависат од понудата и побарувачката;
- Флуктуација на цената;

- Нема фиксирано курс;
- Сигурност на лозинката(можни се копии/слики од екранот на заднината);
- Доколку нешто негативно се случи, нема кој да се преземе одговорност (ова особено се однесува на децентрализираните криптовалути).

## 1.2.Историски развој на криптовалутите

Криптовалутите се уште се во повој, а нивниот развој започна дури со развојот на Интернетот во 1990-тите. На почетокот, овие валути беа наречени дигитални пари. Ecash стана првата голема криптовалута во 1990 година. Но, нејзината мисија не беше да создаде конкуренција за државни пари, туку да смисли нов и полесен начин на микроплаќања. Меѓутоа, поради недостиг на спонзори, Ecash не успеа да опстојува и банкротираше по неколку години. Други претходници на Биткоин вклучуваат E-gold, Liberty Dollar, Liberty Reserve и e-Bullion. Сепак, тие беа централизирани валути и сето тоа набрзо заврши со апсење на нивните креатори и укинување на валутата од страна на американската влада, која презеде чин на создавање нова валута која се натпреварува со државата, како тероризам или фалсификување државни пари. Друга неуспешна валута што се појави во 1990-тите е CyberCoin. Неговиот крај и последователниот банкрот на компанијата што го лансираше беа поврзани со таканаречениот проблем од 2000 година. Во тоа време, некои компјутери не можеа да го променат датумот од 31 декември 1999 година на 1 јануари 2000 година и наместо тоа се вратија на почетокот на 1900. Сепак, ова предизвика голем број двојно трошење и практично пропаѓање на валутата.

Биткоинот беше наследник на овие неуспешни обиди да се создаде криптовалута. Неговото потекло датира од 2008 година, кога неговиот автор Сатоши Накамото го регистрираше bitcoin.org. Системот стапи во функција една година подоцна, кога првата единица, сега позната како Genesis, беше минирана од самиот Сатоши. Неколку дена подоцна, се случи првата трансакција со биткоин, кога 10 биткоини беа испратени до Сатоши, еден од првите развивачи на системот, Hal Finney. Биткоинот оттогаш станува се повеќе познат на општеството. Првиот израз на цената на Биткоин во однос на американскиот долар беше создаден и на страниците за дискусија, врз основа на потрошувачката на енергија што се користи за негово извлекување. Првата размена на

биткоини за долари се одржа на 12 октомври 2009 година и броеше вкупно 5050 биткоини за помалку од 5 долари.[6]

Оттогаш, целиот крипто свет порасна на речиси 22.500 различни криптовалути со моментална пазарна капитализација што надминува 1 трилион долари. Во основа е поделена на два вида. Првиот тип е самиот Биткоин, кој е најголемата и најпозната криптовалута, а вториот се таканаречените алткоини, кои се сите други криптовалути. Со текот на времето, во крипто светот се формираше одредена фракција на поединци (Биткоин максималисти) кои не признаваат друга криптовалута освен Биткоин. Тие тврдат дека ниедна друга криптовалута нема вистинска употреба и е предодредена да исчезне. Дали ова е вистина или не, само времето ќе покаже. Сепак, доколку големите институции како што се Visa, Mastercard, Starbucks или Adidas си поиграа со оваа идеја, тие немаше да соработуваат со големи проекти за криптовалути. Во денешниот свет на криптовалутите, вклучени се не само компаниите, туку дури и државите.

Друга пресвртница е првата размена на биткоини за вистинска стока, кога на 22 мај 2010 година информатичарот Ласло Ханец размени 10.000 биткоини за 2 пици. Истата година, основана е најголемата берза за биткоини, Mt. Gox[7]. Биткоинот почна да се прифаќа од серверот Викиликс за да плати за спонзорски донации, па дури и беше создаден првиот базен за рударење. Биткоинот продолжи да расте и на почетокот на 2011 година достигна паритет со американскиот долар и неговата вредност постојано растеше. До средината на годината, пазарната капитализација на Биткоин веќе беше 200 милиони долари. Овој брз пораст го предизвика првиот и најголемиот предизвик во историјата на Биткоин. Во рок од 4 дена, криптовалутата падна за помалку од 70 проценти. Како дел од огромната популаризација на Биткоин, се случија и неговите први кражби (Stroukal, 2018). Во 2011 година беше основан илегалниот анонимен веб-пазар Silk Road, кој главно се користеше за продажба на дрога, а Bitcoin беше главната валута овде. Сите овие настани фрлаат лоша светлина врз валутата во подем, но цената сè уште полека растеше. Почнаа да се појавуваат и првите алткоини.

Друг значаен развој беше услугата од BitPay. Ова им овозможи на трговците лесно да прифаќаат биткоини и потоа да ги разменат за долари по тековниот девизен курс. Во

[6] Yermack, D. (2015). Is Bitcoin a real currency? An economic appraisal. In Handbook of digital currency (pp. 31-43). Academic Press.

[7] Decker, C., & Wattenhofer, R. (2014, September). Bitcoin transaction malleability and MtGox. In European Symposium on Research in Computer Security (pp. 313-326). Springer, Cham.

2012 година, почнаа да се појавуваат сè повеќе трговци, без разлика дали со услуги или со реални стоки, кои беа подготвени да прифатат Биткоин за нивната стока. Беше основано и онлајн казино Биткоин, а можностите за плаќање значително се проширија. Во 2014 година цената осцилира околу 1.000 долари. Во февруари истата година, пак, започнаа проблемите на најголемата берза, Mt. Gox. Таа ги прекина сите селекции, вклучувајќи ги и биткоинот. Откриено е дека берзата физички имала помалку биткоини од сметководителите и берзата банкротираше. Ова се рефлектираше во цената на Биткоин, која падна на речиси 340 долари во текот на годината.[8] Од тогаш, сепак, криптовалутите претежно пораснаа. Се појавија во универзитетската настава и имаше се повеќе места каде што можеше да си ги платиш долговите со нив. Во 2017 година се случи првиот хардвер во рамките на биткоин мрежата и на тој начин Биткоинот беше поделен на две валути, Биткоин и Биткоин Кеш. Главната причина за хардфорк беа различните мислења во заедницата и пристапот кон проширување на блоковите. Во текот на 2017 година, цената повторно нагло порасна на 18.000 долари, а потоа полека опаѓа и последното големо зголемување дојде на крајот од 2020 и 2021 година, кога цената се искачи на неверојатни 60.000 долари, околу кои сега се движи.

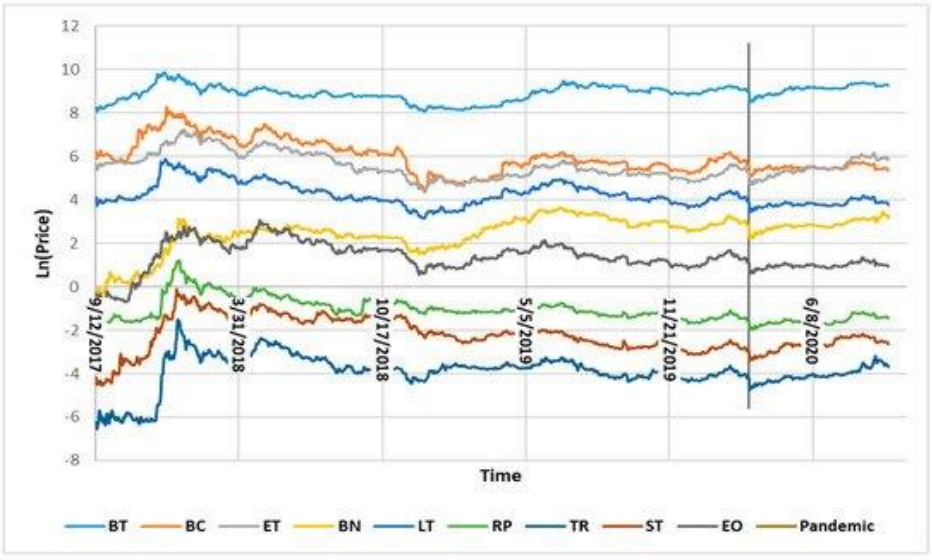
Во 2021 година, Ел Салвадор го воведе Биткоинот како законско средство за плаќање, заедно со американскиот долар. Овој брзорастечки пазар повеќе не е само мала песочна кутија за неколку ентузијасти за криптовалути, туку стана глобален пазар што сите влади, инвестициски фондови и банки мора да го почитуваат и да го сметаат за вистинска предност. Пред години, еден американски бизнисмен и инвеститор даде многу позната изјава дека Биткоинот ќе падне на нула. Легендарниот инвеститор Ворен Бафет е познат и по својот негативен став кон криптовалутите. И сепак, Биткоинот постои и напредува веќе 17 години.

Во студијата на Aysan и сор., (2021) главната цел била да се испитаат меѓусебните односи меѓу најдобрите криптовалути на крипто берзата во присуство и отсуство на пандемијата COVID-19. Деветте избрани криптовалути се Bitcoin, Ethereum, Ripple, Litecoin, Eos, BitcoinCash, Binance, Stellar и Tron, а нивните дневни податоци за затворање на цената се земени од coinmarketcap во периодот од 13 септември 2017 до 21 септември 2020 година. Постојат силни докази за долгорочна врска помеѓу Биткоин и алткоините, без разлика дали е период пред пандемијата или за време на

[8] Stroukal, D. (2018). Can Bitcoin become money? Its money functions and the regression theorem. International Journal of Business and Management, 6(1), 36-53.

пандемијата.[9] Исто така, откриено е дека цените на овие криптовалути и нивната меѓусебна врска се отпорни на пандемијата. Се препорачува кога инвеститорите креираат инвестициски планови и стратегии, тие можат многу да ги земат предвид биткоинот и алткоините заедно, бидејќи тие даваат одржливост и издржливост на долг рок против геополитичките ризици, па дури и во тешкото време на пандемијата COVID-19.

Графикон 1. Заеднички движења на криптовалути




Извор: Aysan, A. F., Khan, A. U. I., & Topuz, H. (2021). Bitcoin and altcoins price dependency: Resilience and portfolio allocation in COVID-19 outbreak. *Risks*, *9*(4), 74.

Криптовалутата е децентрализиран систем за плаќање каде што преносот на сопственост се врши исклучиво криптографски[10]. Криптовалутата се управува преку peer-to-peer компјутерска мрежа, со што се обезбедува нејзината безбедност. Сопственоста на криптовалутите се пренесува преку трансакции. Историјата на трансакциите, како и информациите за сопственоста на криптовалутите, се чуваат во структура на податоци на блокчејн. Секој член на peer-to-peer мрежата го чува целиот блокчејн.

Криптовалутата е поделена на две големи групи: монети и токени. Монетите претставуваат криптовалута со свој блокчејн. Токените не се базирани на блокчејн; тие

[9] Aysan, A. F., Khan, A. U. I., & Topuz, H. (2021). Bitcoin and altcoins price dependency: Resilience and portfolio allocation in COVID-19 outbreak. Risks, 9(4), 74.
[10] Lansky, J. Analysis of cryptocurrencies price development. *Acta Inform. Pragensia* **2016**, *5*, 118–137.

се користат како паметен договор во блокчејнот на друга криптовалута - најчесто, Ethereum. Во февруари 2021 година, имаше над 8600 криптовалути низ целиот свет[11]. Според CoinMarketCap, криптовалутите вклучуваат сè што се тргува на најмалку две берзи, а ги исполнува критериумите на формалната дефиниција за криптовалута. На крајот на февруари 2020 година, најзначајните криптовалути во однос на пазарната капитализација вклучуваа: Bitcoin, Ethereum, XRP, Bitcoin Cash, Bitcoin SV, Litecoin, Tether, EOS, Binance Coin и Tezos. На крајот на февруари 2021 година, тие вклучуваа: Bitcoin, Ethereum, Cardano, Tether, Binance Coin, Polkadot, XRP, Litecoin, Chainlink и Stellar. Во рок од една година, овие промени ја одразуваат нестабилноста на младиот пазар на криптовалути во однос на брзиот развој на технологиите и употребата на овие технологии во пракса.

Табела 1: Табела на криптовалути по вредност и влијание (2025 година)[12]

**Cryptocurrencies**

| Rank | Name | Symbol | Market Cap | Price |
|---|---|---|---|---|
| 1 | Bitcoin | BTC | $2,368,080,386,646 | $118,959.63 |
| 2 | Ethereum | ETH | $557,450,909,355 | $4,618.17 |
| 3 | XRP | XRP | $184,753,303,307 | $3.11 |
| 4 | Tether USDt | USDT | $165,174,264,728 | $1.00 |
| 5 | BNB | BNB | $118,245,955,368 | $848.93 |
| 6 | Solana | SOL | $105,499,464,404 | $195.49 |
| 7 | USDC | USDC | $67,749,327,534 | $0.9998 |
| 8 | Dogecoin | DOGE | $34,460,473,657 | $0.2289 |
| 9 | TRON | TRX | $33,946,585,756 | $0.3585 |
| 10 | Cardano | ADA | $32,884,985,317 | $0.9234 |

[11] CoinMarketCap. Cryptocurrency Prices, Charts and Market Capitalizations. 2021. Available online: https://coinmarketcap.com/

[12] Извор: Coin Market: https://coinmarketcap.com/all/views/all/

Во јануари 2021 година, капитализацијата на пазарот на криптовалути надмина 1 трилион американски долари, а во април 2021 година, дури 2 трилиони американски долари. Само во 2020 година, вкупната капитализација на пазарот на криптовалути се зголеми за 300%.[13] Особено, ова зголемување на каматите е поврзано со економската криза, забрзана од глобалната пандемија COVID-19 и зголемениот интерес од институционалните инвеститори.[14] Овие инвеститори се обидуваат да ги диверзифицираат своите инвестициски портфолија за подобро да ги заштитат своите средства од влијанијата на економската криза.[15] Заедно со зголемениот интерес на овие институционални инвеститори, малопродажните инвеститори исто така ќе станат сè повеќе заинтересирани за тргување со мали количини криптовалути за свои лични потреби. На малите пазари, како што е оној на криптовалутите, малопродажните инвеститори се од големо значење. Оваа статија е исто така фокусирана на нив.

По повеќе од една деценија развој на криптовалутната технологија и нејзините делумно технолошки делови (на пр., блокчејн, децентрализирани технологии), ваквите технологии може да се наречат технологии за општа намена[16]. Технологиите за општа намена може да се дефинираат како технологии кои имаат потенцијал да имаат голем ефект врз општеството преку нивното влијание врз постојните економски, како и општествени структури. Технологијата на криптовалути има таков потенцијал. Со други зборови, овие технологии се на замисленият врв на технолошкиот меур, вклучувајќи „голем број класи на производи или сектори кои ги користат првите на дното“[17]. Затоа, може да се претпостави дека ваквите технологии имаат широка примена и прифаќање во општеството. Во врска со ова, одржливиот развој на криптовалутната технологија, а со тоа и на пазарот на криптовалути, претставува важен аспект.

Одржливоста на понатамошниот развој на пазарот на криптовалути е поврзана со позитивниот став на корисниците. Од една страна, треба да се зголеми прифаќањето на

[13] De Best, R. Market Capitalization of Cryptocurrencies from 2013 to 2020. 2021. Available online: https://www.statista.com/statistics/730876/cryptocurrency-maket-value/
[14] Umar, M.; Su, C.-W.; Rizvi, S.K.A.; Shao, X.-F. Bitcoin: A safe haven asset and a winner amid political and economic uncertainties in the US? Technol. Forecast. Soc. Chang. 2021, 167, 120680.
[15] Mnif, E.; Jarboui, A. COVID-19, bitcoin market efficiency, herd behaviour. Rev. Behav. Financ. 2021, 13, 69–84.
[16] Unalan, S.; Ozcan, S. Democratising systems of innovations based on Blockchain platform technologies. J. Enterp. Inf. Manag. 2020, 33, 1511–1536.
[17] Bresnahan, T.F.; Trajtenberg, M. General purpose technologies “Engines of growth”? J. Econom. 1995, 65, 83–108.

технологијата за криптовалути кај сите сегашни генерации. Од друга страна, усвојувањето на таква технологија од страна на помладите генерации економски активни луѓе мора да се испита и охрабри, бидејќи овие помлади генерации се поотворени за употреба на нови технологии[18] и имаат позитивно влијание врз постарите генерации.[19] Всушност, ова истражување за ставот на потенцијалните корисници може да помогне да се разјасни пристапот на луѓето кон технологијата за криптовалути.

Поради фактот што технологијата за криптовалути е толку нова, оваа студија е фокусирана на најдостапната форма на употреба на криптовалути, т.е. тргување и инвестирање во криптовалути на берзи за криптовалути. Ова главно се должи на поврзаноста на таквите инвестиции со технолошката позадина на користењето на одредена криптовалута. Од долгорочна перспектива, инвеститорите мора да размислат (со алтернативи на криптовалути на Биткоин) дали тимот или заедницата во позадина на технолошкиот развој на одредена криптовалута добро ја вршат работата и дали употребливоста на дадената криптовалута во пракса ќе се подобри во иднина. Само овој пристап ќе го зголеми бројот на нови корисници и ќе ги подобри инвестициите, бидејќи технологиите без корисници ја немаат целта за која се дизајнирани. Од друга страна, од краткорочна перспектива, шпекулативното тргување со криптовалути се базира на медиумски сентимент кој е ограничен во однос на времето и често е ирационален. Одржливоста на криптовалутата не е поврзана со брзиот интерес на инвеститорите (т.н. „економски меур“); таа е поврзана со континуираната употреба и развој на технологијата за криптовалути, вклучително и нејзината употреба во рамките на новите сектори.

## 1.3. Предности и недостатоци на користењето криптовалути

Криптовалутата е технолошки иновативен финансиски инструмент кој значително го прошири своето присуство. Иако носи со себе голем број предности, таа е придружена и со некои недостатоци. Forbes advisor (2023) ги наведува главните предности и недостатоци што се јавуваат при користењето на криптовалути.

Главните предности се:

[18] Vogels, E.A. Millennials Stand Out for Their Technology Use, But Older Generations Also Embrace Digital Life. 2019. Available online: https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/
[19] Taipale, S. Intergenerational Connections in Digital Families; Springer: Berlin, Germany, 2019.

- Децентрализација – оваа предност произлегува од блокчејн технологијата, која овозможува трансакциите да се извршуваат без трети страни и без надзор на централните банки и финансиските институции, и на крајот сето ова води до главната цел, која е насочена кон обезбедување независност од централните власти, намалување на потребата од посредници и со тоа намалување на трошоците за трансакции.
- Брзи и евтини трансакции – брзите и евтини трансакции со криптовалути се овозможуваат преку глобалната мрежа – Интернет, а оваа предност е особено важна бидејќи овозможува трансакциите да се извршуваат со минимални надоместоци.
- Безбедност и транспарентност – технологијата на која се базира целиот крипто свет обезбедува транспарентност и високо ниво на заштита, што сето тоа го отежнува фалсификувањето и манипулирањето со трансакции.
- Лесна достапност – криптовалутата е достапна за сите луѓе кои имаат пристап до Интернет. Оваа предност им овозможува на луѓето без банкарски сметки или други финансиски услуги да учествуваат во глобалниот економски систем.

Клучните недостатоци вклучуваат:

- Висока волатилност – овој недостаток е поврзан со цените на криптовалутите кои имаат драстични флуктуации во кратки временски периоди, што ја прави нивната употреба многу ризична.
- Безбедносни ризици – иако блокчејн технологијата обезбедува исклучително високо ниво на безбедност, крипто светот не е поштеден од хакерски напади и кражби.
- Зависност од технологијата – криптовалутите бараат одредено ниво на разбирање на техничките прашања и пристап до интернет, што во крајна линија е во спротивност со фактот дека криптовалутата е достапна за сите.

## 1.4. Извор на криптовалути

Постојат два вида извори - отворен код и затворен код. Отворениот код е пожелна карактеристика бидејќи му овозможува на секого да го истражи изворниот код, со цел да ја процени неговата функционалност, квалитет, сигурност, да идентификува безбедносни проблеми и слично. За да се поттикне довербата во дистрибуиран

економски систем како што е криптовалутата, повеќето криптовалути се објавуваат како отворен код. Отвореното кодирање во голема мера помогна во ширењето на криптовалутите, а напредокот сигурно би бил побавен доколку програмерите мораа да ја објават својата криптографија. Иако многу корисници на криптовалути веруваат дека сите крипто паричници треба да бидат отворени, ова може да предизвика одредени проблеми. Неодамнешен пример за таква ситуација беше демонстриран за време на хакирањето на валутата Ethereum, кога дури 3,6 милиони етери беа ефикасно исцрпени, што се претпоставува дека е проневера од самиот отворен код.[20]

## 1.5. Целта на криптовалутите

Некои криптовалути се дизајнирани да надминат специфични проблеми, други се дизајнирани да го подобрат користењето на ресурсите, додека други имаат поширока визија што користи комбинации на методи за создавање нови функции и апликации засновани на методологијата на криптовалути. Секоја трансакција со криптовалути вклучува можност за скрипта за креирање интелигенција (т.е. Dobby) што се додава на секоја трансакција. Криптовалутите од прва генерација, како што е биткоинот, обезбедуваат основна можност за скриптирање што се користи за да се обезбеди интегритетот на протокот на трансакции, за секоја конкретна трансакција. Сепак, криптовалутите од втора генерација имаат дополнителни функции што го подобруваат нивото на интелигенција на Dobby, така што попаметното донесување одлуки може да се имплементира без потреба од човечки влез. Идентификувани се три типа криптовалути, според нивните намени:

-1) „Шеми за валути само за трансакции“ (eng. Transaction Only Currency Schemes) имаат за цел да задолжуваат и потврдуваат сметки и да потврдуваат трансакции. Примери за такви системи вклучуваат валути Fiat, Warcraft Gold и Bitcoin.

-2) „Систем за трансакции и апликации“ (англиски: Transaction and Application type) генерално се однесува на криптовалути од втора генерација, каде што покрај можноста за трансакции, криптовалутата има и некаква форма на интегрирана апликација или функција што е корисна надвор од аспектот на трансакцијата со криптовалути.

[20] Bccrwp (2019), Open Source vs zatvoreni izvor za Cryptocurrency novčanike: https://hr.bccrwp.org/compare/open-source-vs-closed-source-for-cryptocurrency-wallets-466458/

-3) таканаречените Turing Complete платформи за развој на апликации од трети страни и дистрибуирана поддршка за апликации, каде што ниеден централен јазол не ја извршува апликацијата.

## 1.6. Криптовалутите како инвестициски објект

Криптовалутите станаа вистинска сензација во финансискиот свет во последните неколку години, и како резултат на тоа, се појави голема љубопитност и внимание од инвеститорите. Инвеститорите ја гледаат криптовалутата како дигитална форма на средства што им отвора бројни можности, што резултира со реализација на потенцијално значајни приноси и диверзификација на нивните портфолија. Генерално, таквата инвестиција е ризична и потребно е внимателно да се анализира ризикот пред да се донесе одлука.

NerdWallet (2023) го наведува следново; инвестирањето во криптовалути носи неколку привлечни карактеристики што се рефлектираат во брзиот раст на вредноста, транспарентноста на трансакциите и можноста за диверзификација на портфолиото, но од друга страна постои висок степен на ризик со овој вид инвестиција, што може да се карактеризира со недостаток на регулатива, безбедносни предизвици и висока волатилност.

Investopedia (2022) наведува неколку клучни точки што треба да се земат предвид пред да се инвестира:

- долгорочна перспектива - долгорочните перформанси на овој пазар се сè уште неизвесни, а инвеститорите треба да ги земат предвид своите финансиски цели и стратешки пристап кон инвестирањето,
- недостаток на регулатива - криптовалутите не се регулирани на ист начин како традиционалните финансиски средства, што ги прави многу поподложни на ризик, манипулација на пазарот, измама и други неправилности,
- разновидност на криптовалути - постојат многу различни криптовалути, секоја со свои карактеристики и намена, а изборот на добра инвестиција бара многу време и напор за темелно истражување и разбирање,
- волатилност - криптовалутите се познати по нивната висока волатилност. Цените на криптовалутите можат драматично да варираат во краток временски период, што може да резултира со брз раст, но и со брз пад на вредноста.

Криптовалутата може да биде профитабилна инвестиција, но исто така носи и значителни ризици. Пред да се одлучи за инвестирање, важно е внимателно да се истражи, разбере и на крајот да се има јасна стратегија и да се постават реални очекувања со цел да се донесе најправилната инвестициска одлука.

## 1.7. Делење на криптовалутите по генерација

Криптовалутите можат да се поделат на три генерации според фазата на развој на блокчејн.

- Прва генерација (на пример, Биткоин)
- Втора генерација (на пример, Ethereum)
- Трета генерација (на пример, Cosmos, Cardano, Polkadot).

## 1.8. Прва генерација Биткоин

Слика 1.Логото на Биткоин



Извор: https://bitcoin.org/en/

Биткоинот е првата успешна криптовалута. Биткоинот е децентрализирана, дигитална валута, која е создадена во 2009 година од анонимен развивач под псевдонимот Сатоши Накамото. Зборовите *„peer to peer“* се однесуваат на компјутерска мрежа во која нема централен сервер низ кој можат да течат сите податоци. Во овие мрежи, според тоа, секој преносен јазол е еднаков и корисниците директно комуницираат меѓу себе (Stroukal, 2018). Како што веќе споменавме, во мрежите без централна власт, се

соочуваме со таканаречениот проблем со двојното трошење. Програмерите на Биткоин најдоа решение за овој проблем со создавање на нова блокчејн технологија. Блокчејн или „синџир блок“ е поврзана листа со врски за блокирање на предците. Под блок подразбираме резиме на потврдени трансакции со одредена големина. Врските се посредуваат со користење на таканаречениот „хаш“ од претходниот блок, така што секој блок има јасно дефиниран предок. Така, овој концепт ви овозможува да ја зачувате историјата на таков начин што таа не може да се препишува, бидејќи ако напаѓачот сака да преработи еден даден блок, ќе мора да ги преработи сите негови предци. Во однос на функцијата, тоа е всушност една голема книга која е јавно достапна за секој корисник. Тие потоа ги потврдуваат трансакциите и на тој начин ја заземаат позицијата на централна банка. Овој систем се нарекува систем заснован на консензус затоа што секој мора да се согласи за една одредена верзија на вистината.

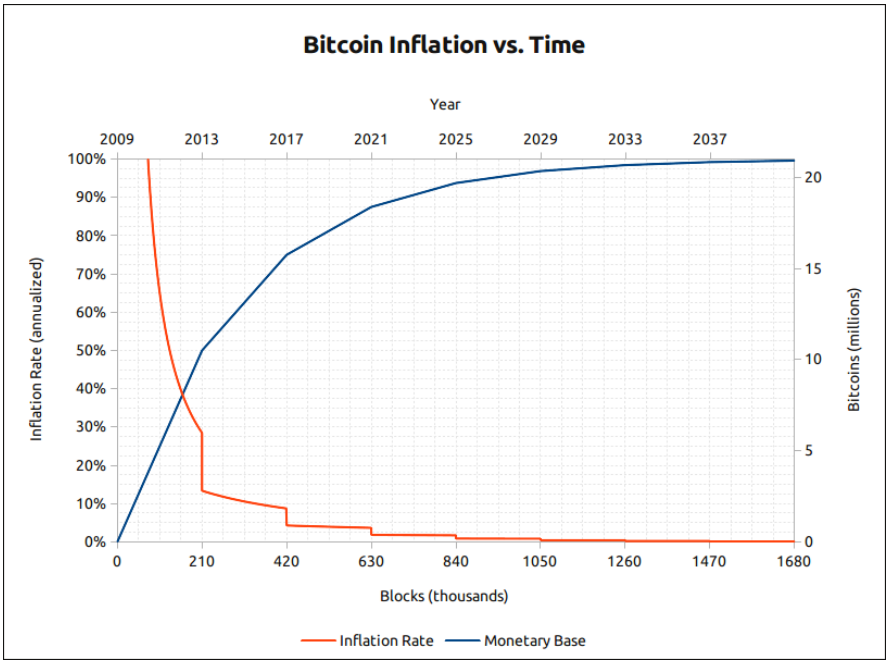
Целиот концепт на потврдување плаќања тогаш функционира како лотарија. За да се ограничи бројот на луѓе на оваа лотарија, лотаријата е условена од потрошувачката на енергија како скапо средство, кое потоа служи како доказ за нивната работа (доказ за работа) за потврда на уплатата. „Играчите“ едноставно се обидуваат да ги користат нивните компјутерски уреди за да генерираат број кој е помал од бројот што математички е изведен од трансакциите што треба да се внесат во книгата. Овој баран број се генерира со помош на функцијата за хаш. Ова е посебен тип на функција која, по внесување на која било низа букви, бројки или други податоци, генерира случаен број, кој е секогаш ист за една дадена низа. Кој прв ќе го најде бројот, добива на лотаријата, а со тоа и право да внесе нова трансакција во заедничката книга, која потоа ја дистрибуира до сите корисници како тековната верзија и ја добива поврзаната награда во форма на провизија за трансакција и ново пронајдени биткоини.

Вкупниот број на биткоини во изворниот код е ограничен на 21 милион од почетокот. Анонимниот автор на оваа валута сакаше да постигне јасно препознатлива реткост на Биткоин и на тој начин да спречи негова девалвација. Затоа, новата валута се генерира со процесот на потврда на плаќањето. Големината на наградата во форма на новопронајдени биткоини се намалува со текот на времето (соодветно се намалува со бројот на постоечки биткоини, каде што во просек се наоѓа по еден хаш на секои 10 минути, и затоа е во основа ист), поточно се преполовува. На почетокот во 2008 година, наградата од 50 биткоини беше заслужна за верификација на трансакцијата;

денес, наградата е само 6,25 биткоини. Според оваа функција, сите биткоини треба да се минираат приближно во 2140 година (https://www.bitcoinblockhalf.com/).

Следниот график го прикажува процесот на развој на генерирањето Биткоин.

Графикон 2. Инфлација на биткоин наспроти време




Целиот процес на оваа лотарија се нарекува рударство и оваа иновација е една од главните причини за моменталната вредност на Биткоин.

Биткоинот е софтвер со отворен код, што значи дека неговиот код е јавно достапен и секој може да го гледа или менува. Модификациите на мрежата може да ги предложи секој преку протоколот BIT (Bitcoin improvement proposal-Предлог за подобрување на биткоин). Ова е документ кој содржи предлози за промени во сегашниот систем. Таквата промена може да биде предложена од секој, а нејзината последователна корист или можна имплементација се занимава со развојниот тим на Bitcoin Core (Bitcoin Core е само името на софтверот што го содржи Bitcoin). За прифаќањето на дадената промена последователно гласаат поединечни рудари, кои го прават тоа за време на рударството со поставување на битови во заглавијата на новооткопаните биткоини. Договорот вообичаено мора да биде најмалку 75% за модификацијата да биде прифатена, или 95% за промена која не може да се врати. Ако промената биде прифатена од рударот, таа ќе биде заклучена и новата верзија на софтверот ќе стапи на сила. Сепак, никој не може да биде принуден да се ажурира низ целата биткоин мрежа.

Затоа, целиот систем на ажурирања е поделен на таканаречен „софтвер“ и „хардвер“. Софтверот е ажурирање без кое системот сè уште работи. Новиот систем е дизајниран да биде компатибилен наназад, а корисниците кои не го прифаќаат системот нема да очекуваат некоја значајна промена освен недостатокот на нова системска функционалност што не можат да ја користат. Сепак, новиот софтвер мора да биде прифатен од сите рудари без чија поддршка новото подобрување не би било возможно, бидејќи никој не би можел да ги генерира изменетите блокови. Поради оваа причина, на рударите им е дозволено да гласаат за нови функции и да отфрлат некои од нив. Доколку некој од рударите не го стори тоа и не го прифати новиот софтвер, нивните новопронајдени блокови ќе се сметаат за неважечки според новиот систем и рударот ќе го изгуби правото на својата награда, што е доволна мотивација да се префрли на новата верзија. Од друга страна, Hardfork е порадикален поради промената и повеќе не дозволува поддршка за постарите верзии, каде што сите корисници обично треба да се префрлат на новиот софтвер. Ако тоа не се случи, старата верзија на софтверот ќе ги смета новите блокови за неважечки и блокчејнот ќе биде поделен на две валути со трајно затворање, чија вредност ќе биде одредена од различна големина и карактеристики на заедницата.

## 1.9.Конкуренти на пазарот на криптовалути

Биткоинот се најпопуларните дигитални пари - се проценува дека вкупниот број на „дигитални монети“ ја надминува вредноста од 853 милијарди долари.

Сепак, далеку од тоа да биде единствениот Биткоин - има многу други конкуренти. Најпопуларните и најпознатите се Ethereum, Tether, XRP и Cardano. Ethereum, кој се базира на технологијата Blockchain, за кратко време достигна вредност од речиси 200 милијарди долари (https://balkans.aljazeera.net/teme/2021/2/9/digitalni-novac-buducnosti).




Слика 2.Покрај Bitcoin, најпопуларни и познати се Ethereum, Tether, XRP и Cardano (EPA)

Криптовалутите најчесто се подредуваат по пазарен удел, што е износот на пари во долари во одредена криптовалута или друг финансиски инструмент. Ако поединецот кој поседува Биткоин одлучи да препродаде одредена сума за X вредности во долари, пазарниот удел на Биткоин ќе се намали за X вредност. Биткоинот се смета за криптовалута која доминира на алтернативни криптовалути бидејќи нејзиниот пазарен удел во моментот на пишување е 169.065.577.529 САД долари е 66,1% од пазарот на криптовалути. Уделот на пазарот може да се потврди со користење на веб-страницата на CoinMarketCap (CoinMarketCap).

Втората најпопуларна криптовалута по удел на пазарот е Етер. Тоа е криптовалута која не е подобрена софтверска верзија на Биткоин, туку има свој посебен блокчејн наречен Ethereum и е верзија на програмабилниот блокчејн. Идејата на мрежата Etherium е да програмира и да изврши паметни договори на неа. Паметниот договор е програмски код испратен до мрежата Etherium (Deployed), кој ги извршува трансакциите без влијание на трето лице, каде што довербата за извршување е загарантирана од Blockchain. На пример, програмскиот код е договор помеѓу две лица и ако се исполнети сите услови од договорот, кодот автоматски ќе изврши стандардна трансакција.

Ether е валута што се користи за плаќање на трансакции на блокчејнот Etherium. Многу честа основа за нови криптовалути е Etherium Blockchain бидејќи е лесно да се работи на нови токени преку паметни договори.

Трета по пазарен удел е криптовалутата Ripple, која всушност е протокол за меѓународни плаќања меѓу банките. Крајната идеја зад валутата Ripple е да се замени тековното решение за трансакции што се користи во банкарскиот свет како SWIFT (Rogina, 2020). Четвртиот по ред е Тетер кој е твз. стабилна монета, чија вредност е секогаш иста во однос на доларот. Тетер е пример за криптовалута која технички воопшто не е бидејќи не користи блокчејн и е централизирана, но многу често се користи во тргувањето со криптовалути. Се користи во ситуации кога сакате да ја одржите стабилната вредност на криптовалутата, односно сакате да го избегнете ризикот од нестабилност на цената на Биткоин или друга профитабилна криптовалута. И покрај постоењето на различни исклучоци, повеќето криптовалути сè уште користат Blockchain технологија за децентрализација на финансиите, односно за создавање криптовалута со идеја таа да биде средство за плаќање или складирање на пари што не е контролирано од трети лица. Некои понови криптовалути се само подобра верзија на постоечките, на пример Litecoin е верзија на Bitcoin што е поевтина и побрза за извршување на трансакциите.

Криптовалутата Dogecoin е создадена како шега, без речиси никаква вредност од 0,04 долари. Името го добило по популарното јапонско анимирано куче Шиба Ину. Популарноста на овој лик набрзо се претвори во вистинска вредност - Dogecoin достигна вредност од дури 10 милијарди долари, а неговата сегашна вредност продолжува да расте со стапка од 6,3 проценти.

Поучени од овој пример, многу јавни личности исто така создадоа свои криптовалути - така што американскиот пејач Акон (Алиаун Тиам) има Акоин, а неговиот колега хип-хоп уметник Лил Јахти има ЈахтиКоин. Иако овие „монети“ моментално имаат исклучително мала вредност, примерот на Dogecoin дава многу надежи за големи профити.

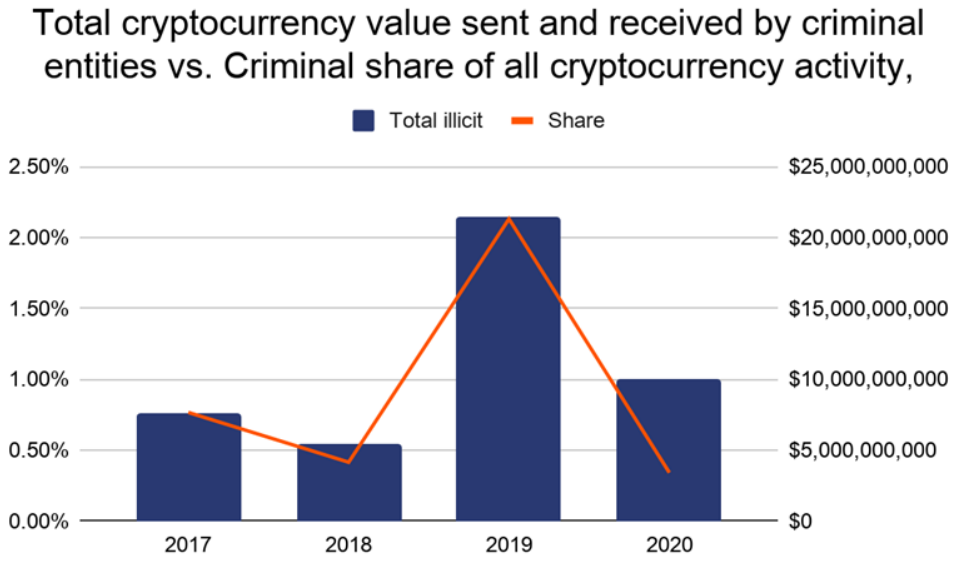
## 1.10.Сајбер безбедноста и криптовалутите

Измамата со криптовалутите стана растечка глобална загриженост, при што различни влади известуваат за зголемување на зачестеноста и загубите од измамите со криптовалути. Помеѓу 2017 и 2018 година, Австралиската комисија за конкуренција и потрошувачи регистрираше зголемување од 190% во загубите за жртвите на измами со криптовалути. Во 2019 година, Управата за финансиско однесување на Обединетото

Кралство издаде предупредување до јавноста откако извештаите за измами со криптовалути тројно се зголемија (Trozze, et.al., 2022). Оваа траекторија на криминалци кои измамуваат поединци кои купиле или извршиле трансакции користејќи криптовалути („корисници“ на криптовалути) сугерира дека просторот на криптовалутите нуди сè уште неискористени можности за криминал.

Брзиот пораст на измамените корисници на криптовалути се чини дека ги надмина соодветните истражувачки напори.

Графикон 3.Chainanalysis: трендови во компјутерскиот криминал поврзан со сајбер криминалот




Извор: https://www.bug.hr/sigurnost/prosle-godine-zabiljezeno-znacajno-manje-kriminala-povezanog-s-kriptovalutama-18422

Во текот на 2019 година, уделот на трансакциите со криптовалути поврзани со разни измами, кражби, финансирање тероризам, заработка од откупнини и други незаконски активности беше 2,1%, или 21,4 милијарди долари во апсолутна вредност. 2020 година и покрај трикратното зголемување на вкупниот износ на трансакции, незаконската активност во криптовалутите беше само 0,34%, или околу 10 милијарди долари (https://www.bug.hr/sigurnost/prosle-godine-zabiljezeno-znacajno-manje-kriminala-povezanog-s-kriptovalutama-18422).

Од оваа сума најмногу отпаѓа на трансакции поврзани со различни криптовалути. По нив следат криптовалутите кои се разменуваат на темна веб-пазари, додека помал удел паѓа на украдени криптовалути и плаќања за откуп поврзани со откуп. Август 2020 година беше најактивен во овој поглед. Во тоа време, таа промени нешто повеќе од 600 милиони долари во криптовалути во светот на сопствениците, сето тоа како резултат на некои измами и други криминални дејствија.

Блокчејн технологијата продолжува да се развива и да наоѓа повеќе случаи на употреба во современиот свет. Една од остварливите области каде што е проучувана и применета е сајбер безбедноста. Блокчејн инфраструктурата ја прави многу практична во справувањето со постојните безбедносни предизвици во областите како што се IoT уредите, мрежите и податоците во преносот и складирањето. Забележано е дека повеќето истражувачи за безбедност на Blockchain се концентрираат многу на усвојувањето на Blockchain безбедност за IoT уредите. Покрај ова, други главни области на безбедноста на блокчејн се мрежите и податоците. Технологијата Blockchain може да се користи за обезбедување на IoT уреди преку посигурни механизми за автентикација и пренос на податоци. Тие можат да ги спречат хакерите да упаднат во овие уреди кои често се испорачуваат со слаби безбедносни конфигурации. Технологијата може да се користи и за обезбедување на мрежи со користење на строга инфраструктура за да се спречат неовластени врски и комуникација (Mathew,2019). И на крај, Blockchain може да обезбеди податоци при пренос и складирање преку шифрирани блокови кои можат да ги отворат само страните кои комуницираат и не се склони кон манипулации. Се проучуваат повеќе случаи на употреба, но овие три го зазедоа централното место. Препорачливо е идните истражувачи да ја разгледаат практичноста на еден блокчејн што може да се користи за развој на безбедносни решенија, бидејќи повеќето од сегашните решенија користат различни блокчејн, па оттука ја попречуваат интеграцијата.

## 1.11.Споредба на пазарите на криптовалути и традиционалните пазари на капитал

Од основањето на Биткоин во 2008 година, криптовалутите станаа сè поважен конкурент на пазарите на капитал и од гледна точка на инвеститорите и од гледна точка на трговците на овие пазари. Создавањето на Биткоин предизвика голема технолошка револуција која за прв пат имаше потенцијал целосно да го наруши

сегашниот финансиски систем. Тоа е токму најпознатата криптовалута која еволуираше од првичното технолошко ветување за нарушување на финансискиот екосистем до најзначајната и најголема конкуренција преку инвестирање на традиционалните пазари на капитал со примена во многу индустрии. Имајќи ја предвид возраста или поточно младоста на пазарот на криптовалути, екстремната нестабилност на цените на криптовалутите и постојаните шпекулативни инвестиции на пазарот на криптовалути, особено во последните години, јасно е дека пазарот на криптовалути почнува да има се поголемо влијание на пазарите на капитал. . За упориште на финансискиот свет се смета гореспоменатата берза на која компаниите позајмуваат капитал со издавање на нивните акции без задолжување или инвеститорите тргуваат со акции за профит. Разликата помеѓу инвеститорот и трговецот се рефлектира во фактот дека тргувањето е обично краткорочно ориентирано каде трговците сакаат да заработат пари со инвестирање врз основа на разлики во цените. Инвеститорите, од друга страна, инвестираат поради долгорочните придобивки врз основа на анализа на финансискиот пазар. Голем број учесници и на пазарот на капитал и на криптовалути се инвеститори кои ги гледаат долгорочните придобивки од инвестирањето на овие пазари, но голем број трговци се повеќе се потпираат на инвестиции на пазарот на криптовалути поради поголемите можности.

Колку е поголема флуктуацијата на средствата, толку е поголем ризикот на средствата и затоа акциите на традиционалните финансиски пазари се сметаат за ризични. Цените на акциите се директно поврзани со перформансите на компанијата што ги издала, а иако има одредени примери, многу е тешко да се предвиди пораст или намалување на цените на акциите. Пазарот на криптовалути е многу поризичен и понеизвесен поради неколку причини. Младоста на пазарот на криптовалути, непостоечката правна инфраструктура и децентрализацијата на пазарот, освен што се споменуваат како позитивни аспекти, влијаат и на високиот ризик на овој пазар. 40

Исто така, пазарот на криптовалути во споредба со традиционалните пазари на капитал е прилично непредвидлив, а тоа може да се види во екстремната нестабилност на цените на криптовалутите, каде што индивидуална голема трговија може значително да ги промени цените на дигиталните валути. Од друга страна, на берзите, поради високата трговска активност помеѓу многу пазарни учесници, големите нарачки вообичаено не влијаат на цените на финансиските средства. Ликвидноста обично се однесува на можноста за брза размена на средствата за пари, но и на леснотијата за

купување или продавање финансиски средства на пазарот без да се влијае на целокупната ценовна стабилност. Кога станува збор за можноста за размена на пари, криптовалутите се уште поликвидни од акциите, а ограничената понуда влијае на способноста да се зачува вредноста на дигиталните валути. Криптовалутите можат многукратно да ја зголемат својата вредност за многу кратко време, но исто така можат да се отстранат исто толку брзо, што е една од најголемите закани, но и можност за инвестирање на овој пазар.

## 1.12.Предности и недостатоци на инвестирање на пазарот на криптовалути

Постојат различни и спротивставени мислења во врска со иднината на криптовалутите воопшто и биткоините особено. Додека, оние со слободарски погледи на животот се оптимисти и го прифаќаат системот на криптовалути, другите автори, економисти и научници од оваа област не се ентузијасти за употребата на криптовалутите во системот на плаќања и финансиски трансакции. Оптимистичкиот поглед на употребата на криптовалутите е поддржан од фактот што тие го олеснуваат преносот на средства помеѓу две страни во трансакцијата; овие трансакции се олеснети преку употреба на јавни и приватни клучеви за безбедносни цели. Овие трансфери на средства се вршат со минимални трошоци за обработка, овозможувајќи им на корисниците да ги избегнат големите провизии што ги наплаќаат повеќето банки. Покрај тоа, многу земји почнаа да го прифаќаат биткоинот како валидна валута. Особено, земјите кои имаат за цел да се ослободат од готовината имаат многу пријателски пристап кон криптовалутите. Аргументот дека промоторите на употребата на биткоин е Пазарна капитализација на биткоин, етереум и други криптовалути, тврдејќи дека пазарот на криптовалути станал многу голем и моќен, па затоа забраната би била скапа за секоја земја. Од друга страна, противниците на криптовалутите тврдат дека криптовалутите се многу нестабилни, може да се користат за перење пари или финансирање нелегални активности. Во овој поглед, Tymoigne (2015) на пример, не е ентузијастичка за користење прекукриптовалути, што дава причини зошто верува дека биткоините не се остварлива електронска валута. Тој забележува дека биткоините се неликвидни и покажале висока нестабилност на цените и дека намалената готовинска вредност на биткоинот е нула. Тој понатаму забележува дека валутата нема централен издавач и дека нема финансиска или економска основа за нејзино создавање. Ивашенко (2016) ги дава предностите и недостатоците на биткоинот како што е наведено подолу.

*Предности*

1. Отворен код за ископување крипто валута – BTC ги применува истите алгоритми што се користат во онлајн банкарството. Единствената разлика на интернет банкарството е откривањето на информации за корисниците. Сите информации за трансакцијата во мрежата на БТК се споделуваат (како, кога), но нема податоци за примачот или испраќачот на монетите (нема пристап до личните информации на паричникот на сопственикот).
2. Без инфлација - максималниот број на монети е строго ограничен со 21 милион биткоини. Бидејќи нема ниту политички сили ниту корпорации кои можат да го променат овој поредок, не постои можност за развој на инфлација во системот.
3. Peer-to-peer криптовалутна мрежа – во таквите мрежи нема главен сервер, кој е одговорен за сите операции. Размената на информации (во овој случај — пари) е помеѓу 2-3 или повеќе софтверски клиенти. Сите инсталирани од корисниците програма-паричници се дел од биткоин мрежата. Секој клиент чува евиденција за сите извршени трансакции и бројот на биткоини во секој паричник. Трансакциите се направени од стотици дистрибуирани сервери. Ниту банките, ниту даноците, ниту владите не можат да ја контролираат размената на пари меѓу нив.
4. Неограничени можности за трансакција – секој од сопствениците на паричникот може да плати на секого, каде било и во која било сума. Трансакцијата не може да се контролира или спречи, така што можете да вршите трансфери каде било во светот каде и да се наоѓа друг корисник со паричник Биткоин.
5. Без граници. Невозможно е да се откажат плаќањата направени во овој систем. Монетите не можат да се лажираат, копираат или трошат двапати. Овие способности го гарантираат интегритетот на целиот систем. Секој месец се зголемува бројот на онлајн продавници, ресурси и компании кои прифаќаат БТК.
6. Ниски трошоци за работа на БТК. Криптовалутата BTC работи како физичка готовина, комбинирајќи ги функциите на е-трговија. Нема потреба да се плаќа провизија и такси на банки и други организации. Главниот дел од таквиот процес е математиката, на која не и се потребни пари. Провизијата во овој систем е помала од кој било друг. Таа изнесува 0,1% од износот на трансакцијата. Оперативните камати одат во паричниците на BTC рударот.

7. Децентрализација. Не постои централен контролен орган во мрежата, мрежата се дистрибуира до сите учесници, секој компјутерски рударски биткоини е член на овој систем. Ова значи дека централната власт нема моќ да диктира правила за сопствениците на биткоини. И дури и ако некој дел од мрежата оди офлајн, платниот систем ќе продолжи да работи стабилно.
8. Лесен за употреба. Имајќи предвид дека постапката за отворање сметка за компанијата во украинските банки е премногу комплицирана и може да се одбие без објаснување, користењето БТК е погодно за компаниите. На компанијата и требаат приближно 5 минути за да создаде паричник БТК и веднаш почнува да го користи без никакви прашања и провизии.
9. Анонимност. Тој е целосно анонимен и во исто време целосно транспарентен. Секоја компанија може да создаде бесконечен број на биткоин адреси без повикување на име, адреса или која било друга информација.
10. Транспарентност. БТК ја чува историјата на трансакциите што некогаш се случиле. Се нарекува секвенцијален синџир на блокови или блокчејн. Блок синџирот чува информации за сè. Значи, ако компанијата јавно ја користела адресата на БТК, тогаш секој може да види колку БТК поседува. Ако адресата на компанијата не биде јавно потврдена, тогаш никој никогаш нема да знае дека и припаѓа на оваа компанија. За целосна анонимност, компаниите обично ја користат единствената адреса на БТК за секоја трансакција.
11. Брзина на трансакцијата. Способноста да испраќате пари насекаде и на кој било за неколку минути по мрежата на БТК ќе го обработи плаќањето.
12. Му припаѓа само на сопственикот на паричникот. Постои единствен систем за електронско плаќање каде сметката му припаѓа само на сопственикот. На пример, на PayPal ако од која било причина компанијата одлучи дека сопственикот некако ја користи сметката на погрешен начин, системот има право да ги замрзне сите средства на сметката без дури и да го предупреди сопственикот за тоа. Потврдувањето на правилното користење на сметката е целосна одговорност на сопственикот. Со БТК, сопственикот има приватен клуч и соодветен јавен клуч, што е адресата на паричникот на БТК. Никој освен сопственикот не може да повлече биткоини.
13. Нема шанси да користите некои лични податоци за измама. Ова е важна точка. Денес најголемиот дел од купувањата се вршат со кредитни картички. Тие се несигурни. Пополнувајќи ги формуларите на веб-страниците, од клиентите се

бара да ги внесат следните податоци: број на картичка, рок на употреба и код. Тешко е да се најде помалку безбеден начин за плаќање. Затоа, многу често се крадат кредитни картички. Трансакциите со БТК не бараат откривање на какви било лични податоци. Наместо тоа, користи два клуча: јавен и приватен. Јавниот е достапен за сите (т.е. адресата на паричникот БТК), но приватниот клуч е познат само на сопственикот. Трансакцијата треба да се потпише со интеракција на приватни клучеви и примена на математичка функција. Ова создава докази дека трансакцијата ја врши сопственикот.

14. Можност за инвестирање средства во транспарентен и профитабилен ресурс

*Недостатоци*

Според горенаведениот автор Ивашенко (2016) недостатоците се следните:

1. Силна нестабилност - речиси сите подеми и падови на вредноста на БТК директно зависат од декларираните изјави на владите на различни земји. Оваа нестабилност го создава проблемот на краток рок.
2. Големи ризици за инвестирање во криптовалути кои треба да се земат предвид на среден и долг рок. Наше мислење е дека листата на недостатоци на криптовалутите (биткоин) е многу подолга и се поврзани со ризик од перење пари, терористички и други незаконски активности финансирање, недостаток на централен издавач, што значи дека нема правно формално лице кое ќе гарантира во случај на банкрот и слично.

Сепак, иако е многу тешко да се предвиди, многу академици и професионалци од оваа тема тврдат дека иднината на криптовалутите се светли бидејќи ќе ги отстранат трговските бариери и посредниците, ќе ги намали трошоците за трансакциите, а со тоа ќе ја поттикне трговијата и економијата. Како и да е, треба да ги земеме предвид и песимистичките гласови и во академскиот свет, што сугерира дека високиот ризик од нестабилност, ризици од хакирање и недостаток на институционална резервна копија ја прави иднината на криптовалутите не многу оптимистичка.

## 1.13.Криптовалутите во иднина

Во секој случај, иднината е многу тешко да се предвиди, а иднината на финансиските пазари и многу млад и се уште недоволно истражен пазар е уште потешка. Останува да видиме дали криптовалутите ќе успеат да ги заменат парите и од кои овие два пазари ќе зависат еден од друг и дали воопшто ќе зависат. Криптовалутите сè уште не исполнуваат некои од основните својства на валутите, сè уште не станале општо прифатен медиум за размена, а исто така не се ефективно складиште на вредност поради прекумерната нестабилност. За разлика од златото, кое има речиси константна вредност која годишно расте за неколку проценти од криптовалутите, тие сè уште немаат, што се чини дека е една од главните пречки што криптовалутите треба да ги надминат.

Познато е дека златото има одреден процент кој расте на годишно ниво и е многу тешко да се изгуби во вредност и дека на USD и EUR влијаат многу фактори како што е инфлацијата, но промената на вредноста на Bitcoin е толку голема што промените во златото цени се речиси занемарливи. Поради оваа причина, Bitcoin може да се гледа како извор на многу брзи капитални добивки, но од друга страна како висок инвестициски ризик.

Познато е дека во минатото Биткоинот имаше дневни трицифрени промени во цените, а најголемата промена на цената на Биткоинот се случи на 22 февруари 2021 година кога за 19 часа Биткоинот падна од 58 илјади американски долари на 47 илјади. Овој пад очигледно имаше влијание и на некои други криптовалути, но не влијаеше директно на пазарите на капитал и на порастот или падот на вредноста на одредени хартии од вредност.

Останува да видиме дали Биткоин или некоја друга криптовалута ќе го достигне својот целосен потенцијал и успешно ќе влезе во играта на финансиските пазари или ќе се појави друга поуспешна опција. Моментално има премногу криптовалути, а секој ден излегуваат нови, па речиси е невозможно да се предвиди дали има некоја која ќе стане поуспешен конкурент за инвестирање на пазарите на капитал од Биткоин и дали ќе може да ги замени парите. Одредени земји како Флорида и нејзиниот најголем град Мајами веќе овозможија примање плати и плаќање одредени трошоци како комунални услуги и кирија во најпопуларната дигитална валута, а дали тоа ќе им овозможи на

другите останува да видиме. Исто така, некои од технолошки најнапредните компании, како што е Илон Маск на Tesla, освен што инвестираат одредени делови од задржаниот капитал во биткоин и слични дигитални валути, се повеќе се свртуваат кон можноста за купување на сопствени производи во некоја криптовалута. Познато е дека во 2021 година голем број мултинационални компании инвестирале одреден дел од својот капитал во една од актуелните криптовалути, најчесто во Биткоин. Покрај тоа што во 2021 година мултинационалните компании направија повеќе во биткоинот и највредните конкуренти по цена, банките исто така почнаа да инвестираат повеќе и затоа ја потврдува претходно споменатата теза дека останува да се види кога и во која смисла банките ќе се обиде да влезе на пазарот на криптовалути.

Речиси е сигурно дека електронските плаќања и дигиталните пари ќе бидат доминантни во многу блиска иднина. И Светската банка и Светскиот економски форум сметаат дека современата економија е неодржлива од многу причини, а една од нив е прекумерната количина на различни валути во светот, кои заедно прават исклучително комплициран систем за понатамошен развој на светската трговија. Во следната деценија се очекува речиси сите уреди да бидат поврзани на мрежата (IoT, Internet of things), а дигиталните валути се всушност неопходни за брза онлајн трговија.

До пред само неколку години, можевме да купуваме биткоини само преку Интернет, и стоки со мала вредност - до неколку стотици долари. Тоа се промени многу брзо, па сега голем број онлајн продавници, сајтови за е-трговија и голем број банки и финансиски институции прифаќаат криптовалути како и секоја друга „класична“. Многу технолошки компании дури промовираат и претпочитаат плаќања на биткоини, во однос на долари, бидејќи се знае дека нивната вредност сигурно ќе расте во иднина.

Последниот пример покажува колкава е довербата во овие нови валути, особено во Биткоин - компанијата Тесла купи биткоини во вредност од 1,5 милијарди долари и најави дека сега ќе може да се купуваат овие автомобили во криптовалути. Тесла исто така верува дека вредноста на криптовалутите ќе скокне за 20% во следната година.

На овој потег веднаш реагираше пазарот на капитал - вредноста на биткоинот скокна на рекордни 47.000 долари, а пред тоа беше околу 30.000 долари. Поради ова, се поголем број светски берзи, фондови, акционерски компании и инвеститори планираат да инвестираат во криптовалути оваа и следната година, очекувајќи уште поголем раст - и уште поголема заработка.

## 2. Платформи за криптовалути од втора генерација

Криптовалутите што овозможуваат лесно конструирање на паметни договори и децентрализирани апликации често се нарекуваат криптовалути од „втора генерација“. Се одликува со централизиран систем што сѐ држи под контрола – од сигурност, преку транспарентност, па сѐдо крајна употребливост. Исто така, имаат и стручен менаџмент штоактивно работи на нивниот развој и употребливоста. Овде ситуацијата е спротивна во однос на децентрализираните криптовалути: точно се знае кои се сопственици на дигиталните паричници, сите трансакции се транспарентни и можатда се следат(со тоа и да платат данок), сигурноста е на завидно ниво и многу е тешко да се хакираат – дури и да се успее во тоа, коините не можат да го напуштат тој систем и лесно можат да се вратат на нивните сопственици. Централизираните криптовалути, во последно време, се под жесток напад од повеќе страни. Прво, од страна на старомодните криптовалуташиштознаат дека успехот на централизираните криптовалути,во основата, ќе ги уништат старите криптовалути и од страна на системите за трансфер на пари, бидејќи со текот на времето ќе им одземат огромен дел од пазарниот удел и многу денешни гиганти (како „Вестерн јунион“, „Мани грим“ и др.) веројатно ќе одат во заборав, во историјата.[21]

Иако имаше неколку паметни договори изградени врз основа на Биткоин, како што се Mastercoin (сега Omni) и Colored Coins, овие беа тешки за изградба. Ethereum ги направи паметните договори многу полесни за изградба со конструирање на целосно уникатен јазик што може лесно да се интегрира со неговата наменски изградена платформа. Во суштина, Ethereum овозможи лесно додавање ажурирани детали за тековните паметни договори или додавање нови детали за паметните договори во блокови, при што трансакциите се обработуваат истовремено на мрежата. Ethereum е убедливо најчесто користената платформа за изградба на различни децентрализирани апликации.

Криптовалутите што припаѓаат на втората генерација донесоа огромен скок напред во светот на криптовалутите. Пред појавата на втората генерација, криптовалутите се перцепираа само како средство за зголемување на вредноста на парите без можност за понатамошно работење со нив. Ethereum се смета за водечки претставник на втората

[21] Проф. д-р Зоран Колев, Криптовалута – злато на интернет, Статија во „е-Банкар“ број 9, https://www.abit.edu.mk/News2e53.html?IdNews=153&IdLanguage=1&IdRoot=1

генерација. На него беа креирани првите паметни договори, кои се еден вид проширување на даденият блокчејн. Паметните договори доведоа до појава на DeFi (децентрализирано финансирање), кои се апликации фокусирани на обезбедување финансиски услуги. Ова можат да бидат, на пример, менувачници, агенции за изнајмување, осигурителни компании или управување со финансиски деривати. DeFi услугите се достапни за сите, а бидејќи се децентрализирани, многу е тешко да се цензурираат. Примери за DeFi платформи се Uniswap или Balancer. Сите ERC-20 токени (на пр. USDT) работат на мрежата Ethereum, а тргувањето со NFT е исто така популарно во денешно време. Ништо од ова не би било можно доколку не постоеја паметни договори. Тие обично работат на proof of stake (нивните блокови повеќе не се минираат со помош на компјутерски операции, но валидаторите на трансакции се натпреваруваат меѓу себе за да го затворат блокот).

Сепак, широко користените мрежи за криптовалути од втора генерација имаат и свои недостатоци. Тие не беа дизајнирани за толку тешки товари. За време на биковските пазари, кога мрежата е најкористена, трансакциските провизии на Етер мрежата можат да достигнат стотици долари. Овој и други проблеми се решаваат со криптовалути од третата генерација.

## 2.1.Етереум



Слика 3: Лого на Етереум

Етереум е моментално втората најголема и најпозната криптовалута. Тоа е платформа со отворен код базирана на блокчејн, т.е. децентрализирана база на податоци. Сепак, оваа платформа се карактеризира со таканаречени „паметни договори“ кои сакаат да ги децентрализираат класичните договори какви што ги знаеме денес. Овие договори

функционираат благодарение на „Виртуелната машина Етереум“, децентрализирана виртуелна машина. Платформата ви овозможува и да програмирате децентрализирани апликации и други криптовалути кои работат на нејзиниот блокчејн. Затоа, Етереум не е ограничен само на трансакции со криптовалути. Поради своите својства, Етереум се нарекува криптовалута од втора генерација.

## 2.2.Историја

Потеклото на Етереум датира од 2013 година, кога Виталик Бутарин, канадско-руски програмер, објави документ (т.н. бела книга) во кој ја презентираше идејата за Етереум. Тој продолжи да работи на оваа идеја со други луѓе кои беа заинтересирани за идејата. Во меѓувреме, многу луѓе се приклучија на проектот, а една година подоцна Гевин Вуд ја објави таканаречената жолта книга, во која ја формализираше оваа идеја за децентрализирани апликации изградени на блокчејнот. Во летото 2015 година, беше создаден Ethereum кога беше ископан првиот блок.[22]

Една година подоцна, се случи хард форк, кога блокчејнот беше поделен на две гранки (криптовалути), Ethereum и Ethereum Classic. На овој настан му претходеше хакерски напад врз тогаш новоформираната DAO (Децентрализирана анонимна организација). Овој проект, кој развиваше паметни договори на платформата, собра 150 милиони долари за еден месец. Сепак, анонимната хакерска група украде 50 милиони долари во етер. Овој настан доведе до губење на довербата во платформата, што значително се одрази на цената и предизвика гореспоменатата поделба на мрежата. Оние кои не се согласија со промените во мрежата и го отфрлија новиот систем останаа со стариот блокчејн наречен Ethereum Classic. Друга важна пресвртница за Ethereum се случи во 2017 година, кога беше формирана EEA, или Enterprise Ethereum Alliance. Ова непрофитно здружение се состои од водечки глобални компании, истражувачки групи и стартапи.[23] Неговата цел е да го координира развојот на јавните и приватните делови од блокчејнот за решавање на разни проблеми во здравствената заштита, банкарството и другите индустрии. Влезот на големите компании во EEA му даде на Ethereum поголемо медиумско внимание и кредибилитет.

[22] Antonopoulos, A. M., & Wood, G. (2018). *Mastering ethereum: building smart contracts and dapps*. O'reilly Media.
[23] Lewis, A. (2018). *The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them*. Mango Media Inc..

Ethereum 2.0 моментално е во развој, чија цел е да ја подобри брзината од 15 до 30 трансакции во секунда на илјадници до десетици илјади. Исто така, ќе се префрли од механизам „доказ за работа“ на „доказ за удел“. Во овој механизам нема рудари, туку валидатори. Овие валидатори не треба да имаат машини за рударење, но мора да заклучат 32 ETH монети во мрежата за да станат една. Ова значително ќе ја подобри енергетската ефикасност, бидејќи овој метод бара помалку компјутерска моќ. Исто така, ќе има „шардинг“ на блокчејнот, што ќе ја направи целата мрежа поефикасна и ќе ја олесни работата на валидатор, бидејќи тој ќе се грижи за својот „шард“ од блокчејнот.[24]

## 2.3. Рударење на Ethereum

SimplyLearn (2023) го објаснува рударењето на Ethereum како процес на формирање и додавање блокови од трансакции во блокчејн мрежата на Ethereum. За да се изврши трансакција, рударите се одговорни за нејзино одобрување, а при решавање на загатки се користи Hashing Scrypt. Понатаму, истиот извор наведува дека рударењето на Ethereum може да се изврши на три начина:

1. cloud рударење - овој вид рударење се однесува на плаќање на некого провизија за инвестираните ресурси и време и рударење наместо вас, а вие добивате награда,

2. pool рударење, е најлесниот и наједноставниот начин на рударење. Рударењето се одвива во истиот базен со други рудари, а наградата се дели според принципот дека колку повеќе рудари, толку е помал делот од наградата. При користење на овој вид рударење, треба да се земат предвид основни фактори како што се минималната исплата, надоместокот за користење на базенот, кој зависи од количината на криптовалута што ја рударите и најчесто се движи од 1 до 3%, и големината на базенот.

3. соло рударство - овој вид рударство е профитабилен само ако рударот поседува голема количина на ресурси, што доведува до можни недостатоци во форма на трошоци за електрична енергија.

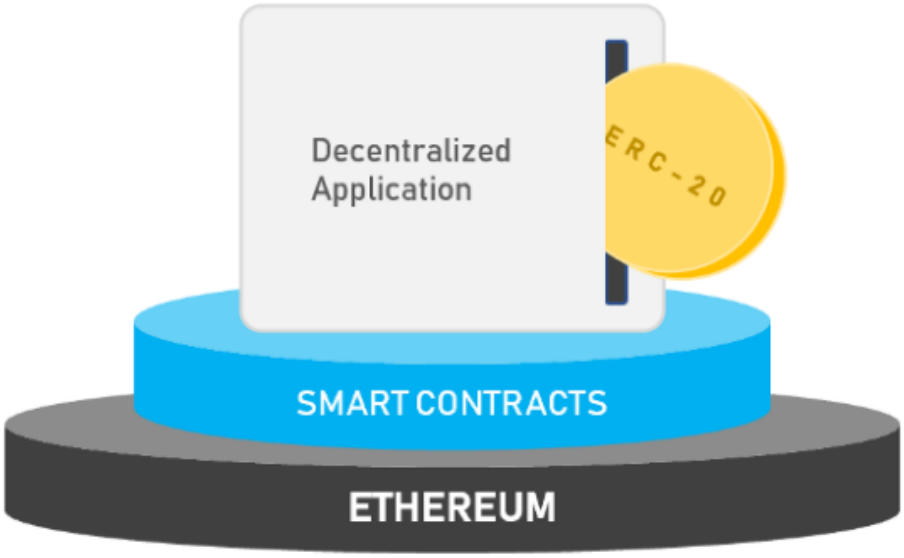
[24] WHAT IS ETHEREUM 2.0 AND WHY DOES IT MATTER? [online]. EC-Council, 2021: https://blog.eccouncil.org/what-is-ethereum-2-and-why-does-itmatter/

## 2.4.Карактеристики

Како што веќе споменавме, Ethereum не е ограничен само на трансакции. Платформата Ethereum овозможува користење на блокчејн за работа со паметни договори и децентрализирани апликации. Паметните договори се програми што нивните развивачи ги поставуваат така што можат, на пример, транспарентно да менуваат имот, акции, пари или други работи без потреба од интервенција од трета страна. Тие можат да обезбедат исполнување на одреден договор или договор кога се исполнети одредени услови. Овие паметни договори и децентрализирани апликации можат да работат благодарение на EVM (Ethereum Virtual Machine), виртуелна машина што го штити блокчејнот од преоптоварување и ја користи компјутерската моќ на целата мрежа.[25]

За секое дејство во мрежата, потребно е да се плати со „гориво“ (гас). За ова се користи етер (ETH), кој е гориво на целата мрежа и исто така се генерира како награда за рударите за минирани блокови. Покрај оваа награда, тие добиваат и надоместоци за трансакции и брокерски услуги во блокчејнот во единици Gas, кои последователно се претвораат во Ether. Благодарение на паметните договори, многу нови криптовалути влегоа во платформата Ethereum и протоколот ERC-20. Постојат стотици криптовалути[26] кои го делат овој стандард и можат да се складираат и префрлат на паричниците на Ethereum. Овие криптовалути ERC-20 беа дистрибуирани преку почетна понуда на монети (ICO). Оваа почетна претплата на монети се одвива во форма на „crowdfunding“, каде што одредена количина од криптовалутата се продава на инвеститорите за Ethereum.[27] Монетите на новата криптовалута потоа се користат како валута ако проектот собере доволна количина и е успешно лансиран. Ethereum моментално има неограничена емисија на монети, во минатото имаше дискусија за воведување ограничување, но до денес ниту едно не е усвоено. До денес се ослободени повеќе од 114 милиони ETH.[28]

[25] Solomon, M. G. (2019). *Ethereum for dummies*. John Wiley & Sons.
[26] Token Tracker [online]. Etherscan, 2020: https://etherscan.io/tokens
[27] Lewis, A. (2018). *The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them*. Mango Media Inc..
[28] Ether Total Supply and Market Capitalization Chart [online]. Etherscan, 2020: https://etherscan.io/stat/supply



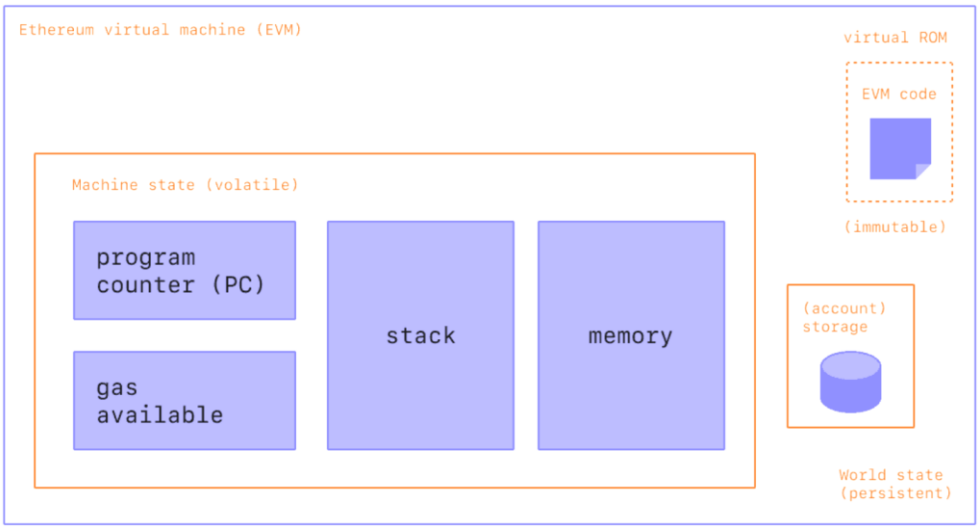

Слика 4: Хиерархија на платформата

Извор: (Towards Data Science Inc., 2018)

Виртуелната машина на Етереум (EVM) е посебна виртуелна машина која работи континуирано и чии непроменливи операции ја одредуваат состојбата на секој блок во блокчејнот на Етереум. EVM не само што регулира што јазлите можат, а што не можат да прават на дистрибуираната книга што ја одржува блокчејнот на Етереум, туку дефинира и специфични правила за промена на состојбата од блок до блок. Способноста да се направи второто овозможува функционалност на паметниот договор по кој Етереум стана познат.

За да разбереме што прави виртуелната машина на Етереум, треба да ги разгледаме секоја од различните функции што ги извршува за да обезбедиме непречено функционирање на мрежата на Етереум. За секој влез што го прима, EVM произведува излез кој е детерминистички по природа и следи математичка функција во наједноставна смисла.

Дејствувајќи како машина за стек што турка минливи вредности нагоре и надолу по стекот, EVM има длабочина од 1024 записи, од кои секој е 256-битен збор. Исто така, одржува привремена меморија во форма на низа од бајти, која се заменува помеѓу две трансакции на блокчејнот на Етереум. EVM ги извршува преведените паметни договори во форма на сет од 140 стандардни опкодови, додека други операции специфични за блокчејн се имплементирани од него.




Слика 5. Шема на виртуелната машина Ethereum[29]

Но, која е вистинската цел на виртуелната машина Ethereum? Виртуелната машина Ethereum сигурно ги извршува сите апликации што работат на мрежата Ethereum, без никакви поголеми пријавени прекини. За програмерите, EVM делува како програма за сеопфатна употреба што извршува помали извршни програми познати како паметни договори на Ethereum, давајќи им слобода да ги пишуваат овие паметни договори на различни програмски јазици, вклучувајќи го и Solidity, за што ќе разговараме подетално подолу. Конечно, EVM е вграден во секој јазол на Ethereum за да извршува паметни договори користејќи бајткод наместо мајчин програмски јазик, изолирајќи го физичкиот компјутер домаќин од машинскиот код на кој работи Ethereum.

## 2.5. Употреба и потенцијал

Поради можностите и потенцијалот на паметните договори, Ethereum има многу употреби. На пример, во банкарството, тие можат да се користат за забрзување на трансакциите, што би било брзо, транспарентно и генерално би ги поедноставило финансиските операции без потреба од интервенција од трети страни. Понатаму, на пример, употребата на блокчејнот Ethereum може да спречи кражба на идентитет, што во моментов се смета за голем проблем во општеството. Големите компании денес поседуваат неисцрпна количина на информации за луѓето и овие податоци лесно можат да се злоупотребат. Користејќи ја оваа технологија, ова би можело да се спречи

[29] Rangel Stoilov (2019). Solidity Smart Contracts: Build DApps In The Ethereum Blockchain

со обезбедување дека само самиот корисник ќе има пристап до лични податоци. Концептот на паметни договори може да се користи првенствено за елиминирање на посредници, или трети страни, во различни индустрии, со што се зголемува транспарентноста на целиот процес и се заштедуваат пари. Постојат многу начини за користење на паметни договори, вклучувајќи IoT (Интернет на нештата), предвидување на пазарот, обложување, паметни мрежи и многу други.[30]

Денес, на платформата има повеќе од 2.500 децентрализирани апликации, од кои некои веќе работат, некои се во развој, а други се во фаза на концепт.[31] Овој број расте, заедно со повеќе од милион сметки кои на некој начин имплементирале паметни договори.[32] Паметните договори имаат потенцијал да станат вообичаен дел од секојдневниот живот во иднина.

## 3. Што се децентрализирани апликации

Да почнеме со тоа што е апликација. Апликацијата е софтвер дизајниран за одредена намена. На пример, Microsoft PowerPoint е апликација што ви овозможува да креирате слајдшоуа за презентации. Децентрализирана апликација е само апликација што нема ниту една точка на информации за да ја извршува апликацијата. На пример, веб-апликација како Facebook ќе има централен сервер за поврзување. Додека секоја апликација изградена на блокчејнот на Ethereum ќе се извршува преку паметни договори дизајнирани да ја извршуваат. Не постои договорена дефинитивна дефиниција за тоа што е DApp, но постои широк консензус за тоа кои се трите главни карактеристики за DApps што вклучуваат монетарна вредност.

Прво, DA апликацијата има тенденција да биде со отворен код: DA апликацијата се карактеризира со својата транспарентна природа. Отворениот код значи дека секој може да го види кодот што е користен за изградба на DA апликацијата. Второ, DA апликацијата има внатрешна валута или токени: Бидејќи децентрализираните апликации се со отворен код, наплаќањето на корисниците за услугата би било бесплодно. Одговорот е да се распределат оскудни ресурси во мрежата со користење

[30] DOMINGUEZ, Nick. These are 11 Real World Use Cases for Ethereum [online]. CoinDiligent, 2020: https://coindiligent.com/ethereum-real-world-use
[31] State of the DApps [online]. State of the DApps, 2021: https://www.stateofthedapps.com/dapps
[32] Top Accounts by ETH Balance [online]. Etherscan, 2020: https://etherscan.io/accounts/c

на оскуден токен. Сопствениците на оскудни ресурси се платени во единици кои се наследени на DA апликацијата. Како што DA апликацијата станува поголема и се користи повеќе, овие оскудни ресурси стануваат повредни. Трето, DA апликацијата ќе има механизам за постигнување децентрализиран консензус: Бидејќи не постои единствен ентитет што ја контролира апликацијата, дистрибуираниот консензус треба да се постигне без доверба. Поради оваа причина, Биткоинот може да се смета за една од првите монетарни DA апликации, како и за првата криптовалута.[33]

**-Развој на DApp: моменталната слика**

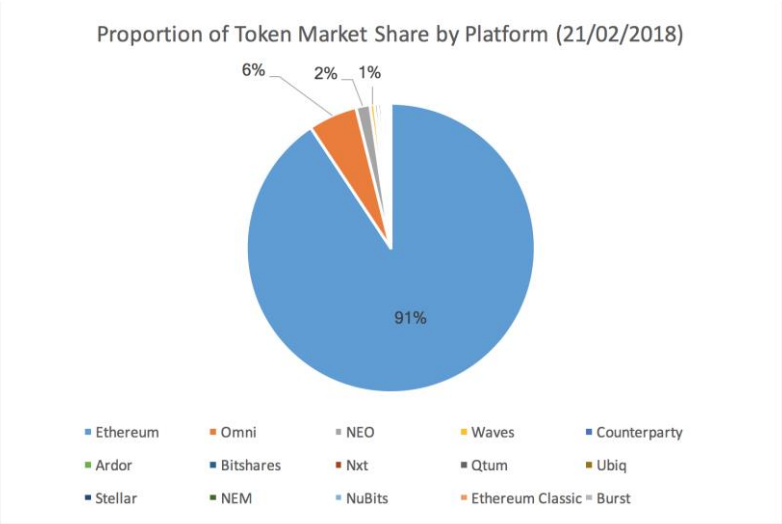
Како што споменавме претходно, главната причина зошто многу DApp-ови се изградени со Ethereum е затоа што тој беше првиот што имплементираше уникатен код за да овозможи нивно широко усвојување. Со Smart Contracts, Ethereum им го олесни на DApp програмерите да креираат свои сопствени токени за да ги напојуваат своите DApp-ови. Стандардот за токени ERC20, развиен во 2015 година, дефинира заедничка листа на правила што еден Ethereum токен мора да ги имплементира. Протоколот на Ethereum стана многу популарен кај компаниите за групно финансирање. Ethereum дури нуди и свој водич што ви покажува како да користите паметни договори за да креирате токен - на крајот се споменува дека тие се многу корисни за групна продажба www.ethereum.org/token.

**-Колку токени се поврзани со Ethereum?**

Од јануари 2018 година, имало повеќе од 21.000 договори за токени ERC20. Најуспешните од овие токени се наведени на www.coinmarketcap.com каде што има вкупно 476 токени изградени на блокчејнот Ethereum. Податоците земени од www.coinmarketcap.com би укажувале дека овие токени имаат моментална пазарна капитализација од над 42 милијарди долари (од 21.02.). Како платформа каде што поединците можат да градат токени, Ethereum е далеку најголем.

[33] https://bookdown.org/Jack_Biggs/Cryptocurrency/second-generation-cryptocurrencies-1.html

Но, други навистина постојат, без сомнение поради успехот на Ethereum. Omni на пример има пазарна капитализација од 2 милијарди долари, а NEO има 738 милиони долари. Доминацијата на Ethereum како платформа за токени е прикажана подолу.




Слика 6. Етереум е домаќин на огромното мнозинство токени[34]

[34] https://bookdown.org/Jack_Biggs/Cryptocurrency/second-generation-cryptocurrencies-1.html

Табела 2. Анализа на десетте најдобри токени на Ethereum

| Code | Token Name | Description | Market Cap |
|---|---|---|---|
| EOS | EOS.IO | Infrastructure for decentralised applications. Despite launching these tokens EOS will be released on a completely different blockchain. | $6,172,324,185 |
| TRX | TRON | TRON is an application intended to allow content creators to be compensated for sharing their content. | $3,053,977,241 |
| VEN | VeChain | Blockchain-as-a-Service company with a mission to build a trust-free and distributed business ecosystem to enable transparent information flow, efficient collaboration, and high-speed value transferring. | $2,941,319,037 |
| OMG | OmiseGo | OmiseGo aims to become the number one peer-to-peer cryptocurrency exchange system. Aims to offer cryptocurrency users an alternative to online exchanges. | $1,917,287,709 |
| ICX | ICON | Wants to "hyper connect the world" by building one of the largest decentralised networks in the world. It is building a platform that will allow various blockchains to interact with each other via smart contracts. | $1,614,402,246 |
| BNB | Binance Coin | Trading platform exclusively for cryptocurrencies: Crypto-to-Crypto. | $974,212,608 |
| PPT | Populus | Intends to become a platform for peer-to-peer invoices. | $895,508,552 |
| RHOC | Rchain | A new type of blockchain technology. It claims to provide content delivery at the scale of Facebook and process transactions at the speed of visa. | $835,089,650 |
| SNT | Status | Mobile operating system of Ethereum. | $703,276,187 |
| MKR | Maker | A stablecoin (no volatility) 1 Dai = One Dollar. | $650,585,812 |

Некои од овие токени се сметаат за вредни за да се појават на листата на топ 20 на http://www.coinmarketcap.com.

Бидејќи крипто пазарот е во опаѓање, треба да погледнеме други вредности и индикатори кои укажуваат на сосема поинаква слика од ценовната и дека Ethereum има причина зошто продолжува да го држи второто место. Подолу се наведени најзначајните апликации на блокчејнот Ethereum.

Паметни договори

- овозможуваат отстранување на посредници користејќи блокчејн технологија.
- можностите се бесконечни, од извршување трансакции, плаќања и позајмување Децентрализирано финансирање (DeFi)
- финансиски услуги каде што нема централен надзорен орган
- елементите на финансискиот систем се заменети со протоколи и паметни договори
- самиот систем станува сè посложен и тешко е да се биде во чекор со сите иновации и проекти поврзани со DeFi системот - најдобар показател за трендот на популарност е информацијата дека во мај 2020 година, износ малку помал од милијарда долари беше „заклучен“ во DeFi протоколи (вкупната вредност на DeFi системот неодамна достигна повеќе од 85 милијарди американски долари)

Програмери

- зголемена побарувачка за програмери (особено во крипто индустријата) бидејќи нови проекти се објавуваат речиси секојдневно и повеќето се лансираат на блокчејнот Ethereum
- Ethereum се гордее со најголемата заедница на програмери EIP-1559
- е предлог од Виталик Бутерин кој го менува сегашниот принцип на трансакциски такси на Ethereum, со што се намалува износот на такси што одеа кај „рударите“ и што би „согорело“ дел од таксата, со што се намалува количината на достапен етер
- овој модел би можел да има многу позитивни импликации за цената на етерот
- имплементацијата на предлогот најверојатно ќе биде во јули оваа година, а етерот би можел да стане дефлациска актива со овој обем на бизнис

Stablecoin

- околу 80% од stablecoin во оптек се на блокчејнот Ethereum
- компанијата за картички Visa објави дека ќе стане првата мрежа за плаќање што ќе го користи Stablecoin USDC за порамнување на трансакции.

NFT

- NFT технологијата има многу потенцијал и многу уникатни случаи на употреба од уметност, колекционерски предмети и видео игри

Токенизација

- влегувајќи во дигиталната доба, готовината наскоро ќе биде заборавена
- лесно е да се создаде сопствена криптовалута/токен со креирање паметни договори
- потенцијално и државите и компаниите би можеле да ја користат технологијата Ethereum за да издаваат свои дигитални валути или токени.
- токенизацијата може да одговара на многу бизнис модели.[35]

### Операција

DApps користат механизми за консензус за воспоставување консензус на мрежата. Двата најчести механизми за воспоставување консензус се доказ за работа (POW) и доказ за учество (POS).

Доказот за работа користи компјутерска моќ за да воспостави консензус преку процесот на рударење . Биткоинот го користи механизмот за доказ за работа. Доказот за удел е механизам за консензус кој ги поддржува DApps преку валидатори кои ја обезбедуваат мрежата со тоа што имаат удел и процент на сопственост врз апликацијата.



Слика 7. Платформа за рударење биткоини составена од десетици единици за графичка обработка

[35] Izvor: Lider, Ethereum ima snažan ekosustav i s razlogom je druga najveća kriptovaluta: https://lider.media/poslovna-scena/hrvatska/ethereum-ima-snazan-ekosustav-i-s-razlogom-je-druga-najvecakriptovaluta-136774

DApps ги дистрибуираат своите токени преку три главни механизми: рударење , собирање средства и развој. Во рударењето, токените се дистрибуираат според однапред одреден алгоритам како награди за рударите кои ја обезбедуваат мрежата преку верификација на трансакциите. Токените може да се дистрибуираат и преку собирање средства, при што токените се дистрибуираат во замена за финансирање во почетната фаза на развој на DApp, како во почетна понуда на монети . Конечно, механизмот за развој дистрибуира токени кои се издвоени за целите на развој на DApp преку однапред одреден распоред.

Постојат три главни чекори што секогаш се случуваат при формирањето и развојот на која било DApp: објавување на белата книга на DApp , дистрибуција на почетните токени и дистрибуција на сопственоста. Прво, се објавува белата книга, во која се опишани протоколите, карактеристиките и имплементацијата на DApp. Потоа, потребниот софтвер и скрипти им се стават на располагање на рударите и засегнатите страни кои ја поддржуваат валидацијата и собирањето средства на мрежата. За возврат, тие се наградени со почетните токени дистрибуирани од системот. Конечно, како што поголем број учесници се приклучуваат на мрежата, или преку користење на DApp или преку придонеси во развојот на DApp, сопственоста на токените се разредува и системот станува помалку централизиран.

## Карактеристики

DApps-ите го имаат својот backend код што работи на децентрализирана peer-to-peer мрежа , за разлика од типичните апликации каде што backend кодот работи на централизирани сервери. DApp може да има frontend код и кориснички интерфејси напишани на кој било јазик што може да прави повици до неговиот backend.

DApps се користат во децентрализираното финансирање (DeFi), во кое dapps извршуваат финансиски функции на блокчејни. Се очекува децентрализираните финансиски протоколи што ги потврдуваат peer-to-peer трансакциите, како што е Aave Protocol, да го нарушат централизираното финансирање и да ги намалат трошоците.

Перформансите на DApp се поврзани со неговата латенција, проток и секвенцијални перформанси. Системот на Bitcoin за валидација на трансакции е дизајниран така што просечното време за ископување на блок на блокчејнот на Bitcoin е 10 минути. Ethereum нуди намалена латенција од еден ископан блок на секои 12 секунди во просек (наречено Време на блок ). За споредба, Visa обработува приближно 10.000 трансакции во секунда. Поновите DApp проекти, како што е Solana , се обидоа да ја надминат таа стапка.

Интернет-поврзувањето е основна зависност на блокчејн системите, што ги вклучува DApps. Високите монетарни трошоци, исто така, дејствуваат како бариера. Трансакциите со мали монетарни вредности можат да сочинуваат голем дел од пренесениот износ. Поголемата побарувачка за услугата, исто така, води до зголемени надоместоци поради зголемениот мрежен сообраќај. Ова е проблем за Ethereum , кој се припишува на зголемениот мрежен сообраќај предизвикан од DApps изградени на блокчејнот Ethereum , како што се оние што ги користат незаменливите токени (NFT). Надоместоците за трансакции се под влијание на сложеноста на паметните договори на DApp и од конкретниот блокчејн.

## Трендови

Ethereum е технологијата за дистрибуирана книга (DLT) која има најголем пазар на DApp. Првата DApp на блокчејнот Ethereum беше објавена на 22 април 2016 година. Од мај 2017 година, бројот на DApp-и што се развиваат растеше со поголема стапка. По февруари 2018 година, DApp-ите се објавуваа секој ден. Помалку од една петтина од DApp-ите ги опфаќаат речиси сите DApp корисници на блокчејнот Ethereum. Околу 5% од DApp-ите опфаќаат 80% од трансакциите на Ethereum. 80% од DApp-ите на Ethereum ги користат помалку од 1000 корисници. На Ethereum, DApp-ите што се берзи опфаќаат 61,5% од обемот на трансакции, финансиските DApp-и опфаќаат 25,6%, коцкарските DApp-и опфаќаат 5%, високоризичните DApp-и опфаќаат 4,1%, а игрите опфаќаат 2,5%. До почетокот на 2025 година, NFT-ите и социјалните dApp-и забележаа зголемување од 6–9% во ангажманот на корисниците, дури и кога употребата на DeFi dApp доживеа скромен пад.

DApps не се широко распространети. Потенцијалните корисници можеби немаат вештини или знаење за ефикасно да ги анализираат разликите помеѓу DApps и традиционалните апликации, а исто така можеби нема да ги ценат тие разлики. Оваа вештина и информации може да бидат тешки за пристап за мејнстрим корисниците. Дополнително, корисничкото искуство за DApps често е лошо, бидејќи тие често се развиваат за да дадат приоритет на функционалноста, одржувањето и стабилноста.

Многу DApps се мачат да привлечат корисници, особено во фазите на нивното основање, па дури и оние што привлекуваат широка почетна популарност се мачат да ја задржат.

Значаен пример беше DApp CryptoKitties, кој значително ја забави мрежата Ethereum на врвот на нејзината популарност. CryptoKitties и други слични DApp Dice Games базирани на игри не успеаја да привлечат слична привлечност оттогаш.

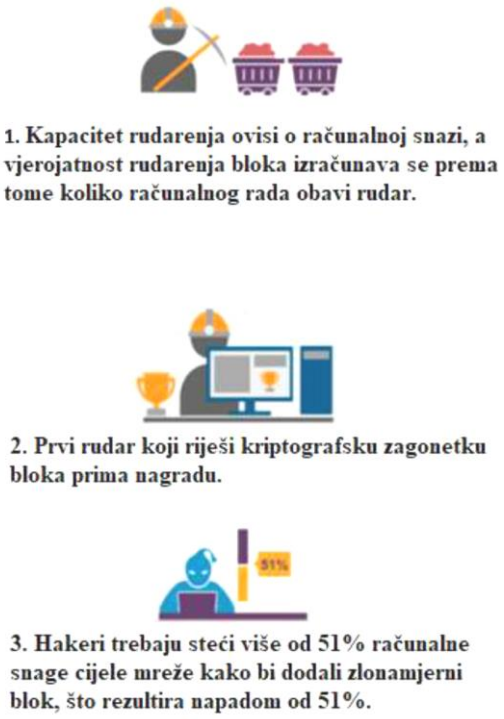
## 4. Механизми за консензус

Клучна карактеристика на блокчејн технологијата е одредувањето кои корисници ќе објавуваат блокови. Кога еден рудар (node) објавува блок, тој ќе биде награден со криптовалута. Ова им овозможува на многу рудари да се натпреваруваат за објавување блокови. Користењето на механизам за консензус може да го реши овој проблем. Им овозможува на група корисници кои не си веруваат едни на други да соработуваат. Двата најчесто користени механизми за консензус се Доказ за работа и Доказ за удел. Некои други механизми за консензус што се користат во светот на блокчејн технологијата се Доказ за авторитет, Доказ за изминато време, Доказ за важност, Доказ за капацитет, Доказ за потрошувачка. Механизмот за консензус е процес на донесување одлуки каде што корисниците на мрежата се согласуваат и поддржуваат одлука во корист на мрежата. Во моделот на консензус, за да додаде блок во блокчејн мрежата, рударот (јазол) мора да реши криптографска загатка (алгоритам). Процесот на решавање на алгоритмот е многу тежок за решавање, затоа бара огромна компјутерска моќ. Откако ќе се реши, тој алгоритам се емитува во мрежата за верификација. Блокот ќе биде доделен на блокчејн мрежата само по успешна верификација.

## 4. 1. Доказ за работа (Proof-of-Work)

Најпознатиот механизам за консензус е Доказ за работа, кој се користи во најпознатата криптовалута во светот, Биткоин. Со години, PoW е популарен избор во криптографијата на криптовалути. Учесникот што користи PoW се нарекува рудар. Рударите извршуваат пресметковна задача и решаваат математички алгоритам за да го заработат правото да генерираат нов блок. Рударите го решаваат алгоритмот со наоѓање специфична хеш функција. Секој блокчејн рудар се обидува да реши хеш вредност, т.е. се обидува да најде специфична вредност (nonce) за да задоволи предефиниран услов за хеширање, т.е. наоѓање нонца вредност што ќе ги сочинува првите 30 бита од неговиот хеш. Рударот се обидува да најде хеш вредности што се помали или еднакви на специфична целна вредност со цел да се постигне консензус во блокчејн мрежата. Секогаш кога рудар ќе најде целна хеш вредност, го емитува тековниот блок до блокчејн мрежата. После тоа, сите други јазли (рудари) ја потврдуваат точноста на неговата хеш вредност. Ако блокот е легитимен, сите јазли го додаваат тој нов валидиран блок во блокчејнот. Слика 5 го илустрира механизмот за консензус базиран на доказ за работа. Главните предности на консензусот за доказ за работа се неговата безбедност, прифатливо ниво на скалабилност и децентрализација. Сепак, процесот на рударење и валидирање на блок во PoW троши многу електрична енергија. Колку е потежок математичкиот алгоритам, толку повеќе компјутерска моќ е потребна за да се реши. Рудар со ограничени ресурси не би можел да реши комплексен алгоритам бидејќи времето за генерирање на целната хеш вредност и стапката на успех зависат од компјутерската моќ на рударот. Затоа, недостатоците на консензусот за доказ за работа се големото време за креирање блок, големата побарувачка за електрична енергија, помалиот капацитет за обработка и зависноста од специјален хардвер.[36]

[36] Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

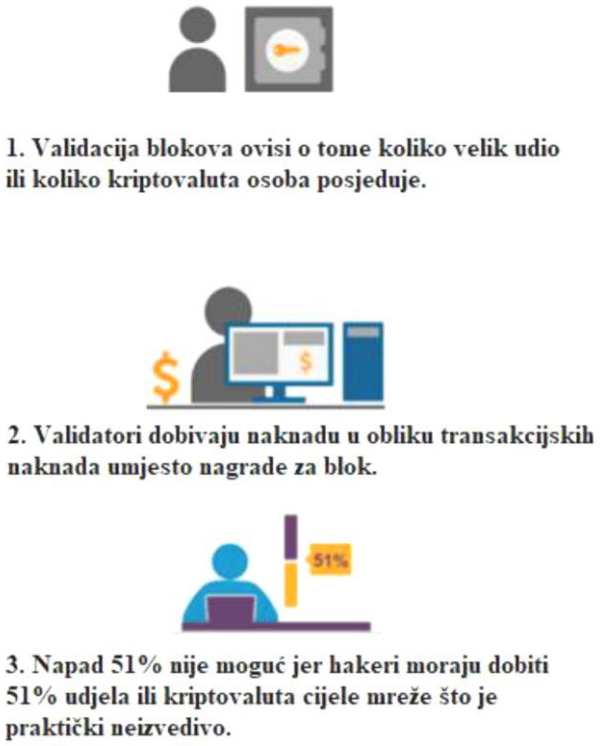



Слика 8. Илустрација на механизмот за консензус за доказ за работа (PoW) Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

## 4.2. Доказ за удел (Proof-of -Stake)

Следниот широко користен механизам за консензус е Доказ за удел. Главната цел на креирањето на концептот Доказ за удел е да се елиминира главниот недостаток на Доказ за работа, т.е. енергетската неефикасност. Во PoS, креаторот на следниот блок се избира преку различни комбинации на случаен избор, удел на понудата и возраст, што би можело да обезбеди скалабилност. Идејата за PoS за прв пат беше воведена во 2011 година, за криптовалутата Peercoin, а подоцна беше користена и во други. Во овој механизам за консензус, јазолот за креирање на следниот блок се избира преку случаен процес, а изборот се прави земајќи ги предвид средствата складирани во паричниците на рударите. Овој метод не бара голема компјутерска моќ за да се потврди кој било доказ, затоа рударите не добиваат никаква награда освен трансакциски такси. Предностите на доказот за удел се енергетска ефикасност, висок проток (можен е многу поголем број трансакции), брзо време на креирање блокови, скалабилност (помала од PoW) и нема потреба од посебен хардвер за рудари. Иако PoS не бара

компјутерска моќ како PoW, тоа зависи од рударите кои поседуваат најголем удел и на крајот блокчејнот може да стане централизиран. Друг вообичаен проблем со PoS се нарекува "nothing-at-stake". Ова значи дека ако рударот во рамките на блокчејн мрежата нема ништо во својот влог додека се однесува лошо, тогаш рударот нема да се плаши дека ќе изгуби нешто. Затоа, рударот нема да наиде на пречка што го спречува да се однесува лошо во рамките на мрежата. Еден пример за нечесно однесување на рударот може да биде креирање два сета нови блока за да се добијат двојни трансакциски такси. На Слика 9, можеме да видиме илустрација на механизмот за консензус за доказ за влог.

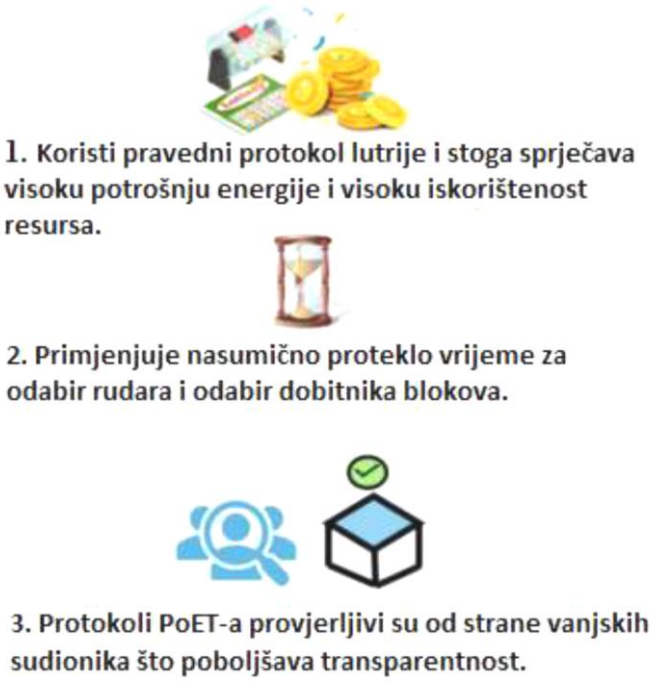



Слика 9. Илустрација на механизмот за консензус за доказ за учество (PoS) Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

### 4.3. Доказ за изминато време (Proof-of –Elapsed-Time)

Доказот за изминато време (PoET) е механизам за консензус кој користи протокол за лотарија. Преку протоколот за лотарија, шемата за консензус на PoET на PoET спречува голема потрошувачка на енергија и голема искористеност на ресурсите од страна на блокчејн јазлите. Овој алгоритам за консензус користи случајно изминато

време за да избере јазли кои ќе добијат права за рударење и да избере добитници на блокови. Исто така, механизмот за консензус на PoET е транспарентен, а резултатите од лотаријата на протоколот PoET се проверливи од надворешни учесници. На Слика 10, можеме да видиме илустрација на механизмот за консензус за доказ за време.

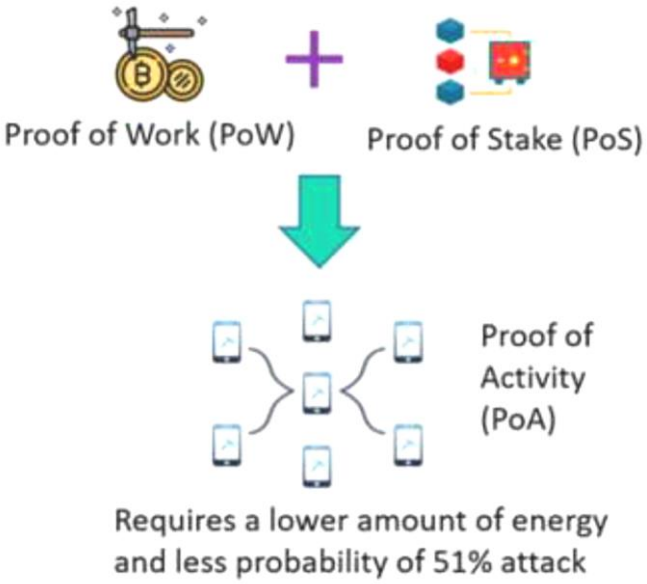



Слика 10. Илустрација на механизмот за консензус за доказ за изминато време (PoET)
Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

## 4.4. Доказ за авторитет (PoA) (Proof-of-Authority)

Друг алгоритам за консензус е Доказ за авторитет (PoA), кој е хибриден механизам за консензус бидејќи ги интегрира и PoW и PoS. Пример за PoA е Peercoin, кој користи механизам за консензус за PoW во комбинација со консензус за PoS. Со интегрирање на PoW и PoS, потребна е помалку енергија, а веројатноста за напад од 51% е намалена. Напад од 51% е вообичаен напад врз блокчејн мрежа, каде што еден рудар или организација ја презема контролата врз поголемиот дел (минимум 51%) од хашретот за рударење и предизвикува нарушување на блокчејн мрежата. Овој процес му овозможува на напаѓачот кој ја презема контролата врз поголемиот дел од хеш-стапката намерно да ги измени или исклучи сите трансакции помеѓу корисниците во

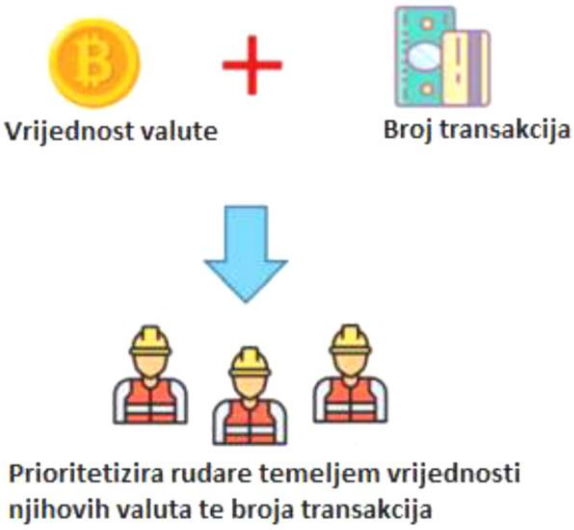
блокчејнот. Проблемот со нападот од 51% е главно во механизмот за консензус на PoW, а PoA значително ги намалува шансите за таков напад. На Слика 11, можеме да видиме илустрација на механизмот за консензус за доказ за авторитет.




Слика 11. Илустрација на механизмот за консензус за доказ за важност (PoA) Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

## 4.5. Доказ за важност (PoI) ( Proof-of-Importance)

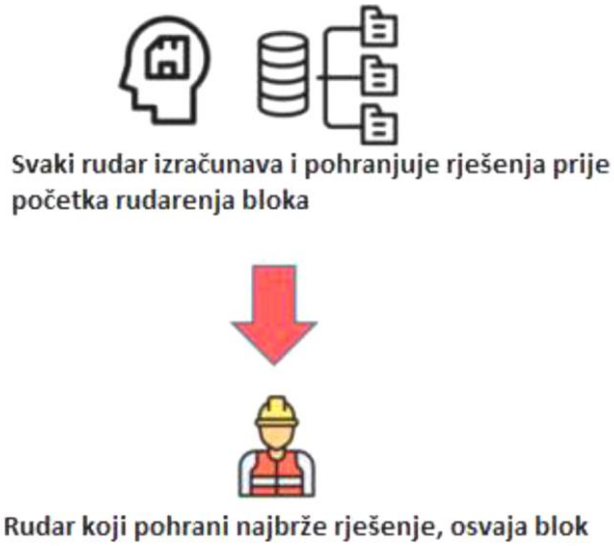
Механизмот за консензус за доказ за важност (PoI) работи на принципот на рударење за доказ за важност. Се користи за да се одредат квалификувани корисници за извршување на потребните пресметки при додавање нов блок во блокчејн мрежата и собирање на трансакциски такси. Консензусот за PoI им дава приоритет на блокчејн рударите кои имаат поголема вредност на криптовалутата и бројот на трансакции што ги извршуваат во соодветната криптовалута. Колку повеќе трансакции извршуваат рударите од нивниот паричник, толку се поголеми нивните шанси да добијат награда за креирање на следниот блок. На Слика 12, можеме да видиме илустрација на механизмот за консензус за доказ за важност.




Слика 12. Илустрација на механизмот за консензус за доказ за важност (PoI) Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

## 4.6. Доказ за капацитет (Proof-of-Capacity)

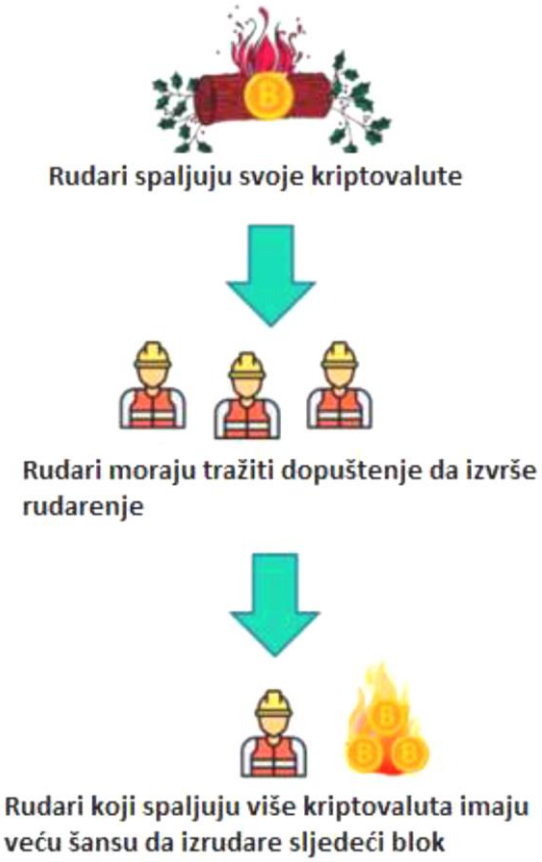
За разлика од PoW кој користи компјутерска моќ, Доказот за капацитет (PoC) користи слободна меморија на тврдиот диск за рударење криптовалути. Овој механизам за консензус вклучува „графичко цртање“ на тврдите дискови на рударите, т.е. извршување пресметки и складирање решенија на тврди дискови пред да започне рударењето на блок. Рударот кој го складира најбрзото (најблиското) решение до алгоритмот на блокот го добива блокот. Користејќи го овој механизам, може да се искористи капацитетот на просторот за складирање на тврдиот диск на корисникот. Секако, колку повеќе простор на тврдиот диск има рударот, толку е поголема шансата за рударење на следниот блок и добивање награда. На Слика 13 може да се види илустрација на механизмот за консензус за доказ за капацитет.




Слика 13. Илустрација на механизмот за консензус за доказ за капацитет (PoC) Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

## 4.7. Доказ за согорување (Proof-of-Burn)

Механизмот за консензус Доказ за согорување (PoB) работи така што рударите на блокчејн ги „согоруваат“ своите криптовалути, т.е. рударите ги испраќаат своите криптовалути на адреса од која не можат да бидат вратени. Со испраќање криптовалути на адреса од која испратените средства никогаш не можат да бидат вратени, на секој рудар му се дава доживотна привилегија да врши системско рударење преку процес на случаен избор. Оние рудари на блокчејн кои трошат/согоруваат поголема количина криптовалути имаат поголема шанса и приоритет за рударење на следниот блок. Слика 14 покажува илустрација на механизмот за консензус Доказ за согорување (PoB).




Слика 14. Илустрација на механизмот за консензус Доказ за согорување (PoB) Извор: Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

## 4.8. Споредба на механизми за консензус

Сега ќе ги прикажеме во табела споредбите на сите механизми за консензус за кои пишувавме претходно. Секој механизам се оценува според неколку клучни карактеристики, имено пристапност, скалабилност, децентрализација, проток и латентност. Овие карактеристики се важни за разбирање на предностите и недостатоците на секој механизам за консензус. Објаснување на колоните:[37]

- Пристапност: означува кој може да учествува во мрежата и каков е процесот на консензус (јавен, приватен, со дозволи, без дозволи).
- Скалабилност: мерка за тоа колку добро системот може да се справи со зголеменото оптоварување.

[37] Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)

- Децентрализација: нивото на распределба на контрола и авторитет на учесниците во рамките на блокчејн мрежата.
- Проток: го означуваме бројот на трансакции што системот може да ги обработи во одреден временски период.
- Латентност: време потребно за постигнување консензус и потврдување на трансакциите.

Табела 3. Споредба на механизми за консензус

| Механизам на консензус | Пристапност | Скалабилност | Децентрализација | Пропусен опсег | Латенција |
|---|---|---|---|---|---|
| **PoW** | Јавно, без дозвола | Висока | Висока | Ниска | Висока |
| **PoS** | Јавно, без дозвола, со дозвола | Висока | Висока | Ниска | Висока |
| **PoET** | Јавно, без дозвола, со дозвола | Висока | Средна | Висока | Ниска |
| **PoA** | Јавно, без дозвола | Висока | Висока | Ниска | Средна |
| **PoI** | Јавно, без дозвола | Висока | Висока | Висока | Средна |
| **PoC** | Јавно, без дозвола | Висока | Висока | Ниска | Висока |
| **PoB** | Јавно, без дозвола | Висока | Висока | Ниска | Висока |

## 5. Паметни договори

Паметен договор е компјутерска програма која автоматски извршува однапред дефиниран договор помеѓу две или повеќе страни, додека условите и алгоритмот за добивање на резултатите од договорот се напишани во форма на програмски код. Терминот паметен договор првпат го вовел Ник Сабо - познат компјутерски научник, адвокат и криптограф, кој го дефинирал во раните 1990-ти како „збир на ветувања, дефинирани дигитално, вклучувајќи ги протоколите со кои страните ги исполнуваат тие ветувања“[38]. Додека автоматите за продажба што постојат од раните 1880-ти се сметаат за први парчиња технологија еквивалентни на паметните договори, во последната деценија паметните договори извршени на дистрибуирани платформи - блокчејни - одеднаш добија на популарност. Во таков контекст, паметните договори ги стекнуваат сите својства на систем базиран на блокчејн - дистрибуција, транспарентност и непроменливост.

Главната теза на Сабо е дека договорите се неопходни за градење доверба во општеството. Две години подоцна, Сабо тврди дека договорите се основните градежни блокови на секоја економија на слободен пазар. Неколку години подоцна, компјутерските научници и математичари развија технички алатки за автоматизирање на договорите. Уште поважно, технологијата што овозможува рана и рудиментарна форма на паметни договори веќе постоеше кога Сабо ги сподели своите мисли со јавноста. Пример за таква технологија е DigiCash (1988) на Чаум, систем за плаќање што ја штити приватноста на корисниците.[39]

Понатаму, Сабо веруваше дека паметните договори треба да бидат проверливи и извршни за да имаат вредност за општеството. На овој начин, паметните договори ќе станат составен дел од општеството што ќе ги намали законските бариери, ќе ги намали трошоците за трансакции, ќе го скрати времето за извршување на договорите и ќе создаде можности за нови форми на бизнис. Сабо беше во право во своите

[38] Szabo, N. Formalizing and Securing Relationships on Public Networks. First Monday, 2,9. (1997), str 1, https://doi.org/10.5210/fm.v2i9.548

[39] Nick Szabo, „Smart Contracts“ (1994): https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

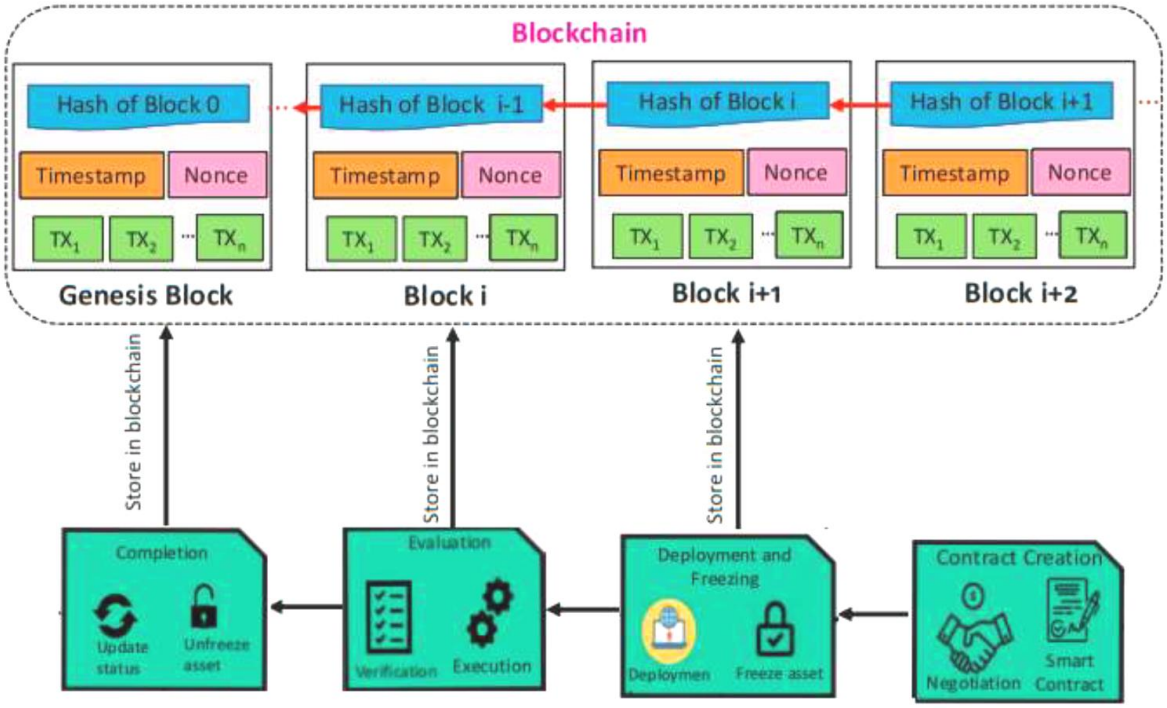
предвидувања: денес, како што паметните договори се развиваат и ги заменуваат некои традиционални договори, трошоците се намалуваат, а извршувањето се забрзува.

Програмските јазици што се користат за пишување паметни договори се Solidity и Serpent. Сепак, пошироко користениот јазик е Solidity.[40]

*Solidity* е програмски јазик на високо ниво, објектно-ориентиран, создаден специјално од мрежниот тим на Ethereum за градење и дизајнирање паметни договори на блокчејн платформи. Инспириран е од јазиците C++, Python и JavaScript.

Solidity е статички типизиран, обезбедувајќи поддршка за наследување, библиотеки и сложени типови дефинирани од корисникот. Со Solidity, можно е да се креираат договори за апликации како што се групно финансирање (*Crowdfunding*), слепи аукции и повеќенаменски паричници. Solidity не е тешко да се научи. Сепак, паметните договори во Solidity се изградени на блокчејнот, така што не можат да се менуваат или бришат. Ова ги прави многу безбеден начин за пренос на нешто од вредност, но може да биде и недостаток за развивачот. Кодот зад паметните договори во Solidity мора да биде беспрекорен и без грешки бидејќи не можете да поправите грешки или да вратите трансакции. Ажурирањето на кодот на Ethereum е единствениот начин да се поправат ранливостите, што не е лесна задача.

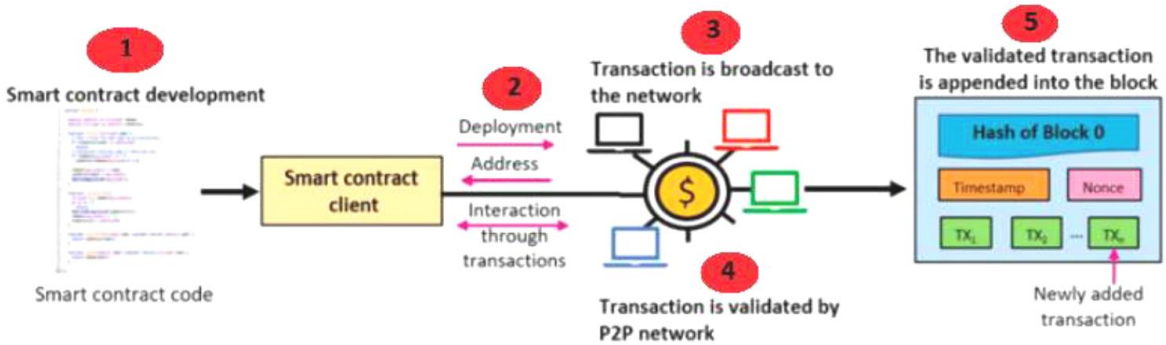
[40] Buterin, V.: Ethereum white paper: a next generation smart contract & decentralized application platform (2013). Available: Ethereum Whitepaper | ethereum.org




Слика 15. Чекори за подготовка на паметни договори

Извор: Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. (2020).

Животниот циклус на паметниот договор има 4 фази: креирање, извршување, интеграција и финализирање, како што може да се види на Слика 16.[41]




Слика 16. Животен циклус на паметни договори

Извор: Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. (2020).

[41] Извор: Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. (2020).

Најпопуларниот блокчејн за извршување паметни договори е Ethereum. На Ethereum, паметните договори обично се пишуваат во Тјуринг-комплетен програмски јазик наречен Solidity, и се компајлираат во бајт-код на ниско ниво за да се изврши од виртуелната машина Ethereum. Поради проблемот со запирање и други безбедносни проблеми, Тјуринг-комплетноста се смета за ризик и намерно се избегнува од јазици како Vyper. Некои од другите програмски јазици за паметни договори на кои им недостасува Тјуринг-комплетноста се Simplicity, Scilla, Ivy и Bitcoin Script. Сепак, мерењата во 2020 година со користење на регуларни изрази покажаа дека само 35,3% од 53.757 паметни договори на Ethereum во тоа време вклучувале рекурзии и јамки - конструкции поврзани со проблемот со запирање.

Неколку јазици се дизајнирани да овозможат формална верификација: Bamboo, IELE, Simplicity, Michelson (може да се верификува со Coq ), Liquidity (се компајлира во Michelson), Scilla, DAML и Pact.

| **Значајни примери на блокчејн платформи кои поддржуваат паметни договори вклучуваат следново:** | |
|---|---|
| **Име** | **Опис** |
| Етереум | Имплементира Тјуринг-комплетен јазик на својот блокчејн, истакната рамка за паметни договори |
| Биткоин | Обезбедува Тјурингов нецелосен скриптен јазик кој овозможува креирање на прилагодени паметни договори врз Биткоин како што се сметки со повеќе потписи , канали за плаќање, депонирани средства, временски брави, атомско тргување преку синџир, оракули или повеќепартиска лотарија без оператор. |
| Кардано | Блокчејн платформа за паметни договори |
| Солана | Блокчејн платформа за паметни договори |
| Трон | Блокчејн платформа за паметни договори |
| Тезос | Блокчејн платформа за паметни договори |
| Лавина | Блокчејн платформа за паметни договори |

Процесите на блокчејн се генерално детерминистички за да се обезбеди византиска толеранција на грешки. Сепак, примената на паметни договори во реалниот свет, како

што се лотарии и казина , бара безбедна случајност. Всушност, блокчејн технологијата ги намалува трошоците за спроведување на лотарија и затоа е корисна за учесниците. Случајноста на блокчејн може да се имплементира со користење на блок-хешови или временски ознаки, пророци, шеми за обврзување, специјални паметни договори како RANDAO и Quanta, како и секвенци од мешана стратегија на Nash рамнотежа.

## 5.1. Создавање паметни договори

На самиот почеток на договорот, вклучените страни преговараат за правата, обврските и забраните од истиот договор. Сите вклучени страни постигнуваат договор по повеќе рунди преговори и дискусии. Адвокатите или советниците на страните го составуваат почетниот договор. Потоа, договорот, кој е напишан на природен јазик, се преведува на програмски јазик кој може да вклучува декларативен и логички јазик. Конверзијата на паметен договор од природен јазик во програмски јазик се состои од неколку фази, имено: дизајн на договор, развој, тестирање и валидација, слично на развојот на софтвер. По неколку повторени процеси, паметниот договор се подготвува и објавува на блокчејн мрежата.[42]

## 5. 2. Извршување паметни договори

Откако ќе се подготви паметен договор, тој се валидира и објавува на блокчејн мрежата. Поради непроменливоста на блокчејнот, паметниот договор не може да се промени откако ќе се објави на блокчејнот. Секоја модификација или корекција на договорот бара креирање на нов договор. Откако договорот ќе се објави и интегрира на блокчејнот, тој е достапен за сите вклучени страни. Во меѓувреме, вклучените страни ги замрзнуваат своите дигитални средства преку нивните дигитални паричници, а истите овие паричници се користат за идентификација на страните.

## 5.3. Интеграција на паметни договори

Откако паметниот договор ќе се интегрира во блокчејн мрежата, договорните клаузули се следат и оценуваат. Секогаш кога ќе се исполни еден од договорените услови (на пр., прием на договорениот производ), следните поврзани дејства автоматски се извршуваат. Исто така е важно да се напомене дека паметниот договор се состои од

[42] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. (2020).

неколку декларативни изјави кои исто така може да имаат логички врски. Затоа, откако ќе се активира услов, следните поврзани дејства автоматски се извршуваат и потврдуваат од страна на рударите на блокчејн. Статусот на верификацијата и извршувањето на договорот се објавува и евидентира на блокчејнот.[43]

Во 1998 година, Сабо предложи дека инфраструктурата за паметни договори може да се имплементира преку реплицирани регистри на средства и извршување на договори со користење на криптографски хаш-синџири и византиска репликација толерантна на грешки. Аскемос го имплементираше овој пристап во 2002 година користејќи го Scheme (подоцна додавајќи го SQLite ) како јазик за скрипти за договори.

Еден предлог за користење на Биткоин за реплицирана регистрација на средства и извршување на договори се нарекува „ обоени монети “. Реплицирани титули за потенцијално произволни форми на имот, заедно со реплицирано извршување на договори, се имплементирани во различни проекти.

Од 2015 година, UBS експериментираше со „паметни обврзници“ кои го користат блокчејнот на биткоин во кои потоци на плаќање хипотетички би можеле целосно да се автоматизираат, создавајќи инструмент за самостојно плаќање.

Желбите за наследство хипотетички би можеле да се спроведат автоматски по регистрацијата на смртоносна книга на родените преку паметни договори. Изводите од матичната книга на родените можат да работат и заедно со паметните договори.

Крис Снук од Inc.com сугерира дека паметните договори би можеле да се користат и за справување со трансакции со недвижности и би можеле да се користат во областа на евиденцијата за сопственички права и во јавниот регистар.

Сет Оранбург и Лија Палагашвили тврдат дека паметните договори би можеле да се користат и во договорите за вработување , особено договорите за привремено вработување, што според нив би било од корист за работодавачот.

[43] Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. (2020).

## 5.4. Правен статус на паметните договори

Видете исто така: Регулирање на алгоритми и закон за технологија на дистрибуирана книга

Паметниот договор обично не претставува важечки обврзувачки договор по закон. Постојат предлози за регулирање на паметните договори.

Паметните договори не се правни договори, туку трансакции кои се извршуваат автоматски преку компјутерска програма или протокол за трансакции, како што се технолошки средства за автоматизација на обврските за плаќање како што е пренос на криптовалути или други токени. Некои научници тврдат дека императивната или декларативната природа на програмските јазици би влијаела на правната важност на паметните договори.

Во некои јурисдикции, правните научници испитувале како ригидноста на паметните договори се поврзува со традиционалните доктрини како што е договорната непредвидливост. На пример, колумбиската правна наука предложила прилагодување на теоријата за претстојна отежнатост (teoría de la imprevisión) за да се објаснат високите економски и системски трошоци за поништување на ефектите од паметните договори преку судска интервенција, нагласувајќи ја потребата за интернализирање на овие трошоци и развивање нови процедурални механизми за дигитални средини.

Од лансирањето на блокчејнот Ethereum во 2015 година , терминот „паметен договор“ се применува за пресметка за општа намена што се одвива на блокчејн. Националниот институт за стандарди и технологија на САД го опишува „паметниот договор“ како „колекција од код и податоци (понекогаш наречени функции и состојба) што се распоредува со користење на криптографски потпишани трансакции на блокчејн мрежата“. Во ова толкување, паметниот договор е секаков вид компјутерска програма што користи блокчејн. Паметниот договор може да се смета и за безбедна складирана процедура , бидејќи неговото извршување и кодифицираните ефекти (како што е преносот на токени помеѓу страните) не можат да се манипулираат без да се модифицира самиот блокчејн. Во ова толкување, извршувањето на договорите е контролирано и ревидирано од платформата, а не од произволни програми од страната на серверот што се поврзуваат со платформата.

Во 2018 година, во извештајот на американскиот Сенат се вели: „Иако паметните договори може да звучат ново, концептот е вкоренет во основното договорно право. Вообичаено, судскиот систем решава договорни спорови и ги спроведува условите, но исто така е вообичаено да се има и друг метод на арбитража, особено за меѓународни трансакции. Со паметните договори, програмата го спроведува договорот вграден во кодот.“ Државите во САД кои донеле закон за употреба на паметни договори се Аризона, Ајова, Невада, Тенеси, и Вајоминг.

Во април 2021 година, Работната група за јурисдикција во Велика Британија (UKJT) ги објави Правилата за решавање на дигитални спорови (Правилата за дигитално решавање на спорови), кои имаа за цел да овозможат брзо решавање на правни спорови поврзани со блокчејн и крипто во Велика Британија.

Во 2021 година, Правната комисија на Англија и Велс советуваше дека паметните правни договори можат да бидат признати и спроведени според постојното англиско право.

### 5.5. Финализирање на паметниот договор

Статусот на вклучените страни се ажурира по евалуацијата на паметниот договор. Блокчејн мрежата ги евидентира сите извршени трансакции и ажурираните салда на сите страни. Вклучените страни ги пренесуваат дигиталните средства според договорените правила. Дигиталните средства се отклучуваат само откако ќе се заврши преносот, со што се завршува животниот циклус на паметниот договор. Треба да се напомене дека за време на фазите од животниот циклус на извршување и замрзнување на дигиталните средства, интеграција и евалуација и финализирање на паметниот договор, серија трансакции се објавуваат и евидентираат во блокчејн мрежата.

### 5.6. Како функционираат паметните договори

Паметниот договор е дел од код што имплементира произволни правила. Корисен начин на размислување за паметните договори е само да се сфати дека паметните договори се во суштина исти како и договорите - со таа разлика што тие автоматски ќе ги извршат сите дејства за кои вклучените страни се договориле.

Да го искористиме сценариото на Виталик Бутерин (креаторот на Ethereum) за да објасниме што е паметен договор. Понатаму, да речеме дека сценариото е дека А сака да му плати на Б 500 долари за да изгради веб-страница.

1. Договорен договор: А вложува 500 долари во договорот, средствата се блокирани.
2. Б завршува веб-страницата и испраќа порака до договорот барајќи да ги отклучи средствата
3. Доколку А се согласи, средствата се ослободуваат.
4. Ако Б одлучи да не ја заврши веб-страницата, Б може да се откаже со испраќање порака за откажување од средствата.
5. Ако А и Б не се согласат, ќе зависи од дефиниран судија (и А и Б се согласуваат за тоа кој е тој на почетокот) да одлучи.

Според зборовите на Виталик: „Основниот концепт [на паметен договор] е ако имате некаков нов вид апликација, она што би го направиле е да ги напишете правилата на вашата апликација во дел од кодот... Земете го овој дел од кодот, ова би го нарекле договор“. Откако ќе го поставите ова на блокчејнот, имате посебен вид сметка која во суштина е контролирана од кодот што сте го напишале. Во моментот кога ќе испратите еден етер на таа сметка, се откажувате од контролата врз таа сметка и никој повеќе не ја контролира - тоа е во суштина робот што седи на врвот на блокчејнот.

Паметните договори овозможуваат размена на пари, стоки, недвижен имот, хартии од вредност и други средства. Овие договори се чуваат и реплицираат во дистрибуирана книга, каде што информациите не можат да се фалсификуваат или бришат. Во исто време, енкрипцијата на податоците ја обезбедува анонимноста на страните во договорот. Важна карактеристика на паметните договори е тоа што тие можат да дејствуваат само во рамките на нивниот дигитален систем врз средствата што им се достапни.

## 5.7. Безбедност на паметните договори

Кога сè оди според планот, паметните договори го забрзуваат усвојувањето и растот на блокчејнот, но често се појавуваат безбедносни слабости што водат до губење на довербата и кражба на средства. Безбедноста на паметните договори се однесува на

принципите и практиките што ги користат програмерите, корисниците и берзите при креирање или интеракција со паметни договори. Блокчејнот е динамична индустрија од милијарда долари, па затоа злонамерните актери често бараат ранливости во паметните договори за да остварат брз профит. Овие слабости можат да резултираат со исцрпување на сите средства од паричникот на паметните договори. Како што наведовме претходно, паметните договори работат во рамките на непроменлива децентрализирана блокчејн мрежа, што значи дека нивните резултати не можат да се фалсификуваат со цел нелегална профит. Сепак, оваа непроменливост не е само предност, туку и недостаток. На пример, во 2016 година, сајбер-криминалците ја хакираа децентрализираната автономна организација „DAO“ и злоупотребија милиони долари во Ethereum со искористување на ранливостите во кодот на паметните договори. Бидејќи паметниот договор „DAO“ беше непроменлив, програмерите не можеа да го корегираат кодот. Се верува дека добро напишаните паметни договори се исклучително тешки за хакирање и претставуваат најсигурен начин за складирање документи во дигиталниот свет. Сепак, важно е да се запомни дека целиот код е напишан од човечки програмери кои се подложни на грешки. Бидејќи паметниот договор е видлив за сите корисници на блокчејн, можните ранливости стануваат видливи и низ целата мрежа и не е секогаш можно да се елиминираат поради непроменливоста.

Некои од познатите човечки грешки се следниве:

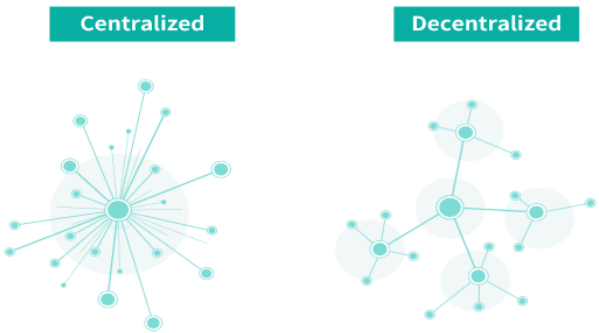
- Рекурзивни повици: Паметниот договор повикува друг надворешен договор пред да изврши промени. Сепак, после тоа, надворешниот договор може повторно да го повика почетниот паметен договор без овластување бидејќи неговата состојба сè уште не е ажурирана.
- Пречекорување: При извршување на аритметички пресметки, паметниот договор може да го надмине ограничувањето за складирање. Ова може да резултира со неправилно пресметување на износот.
- Рано искористување: Лошо дизајнираниот код содржи информации за претстојните трансакции што надворешните страни можат да ги искористат за сопствена корист.

Безбедноста на паметните договори може да се подобри преку темелен преглед на кодот, тестирање и ревизија, имплементација на најдобри практики, формална

верификација, континуирано следење и навремени надградби на безбедносните мерки. Сепак, важно е да се има предвид дека ниеден систем не е целосно непробоен, а редовното одржување и следење на најновите безбедносни практики е клучно за обезбедување на безбедноста на паметните договори.

## 5.8. Децентрализиран систем

Како што споменавме претходно, паметните договори се програмирани договори што се извршуваат на блокчејн. Тие користат децентрализиран систем и блокчејн технологија за автоматизирање на извршувањето на договорните услови. Децентрализираните системи играат клучна улога во контекст на паметните договори. Наместо да се потпираат на еден централен орган, паметните договори користат дистрибуиран систем со повеќе јазли кои независно ги потврдуваат и извршуваат договорите. Децентрализацијата носи голем број предности на паметните договори. Ова обезбедува транспарентност, бидејќи извршувањето на договорите и резултатите се видливи за сите учесници во мрежата. Исто така, обезбедува безбедност, бидејќи не се потпира на еден централен орган што би можел да биде предмет на напад или манипулација. Покрај тоа, децентрализацијата гради доверба, бидејќи извршувањето на договорите се потврдува од повеќе независни јазли. Децентрализацијата, исто така, обезбедува отпорност на грешки и толеранција на грешки. Ако некои јазли откажат или излезат од мрежата, остатокот од системот сè уште може да продолжи да ги извршува договорите. Ова ја обезбедува сигурноста и достапноста на паметните договори.




Слика 17: Илустрација на централизиран и децентрализиран систем (Извор: „Blockchain structure“ (2022): https://www.geeksforgeeks.org/ blockchain -structure/)

## 5.9. Улога во реалниот свет

Денес, паметните договори се многу популарни и можат да заменат разни алатки од реалниот свет. Така, паметните договори станаа и се сè попопуларни меѓу финансиските инструменти, сопственоста на имот, клиничките испитувања, хипотеките, гласањето на избори и многу повеќе.

Денес, вообичаено е да се бара посредник при размена на пари за акции или валута за валута. Ова не е случај со паметните договори, бидејќи тие можат да работат или да се извршуваат без трета страна и потреба од посредник. Проблемот со сопственоста на средствата се јавува при решавање на документацијата, додека со паметните договори таквите работи се решаваат во еден момент и се јавно достапни.[44]

Во однос на клиничките испитувања, паметните договори им помагаат на експертите непречено да споделуваат податоци низ целата индустрија. Покрај тоа, блокчејн технологијата овозможува автентикација на податоците и ја обезбедува нивната точност. Затоа, паметните договори имаат широка примена во здравствената индустрија.

Покрај здравствената индустрија, паметните договори се познати и во хипотекарната индустрија. Во моментов, хипотеките се силно оптоварени со долги процеси и повеќе посредници. Паметните договори можат да ги забрзаат овие процеси и можат да се спроведуваат без потреба од адвокати и трети страни.[45]

Кога станува збор за гласање на избори, сите знаеме колку е долготрајниот процес и колку е ранлив на манипулација од страна на гласачите. Доколку овој процес се спроведува преку паметни договори, секој глас би бил заштитен во главната книга. Покрај тоа, паметните договори би поттикнале поголема излезност на гласачите кои нема да мораат лично да присуствуваат на гласањето.

[44] Cheng, D. What are Smart Contracts? https://www.web3.university/tracks/create-a-smart-contract/what-are-smart-contracts

[45] Hedera, 10 Real-World Smart Contract Use Cases. https://hedera.com/learning/smart-contracts/smart-contract-use-cases

## 5.10. Предности и недостатоци на паметните договори

Предностите на паметните договори се поврзани со блокчејн технологијата. Сите други предности на паметните договори зависат од самата технологија. Некои од предностите на паметните договори се ефикасноста, точноста и непроменливоста. Овие предности го забрзуваат извршувањето на договорите, невозможноста за човечка грешка и невозможноста за менување на податоците.[46]

Покрај наведените предности, тука се и автономијата и заштедите. Ова значи дека не се потребни посредници, а ризиците од манипулација автоматски се елиминираат. Резервната копија е уште една предност на паметните договори, а сите документи складирани во блокчејн се дуплираат повеќе пати. Брзината и безбедноста се некои од другите предности на паметните договори. Имено, секој документ е криптиран и сите паметни договори се автоматизирани со помош на компјутерски протоколи, што заштедува многу време.

Секако, паметните договори имаат и некои недостатоци. Некои од овие недостатоци се трајноста, човечкиот фактор и дупките во законот. Трајноста се однесува на неможноста за промена на податоците, што е класифицирано како недостаток бидејќи ако има грешка во договорот, таа повеќе не може да се исправи. Покрај тоа, дупките во законот се недостаток бидејќи во теорија дозволуваат договорите да се склучуваат со лоша намера.[47]

Покрај овие недостатоци, постојат и недостатоци како што се нејасни услови. Понекогаш договорите вклучуваат услови што не се разбирливи, и затоа паметните договори не се во можност да извршат нејасни услови.[48]

Техничката сложеност и ограничената функционалност се некои други недостатоци на паметните договори. Денес, паметните договори се дефинирани на начин што „ако се случи x, тогаш ќе се случи y“ и затоа се помалку ефикасни во посложени процеси. Покрај тоа, самата имплементација е многу сложена и бара високо ниво на

[46] The Investopedia Team (2024). What Are Smart Contracts on the Blockchain and How Do They Work? https://www.investopedia.com/terms/s/smart-contracts.asp
[47] The Investopedia Team (2024). What Are Smart Contracts on the Blockchain and How Do They Work? https://www.investopedia.com/terms/s/smart-contracts.asp
[48] CFI Team, Smart Contracts. https://corporatefinanceinstitute.com/resources/valuation/smart-contracts/

техничка експертиза. Ова ги ограничува многу компании и поединци од користење на паметни договори.[49]

Како заклучок, паметните договори имаат и предности и недостатоци, како и сè друго на овој свет, но како што блокчејн технологијата се развива секојдневно, овие недостатоци последователно ќе се намалат или целосно ќе исчезнат со текот на времето.[50]

## 5.11. Безбедносни проблеми

Податоците за трансакциите од паметен договор базиран на блокчејн се видливи за сите корисници во блокчејнот. Податоците овозможуваат криптографски преглед на трансакциите, но ова води до ситуација каде што грешките, вклучително и безбедносните дупки, се видливи за сите, но можеби не се брзо поправени. Таквиот напад, кој е тешко да се поправи брзо, беше успешно извршен на DAO во јуни 2016 година, исцрпувајќи етер во вредност од приближно 50 милиони американски долари во тоа време, додека програмерите се обидуваа да дојдат до решение кое ќе добие консензус. Програмата DAO имаше временско одложување пред хакерот да може да ги отстрани средствата; беше направена тврда форка на софтверот Ethereum за да се вратат средствата од напаѓачот пред да истече временското ограничување. Други напади со висок профил вклучуваат напади со повеќепотписни паричници Parity и напад со целоброен прелив/прелив (2018), со вкупен износ од над 184 милиони американски долари.

Проблемите кај паметните договори на Ethereum, особено, вклучуваат двосмисленост и лесни, но несигурни конструкции во неговиот договорен јазик. Солидност, грешки во компајлерот, грешки во виртуелната машина на Ethereum, напади врз блокчејн мрежата, непроменливоста на грешките и тоа што не постои централен извор што ги документира познатите ранливости, нападите и проблематичните конструкции.

[49] FinaryLabs (2023). Advantages and Disadvantages of Smart Contracts.https://medium.com/coinmonks/advantages-and-disadvantages-of-smart-contracts-91d8bcf4ad27
[50] Исто.

### 5.12. Разлика од паметните правни договори

Паметните правни договори се разликуваат од паметните договори. Како што споменавме погоре, паметниот договор не е нужно правно извршлив како договор. Од друга страна, паметниот правен договор ги има сите елементи на правно извршлив договор во јурисдикцијата во која може да се спроведе и може да се спроведе од страна на суд или трибунал. Затоа, иако секој паметен правен договор ќе содржи некои елементи на паметен договор, не секој паметен договор ќе биде паметен правен договор.

Не постои формална дефиниција за паметен правен договор во правната индустрија.

Рикардискиот договор е еден вид паметен правен договор.

## 6. Програмски јазик Solidity

Solidity е програмски јазик на високо ниво, објектно-ориентиран, за имплементација на паметни договори, кој работи на виртуелната машина Ethereum. Solidity е инспириран од добро познати програмски јазици како што се C++ и JavaScript.[51] Solidity е статички типизиран и поддржува наследување, библиотеки и сложени типови дефинирани од корисникот, меѓу другото. Една датотека може да содржи повеќе договори, но сите договори во рамките на една датотека делат еден именски простор. Се користи за креирање токени на блокчејнот Ethereum.

Како што екосистемот Ethereum продолжува да расте, Solidity стана неопходна алатка за програмерите кои сакаат да креираат децентрализирани апликации и да ги искористат многуте придобивки што ги нуди самиот блокчејн.[52] Основачот на Ethereum, Виталик Бутерин, го предложи Ethereum како протокол што би ја проширил функционалноста на блокчејнот воведен од Bitcoin, со дополнителната функционалност на паметните договори. Според неговата визија, Ethereum би можел да работи со комплексна мрежа од паметни договори, кои условно извршуваат делови од код што работат на дистрибуирана, глобална мрежа од компјутери.

[51] Werkheiser, B. (2023). What is Solidity? https://www.alchemy.com/overviews/solidity
[52] Okoba, G. (2023). Solidity for Beginners: understanding the features of Solidity.https://coinsbench.com/solidity-for-beginners-understanding-the-features-of-solidity-53adc9a19d1e

Паметните договори им овозможуваат на програмерите да креираат нови криптовалути, да градат DeFi апликации и друго.

### 6.1. Намена и основни карактеристики

Основните концепти, т.е. основната намена на програмскиот јазик Solidity, се паметните договори опишани претходно. Заедно со паметните договори, секако, постојат типови на податоци, функции, променливи, настани, наследување, концепти специфични за Ethereum и една од најважните ставки, т.е. карактеристики - безбедност, што е клучен фактор во Solidity. Програмерите мора да ги разберат ранливостите како што се повторно влегување, прелевање на цели броеви и други за да пишуваат и безбедни и „паметни“ договори.

Токените се градежните блокови на Solidity - тие претставуваат места за складирање каде што податоците можат да се складираат и манипулираат. Постојат четири вида токени, барем што се однесува до Solidity: клучни зборови, идентификатори, литерали и интерпункција. Клучните зборови се зборови што имаат посебно значење и не можат да се користат како имиња на променливи. Примери за клучни зборови се договор, библиотека, интерфејс, прагма и модификатор. Идентификаторите се имиња дадени на ентитети како што се променливи, функции и договори, а литералите се вредности вградени во програмскиот јазик Solidity, како што се броеви, низи и булови вредности. Интерпункцијата е симбол што се користи за структурирање, како што се виткани загради, загради и точки-запирки.

## 7. Блокчејн технологија

Во својата наједноставна форма, блокчејн е дигитална датотека што се користи за складирање на податоци, а овие податоци се дистрибуираат (дуплираат) низ многу компјутери (децентрализирано).

Подетално и технички, блокчејн е базиран на peer-to-peer1 технологија, каде што целиот систем е составен од јазли (peers). Секој јазол во мрежата одобрува и евидентира секоја трансакција што се случува во мрежата. Ова значи дека секоја нова трансакција додадена во мрежата се потврдува и се додава во главната книга на

секој јазол. Овој децентрализиран начин на евидентирање на трансакциите во главната книга се нарекува дистрибуирана технологија на главната книга (DLT).

Блокчејн е еден вид DLT. Секоја складирана трансакција во блокчејн се нарекува блок. Секој блок е поврзан со претходниот блок користејќи криптографски хаш. Значи, ако некој сака да манипулира со одреден блок, ќе мора да манипулира со сите претходни блокови во синџирот, што е невозможно/исклучително тешко бидејќи сите јазли имаат иста главна книга и секоја промена е видлива. Ова создава непроменлив запис на блокови што не бара надворешен авторитет. Значи, во својата наједноставна форма, блокчејн е синџир од блокови. Тоа е процес или технологија за снимање информации во форма на блокови што спречува промени, хакирање или измама.[53]

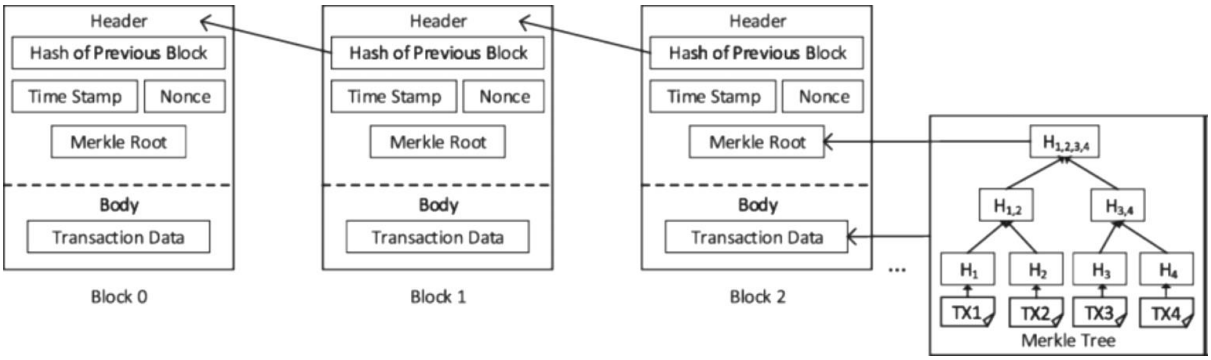
### 7.1. Структура на блокчејн

За подобро да ја разбереме структурата на блокчејн, прво ќе ги разгледаме основните компоненти потребни за структурата на блокчејн. Според Дуган, основните компоненти на блокчејн архитектурата се јазол, трансакција, синџир, рудари, консензус и блок.[54]

- Јазол - корисник или компјутер во рамките на блокчејн архитектурата (секој има независна копија од целиот блокчејн од записи)
- Трансакција - најмалата единица на системот (записи, информации итн.) што служи за целите на блокчејн.
- Ланец - низа од блокови по специфичен редослед
- Рудари - специфични јазли кои го извршуваат процесот на верификација на блок пред да додадат нешто во структурата на блокчејнот
- Консензус - збир на правила и договори за извршување операции во блокчејнот
- Блок: структура на податоци што се користи за складирање на збир на трансакции кои се дистрибуираат до сите јазли во мрежата. Голем број трансакции се случуваат секој ден низ целиот свет. Важно е корисниците да ги следат овие трансакции, што го прават со помош на блок структура.

[53] Kurt Dugan (2018). Blockchain for Beginners: Understand the Blockchain Basics and the Foundation of Bitcoin and Cryptocurrencies, CRB Publishing.
[54] Исто.

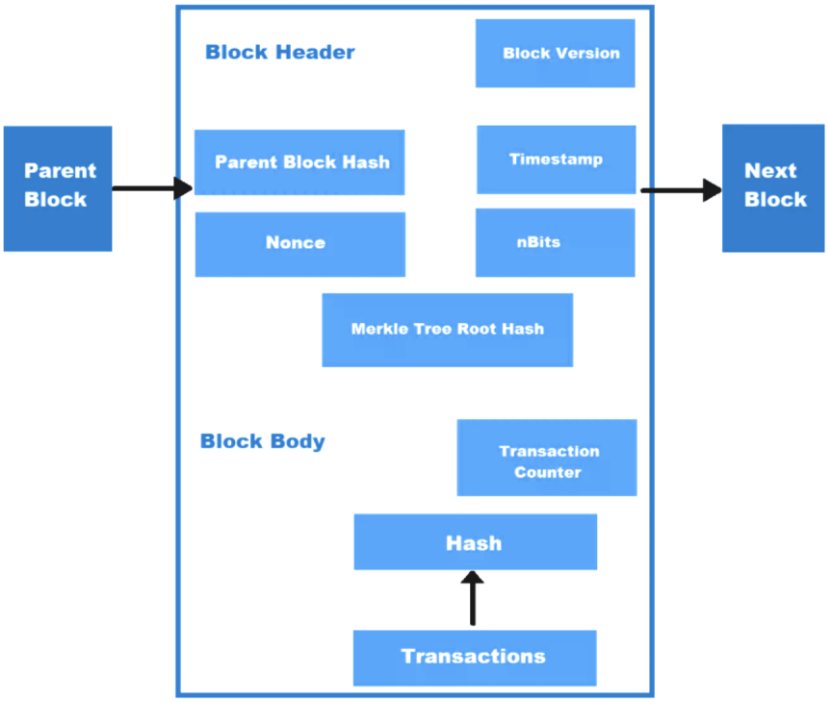
Структурата на блокчејнот и самиот блок ќе бидат објаснети подолу. Како што споменавме претходно, блокчејнот е линеарен синџир на блокови, а еден блок содржи збир на трансакции и други важни детали што ќе ги објасниме подолу. Сите блокови се линеарно поврзани и криптографски обезбедени.




Слика 18: Структура на блокчејн (извор https://www.creative-tim.com/blog/educational-tech/what-is-blockchain -technology-and-how-does-it-work/)

Така, сите блокови се линеарно поврзани едни со други преку вредноста hash[55] на претходниот блок. Хешот на претходниот блок се користи за пресметување на вредноста на хешот на тековниот блок, додека првиот блок нема претходен блокски хеш и се нарекува „блок Genesis“. При додавање нов блок во мрежата, блокчејнот користи механизми за консензус како што се доказ за работа (PoW) и доказ за учество (PoS). Секој блок содржи различни полиња кои можат грубо да се категоризираат како на сликата подолу.

[55] hash - ознака што се користи за означување и поврзување на блокови




Слика 19: Структура на блок (извор: сопствена креација)

Горенаведената слика ќе создаде поедноставна визуелизација на концептуалниот блок во вашата глава. Сепак, самиот блок содржи многу повеќе информации од сликата погоре. Сега ќе ги објасниме позначајните елементи на блокот што се прикажани на сликата:

- Големина на блок: Големината на ова поле е 4 бајти и ја содржи големината на блокот.
- Заглавие на блокот: Големината на заглавието на блокот е 80 бајти. Дополнително содржи различни полиња.
- Бројач на трансакции: Ова поле го содржи бројот на трансакции, а неговата големина е помеѓу 1 и 9 бајти.
- Трансакции: Ова поле ги содржи трансакциите на блокот и неговата големина е променлива.

Заглавието на блокот содржи различни полиња за метаподатоци, кои се:

- Hash на претходен блок: Секој заглавие на блокот дава информации за претходниот или родителскиот блок. Ова поле ја содржи хеш вредноста на

претходниот блок и оваа референца ги поврзува сите блокови. Големината на ова поле е 32 бајти.

- Version: Ова поле го складира бројот на верзијата за да означи надградби на софтверот. Големината на полето за верзија е 4 бајти.
- nBits: Поле од 4 бајти кое ја кажува сложеноста на додавањето блок. Исто така е познато како „Тешкотија“. Според PoW, хешот на блокот треба да биде помал од nBits.
- Timestamp: Ова поле го содржи времето кога е креиран блокот. Големината на ова поле е 4 бајти.
- Nonce: Вредност што се користи за време на рударењето блокови. Големината на ова поле е исто така 4 бајти.
- Merkle tree root: Мерклово дрво е структура што се добива со хеширање на податоците за трансакцијата на блок. Коренот на ова дрво е зачуван во заглавието на блокот под ова поле. Големината на полето е 32 бајти.

Секој нов запис или трансакција во рамките на блокчејнот подразбира изградба на нов блок. Секој запис потоа се проверува и дигитално се потпишува за да се осигури неговата автентичност. Пред тој блок да се додаде во мрежата, мора да биде потврден од мнозинството јазли во системот.

### 7.2. Основни видови блокчејни

Кога зборуваме за видовите блокчејн технологија, разликуваме 4 основни видови: јавни, приватни, конзорциумски и хибридни блокчејни (Башир, 2017, стр. 545)[56]. Јавните блокчејни дозволуваат секого да се придружи и се целосно децентрализирани. На јавните блокчејни, сите јазли имаат еднакви права за пристап до блокчејнот, можат да креираат нови блокови на податоци и да валидираат блокови на податоци. Досега, јавните блокчејни главно се користеа за размена и рударење криптовалути. На овие јавни блокчејни, јазлите „рударат“ криптовалути со креирање блокови за трансакции што се бараат на мрежата преку решавање на криптографски равенки. Како награда за нивната работа, рударите добиваат одредена количина криптовалути.

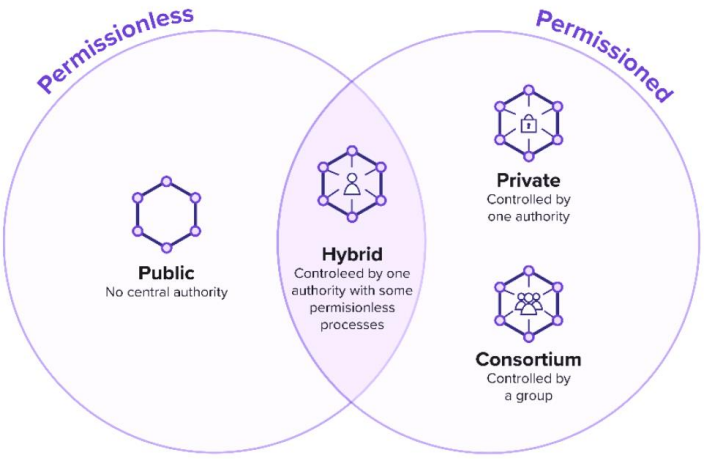
[56] Imran Bashir (2017). Mastering Blockchain , Packt Publishing.

Приватните блокчејни се контролирани од една организација. Во приватен блокчејн, еден централен орган одредува кој може да биде јазол и не мора да им доделува еднакви права на сите јазли за извршување на функциите. Приватните блокчејни се само делумно децентрализирани бидејќи јавниот пристап до тие блокчејни е ограничен. Примери за приватни блокчејни се Ripple и Hyperledger.

И приватните и јавните блокчејни имаат свои недостатоци - јавните блокчејни често имаат подолго време на потврда за нови податоци во споредба со приватните блокчејни, додека приватните блокчејни се поранливи на измами и несакани актери. За да се решат овие недостатоци, развиени се конзорциумски и хибридни блокчејни.

Хибриден блокчејн е комбинација од приватен и јавен блокчејн, како што сугерира името. Овој вид се стреми да ги искористи двата вида. Во хибриден блокчејн, не сите членови имаат еднакви права да потврдуваат трансакции. Само одреден број членови имаат одредени привилегии поврзани со валидноста на трансакциите. Други членови можат да учествуваат во потврдата, но тој избран број членови мора да постигне консензус пред да се изврши трансакцијата.

Овој пристап овозможува одредена децентрализација на овој тип блокчејн, иако сè уште се наклонува кон централизација, што резултира со побрзо извршување на трансакциите на мрежата. Главните карактеристики на хибриден блокчејн се дека јазлите можат да бидат само претходно избрани членови, дека не на секого му е дозволен пристап до мрежата и дека идентитетите на членовите на мрежата се познати однапред. Четвртиот и последен, конзорциумски блокчејн, познат и како федеративен блокчејн, е сличен на хибриден блокчејн по тоа што има карактеристики и на приватни и на јавни блокчејни. Сепак, се разликува по тоа што повеќе организациски членови соработуваат на децентрализирана мрежа. Во суштина, конзорциумски блокчејн е приватен блокчејн со ограничен пристап до одредена група, елиминирајќи ги ризиците што доаѓаат со тоа што еден ентитет ја контролира приватната блокчејн мрежа. Во конзорциумски блокчејн, процесите на консензус се контролирани од претходно дефинирани јазли. Постои валидаторски јазол кој иницира, прима и валидира трансакции. Членовите на јазлите можат да примаат или иницираат трансакции.




Слика 20: Основни типови на блокчејни (извор: „Types of Blockchain: Public, Private, or Something in Between“. (2021): https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between)

### 7.3. Како функционира блокчејнот

Бидејќи веќе подетално ја објаснивме структурата и основните компоненти на блокот во претходните делови, потребно е да се разјаснат 4 клучни компоненти за целосно да се разбере како функционира блокчејнот, а тоа се дистрибуираната книга, peer-to-peer мрежата (P2P), механизмот за консензус и криптографските клучеви. Според (Daniel Drescher, „Blockchain Basics“, (2017) криптографските клучеви се поделени на приватни и јавни клучеви, а секој учесник или јазол ги поседува двата клуча[57]. Тие се користат за креирање дигитален потпис. Дигиталниот потпис претставува единствена и безбедна дигитална идентификација и е најважниот аспект на блокчејн технологијата. Секоја трансакција е сертифицирана со дигиталниот потпис на сопственикот.

Секој нов корисник (јазол) што се приклучува на peer-to-peer блокчејн мрежата добива целосна копија од системот. Кога се креира нов блок, тој се испраќа до секој јазол во рамките на блокчејнот на системот. Секој јазол може независно да провери дали дадените информации се точни. Ако сè е во ред, блокот се додава во локалниот

[57] Daniel Drescher, „Blockchain Basics“, (2017): https://app.scnu.edu.cn/iscnu/learning/block_chain/Blockchain%20basic.pdf

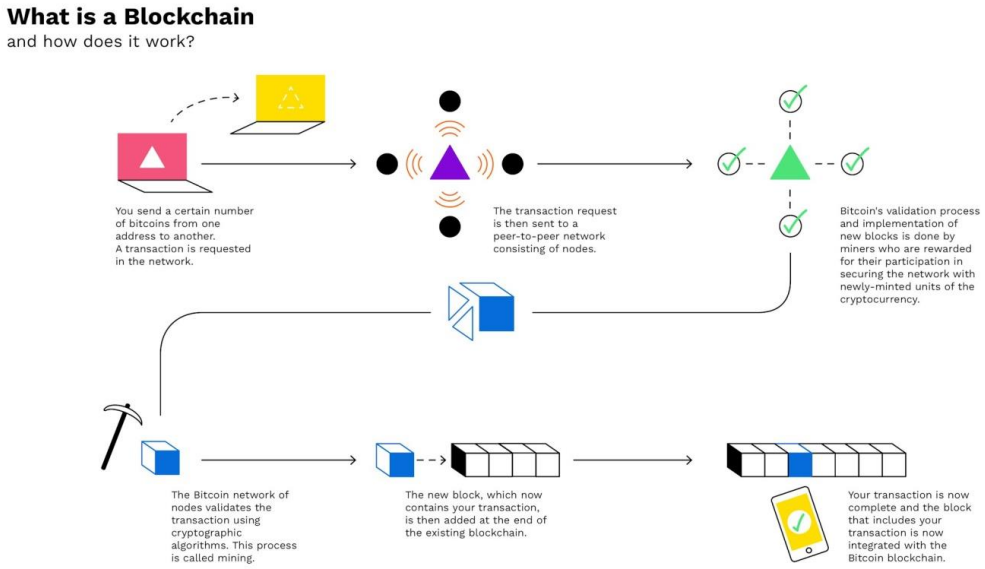
блокчејн во секој јазол. Мора да напоменеме дека работи првенствено на децентрализиран систем.

Механизмите за консензус се збир на правила што одредуваат како децентрализираната компјутерска мрежа постигнува договор за тоа кои трансакции се валидни, а кои не. Тоа е апсолутно суштинска компонента на секоја блокчејн мрежа. Двата најпопуларни механизми се механизмите Proof-of-stake и Proof-of-work. Во блокчејнот Proof of Work, сите јазли учествуваат во процесот на рударење криптовалути за да се обезбеди точноста на секој новокреиран блок. Во блокчејн „Proof-of-stake“, сите учесници ги потврдуваат сите трансакции, вклучувајќи ги и трансакциите вклучени во блокови што ги додале други јазли.

Сите трансакции се чуваат во дигитална книга наречена *дигитална книга (DLT)*. Дигиталната книга функционира како табела што ги содржи сите бројни јазли во мрежата и има историја на сите купувања направени од секој јазол. Информациите содржани во дигиталната книга се исклучително безбедни, а дигиталниот потпис ја штити од манипулација. Она што е посебно кај оваа книга е тоа што секој може да ги види податоците, но никој не може да ги менува.

Сега кога накратко ги објаснивме најважните компоненти за функционирање на блокчејн, да ги разгледаме чекорите за додавање блок во блокчејн мрежата:

1. Јазол креира нова блокчејн трансакција користејќи ја својата компјутерска моќ.
2. Трансакцијата се споделува со сите јазли на блокчејн платформата.
3. Сите јазли пресметуваат равенки, ја проверуваат валидноста на блокчејн трансакцијата и можат да користат консензусни алгоритми за да донесуваат одлуки.
4. Јазлите гласаат едногласно за вклучување на трансакција во блок.
5. Еден блок може да содржи различни трансакции сè додека не се наполни.
6. На блокот се применува уникатен идентификатор, кој го содржи криптографскиот преглед на тековниот блок и прегледот на претходниот блок.
7. Блокот се додава во синџирот, а главната книга се ажурира на сите јазли.
8. Процесот на додавање блокови во блокчејн мрежата се нарекува рударење.




Слика 21: Како функционира блокчејн технологијата (Извор: https://www.bitpanda.com/academy/en/lessons/how-does-a-blockchain-work/)

## 7.4. Ограничувања на блокчејнот

Како и секоја технологија, блокчејнот не е совршен и има свои недостатоци и ограничувања. Некои од нив се однесуваат на скалабилноста, прилагодливоста, приватноста, начинот на кој е регулирана целата мрежа и фактот дека блокчејнот е релативно нова технологија и затоа сè уште не е целосно истражен.[58]

Со зголемената употреба на блокчејнот и постојаното зголемување на корисниците, се појавува проблем. Трансакциите се натрупуваат и системот не може да ги обработи доволно брзо. Со секоја трансакција, нов блок се додава во блокчејнот, а секој блок има сè повеќе податоци во него бидејќи ја содржи историјата на податоците од блоковите пред него. Блокчејн технологијата во моментов е премногу млада за да се поврзе и интегрира со постојните системи и не постојат два различни блокчејна кои можат лесно да комуницираат едни со други. За да се развива технологијата и да биде употреблива секојдневно на глобалниот пазар, треба да се развие некаков облик на стандардизација. Стандардизацијата би овозможила многу подобра интероперабилност и прилагодливост. Трансакциите извршени на блокчејнот се објавуваат глобално и не

[58] Bashir I., (2017) Mastering Blockchain. Birmingham UK: Packt Publishing.Ltd

се шифрирани во повеќето апликации што работат на блокчејнот. Доколку податоците видливи во трансакциите се лични податоци, на пример здравствени или финансиски податоци, се јавува проблем кој, во зависност од земјата, може да биде од правна природа. Ова би можело да се стави крај ако преку трансакциите се испраќаат само шифрирани податоци, но потоа се појавува проблемот дека ако клучот за дешифрирање на одредени податоци се изгуби, а исто така и ако клучот за дешифрирање е украден и податоците се објавени, сите податоци ќе бидат дешифрирани и објавени засекогаш на блокчејнот.

Во зависност од делот од светот, блокчејнот е регулиран различно и ова претставува голем проблем во однос на глобализацијата и глобалниот деловен пазар. На пример, во Европската Унија постои проблем со јавните блокчејн платформи и новата регулатива „Општа регулатива за заштита на податоци (GDPR)“ за заштита на личните податоци. Бидејќи податоците објавени на јавен блокчејн се достапни за сите, и доколку станува збор за лични податоци според новите регулативи за заштита на податоци, тие не треба да се откриваат. Во Источна Азија е во сила таканаречениот пристап „прво бизнисот, а потоа регулација“, според кој на компаниите од блокчејн им е дозволено да работат без никакви ограничувања. Кина, од друга страна, има целосно ограничување на операциите со криптовалути, со што се ограничува и самата блокчејн технологија и нејзиниот напредок. Додека земји како Јужна Кореја ја прифаќаат блокчејн технологијата и нејзините можни иновации, бизнисите што ја користат сè уште воопшто не се регулирани.[59]

Да заклучиме дека блокчејн е многу интересен концепт што би можел да го поедностави, а не нужно да го олесни бизнисот на глобално ниво доколку може да се постигне договор за неговата регулација и проблемот со скалабилност што во моментов го задушува огромното мнозинство од сообраќајот на блокчејн.

[59] Bashir I., (2017) Mastering Blockchain. Birmingham UK: Packt Publishing.Ltd.

## Заклучок

Дигиталната економија е резултат на процесот на трансформација што го носат ИКТ, или информатичко-комуникациската технологија. Таа е во постојан развој и нејзините модели претставуваат вистинска бизнис револуција. За да се имплементира дигиталната технологија во компаниите, потребно е да се спроведе целата дигитална трансформација на компанијата, од глава до пети. Потребно е полека да се опфатат сите сектори за да дигитализацијата на бизнисот биде валидна, функционална и, пред сè, профитабилна. Дигиталната трансформација се стреми да помогне во развојот на самиот живот, на компаниите и на самите градови, преку клучни технологии како што се BigData, програмите за паметни градови, сајбер безбедноста и Интернетот на нештата. Сите овие технологии изгледаат далечна во иднината, но секој ден бројот на IoT уреди расте експоненцијално. Паралелно со развојот на дигиталната економија, доаѓаат и виртуелните пари, или криптовалути. Тие претставуваат дигитална репрезентација на одредена вредност што нема карактеристики на реални или фиат пари. Она што е важно е блокчејн технологијата, која носи напредок во компјутерскиот и деловниот сектор. Иако е ново име во светот на технологијата, таа доби огромна популарност во текот на две генерации криптовалути, Биткоин и Етереум. Иако денес постојат илјадници видови криптовалути, овие две криптовалути „пишуваат историја“; Биткоинот како прва криптовалута досега и Етереум кој црпи повеќе можности од блокчејн технологијата. Криптовалутите добија неверојатна популарност. Ова го покажуваат и фактите за тоа колку е вреден пазарот на криптовалути, бидејќи многу земји и големи корпорации ги прифаќаат криптовалутите како мерка за вредност и средство за размена.

Криптовалутите се феномен со кој се справуваат економисти, адвокати, ИТ експерти, хакери, централни банки и безбедносни служби. Една од причините што првично ги привлече поддржувачите на технологијата, интернетот и инвеститорите е фактот што криптовалутите не се предмет на контрола од централните банки или владини агенции, туку нивната вредност ја одредуваат мноштво компјутери. Имено, тие се заштитени од инфлација со математичка функција што спречува нивното количество да се зголеми над однапред одредена граница. Друга карактеристика на криптовалутите, препознаена како предност, се рефлектира во елиминирањето на посредниците, што ги прави трансакциите поевтини - особено во меѓународните плаќања. Предноста на

криптовалутите е што тие се базираат на децентрализиран систем без постоење на регулаторен орган. Од друга страна, токму децентрализацијата, анонимноста на корисниците и отсуството на регулаторна агенција се покажуваат како главен недостаток. Со оглед на тоа што понудата на криптовалути е речиси неограничена, а побарувачката е неизвесна, долгорочниот раст на вредноста не е одржлив. Дури и ако одеднаш изгубат вредност, што е реално сценарио, криптовалутите веќе понудија придонес за разбирање на функционирањето на парите, придобивките од користењето пари и подобрувањето на плаќањата. Слично на фактот дека во 20 век американскиот долар служеше како глобална валута, честопати само затоа што повеќето луѓе во светот веруваа дека САД и неговиот финансиски систем ќе имаат најдобри шанси за опстанок, криптовалутите се поткрепени само со доверба. Вкупната вредност на сите криптовалути е само неколку милијарди долари и тие постојат како протокол што се извршува од далечина. Затоа, тие ќе постојат паралелно со постојните валути. Иако нивното присуство ќе биде релативно мало, тие можат да се користат како средство за пресметка како SDR - кои првично беа замислени како светска валута. Горенаведените сличности претставуваат и единствени паралели помеѓу криптовалутите и наднационалните валути како што се еврото или специјалните права на влечење.

Криптовалутите можат да се наметнат како посакуван начин за трансфер на пари. Имено, трансферот на пари врз основа на криптовалути не се потпира на банки или други посредници што ги користат современите системи. Затоа, нема високи провизии или високи трошоци. Според тоа, доколку комисиите за хартии од вредност и/или агенциите одговорни за надзор на финансиските услуги го поддржат воспоставувањето фондови или индекси поврзани со криптовалути или одобрат слични иновации или деривати, вредностите на криптовалутите дополнително би се зголемиле. Сепак, токму употребата на криптовалути во меѓународниот бизнис ги истакнува нивните недостатоци. Прво, правната несигурност и неприфаќањето на криптовалутите од страна на регулаторите го забавуваат процесот на пошироко прифаќање. Во исто време, овој процес е попречен и од честите случаи на сајбер криминал.

Во овој поглед, безбедноста на самите трансакции е обезбедена од блокчејн технологијата. Блокчејн, како технологија која не би дошла до израз доколку Биткоинот не добиеше популарност, е значаен фактор во развојот на финансиските пазари. Со усвојувањето на блокчејн технологијата во бизнисот и меѓународната размена, можноста за широка употреба на криптовалути добива на значење бидејќи

компаниите би ги користеле криптовалутите повеќе меѓу себе, елиминирајќи ги посредниците. Покрај тоа, блокчејн технологијата може да има широка примена независно од финансиските пазари, како што се водење на граѓански регистри, разни регистрации, проверка на здравствени картички, гласање на избори итн. Сепак, блокчејн е само првиот регистриран обид за контрола на испраќањето електронски пари. Создавањето и одржувањето на децентрализирана мрежа е сложена задача која бара многу поголеми ресурси (време, поврзаност и обработка) од централизираните мрежи. Според тоа, максималниот опсег на криптовалутите е да симулираат модерно електронско клиринг на глобално компјутеризирано општество. Затоа, тие претставуваат само привремено решение кон поширока употреба на децентрализирани бази на податоци и приватни пари. Во моментот кога ќе се појави проблем што една валута не може да го надмине, на нејзино место ќе се појави друга валута, која ќе содржи елементи што го надминуваат тој недостаток. Точно така функционира интернетот. Ако некоја страница или апликација на интернет исчезне, тоа нема да доведе до исчезнување на интернетот, туку друга ќе се појави на нејзино место.

## Користена литература


1. Antonopoulos, A. M., & Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O'reilly Media.
2. Aysan, A. F., Khan, A. U. I., & Topuz, H. (2021). Bitcoin and altcoins price dependency: Resilience and portfolio allocation in COVID-19 outbreak. Risks, 9(4), 74.
3. Bashir I., (2017) Mastering Blockchain. Birmingham UK: Packt Publishing.Ltd
4. Bccrwp (2019), Open Source vs zatvoreni izvor za Cryptocurrency novčanike: https://hr.bccrwp.org/compare/open-source-vs-closed-source-for-cryptocurrency-wallets-466458/
5. Bresnahan, T.F.; Trajtenberg, M. General purpose technologies “Engines of growth”? J. Econom. 1995, 65, 83–108.
6. Buterin, V.: Ethereum white paper: a next generation smart contract & decentralized application platform (2013). Available: Ethereum Whitepaper | ethereum.org
7. CFI Team, Smart Contracts. https://corporatefinanceinstitute.com/resources/valuation/smart-contracts/
8. CoinMarketCap. Cryptocurrency Prices, Charts and Market Capitalizations. 2021. Available online: https://coinmarketcap.com/
9. Daniel Drescher, „Blockchain Basics“, (2017): https://app.scnu.edu.cn/iscnu/learning/block_chain/Blockchain%20basic.pdf
10. De Best, R. Market Capitalization of Cryptocurrencies from 2013 to 2020. 2021. Available online: https://www.statista.com/statistics/730876/cryptocurrency-maket-value/
11. Decker, C., & Wattenhofer, R. (2014, September). Bitcoin transaction malleability and MtGox. In European Symposium on Research in Computer Security (pp. 313-326). Springer, Cham.
12. DOMINGUEZ, Nick. These are 11 Real World Use Cases for Ethereum [online]. CoinDiligent, 2020: https://coindiligent.com/ethereum-real-world-use
13. Ether Total Supply and Market Capitalization Chart [online]. Etherscan, 2020: https://etherscan.io/stat/supply

14. http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, str. 13., 2019.
15. https://hackernoon.com/everything-you-need-to-know-about-smart-contracts-a-beginners-guide-c13cc138378a, 2019.
16. https://www.cryptonewsz.com/why-did-buterin-create-ethereum/23077/, 2019.
17. Investopedia (2022) How to Invest in Cryptocurrency: https://www.investopedia.com/investing-in-cryptocurrency-5215269
18. Kurt Dugan (2018). Blockchain for Beginners: Understand the Blockchain Basics and the Foundation of Bitcoin and Cryptocurrencies, CRB Publishing.
19. Lansky, J. Analysis of cryptocurrencies price development. Acta Inform. Pragensia 2016, 5, 118–137.
20. Lewis, A. (2018). The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them. Mango Media Inc..
21. Lider, Ethereum ima snažan ekosustav i s razlogom je druga najveća kriptovaluta: https://lider.media/poslovna-scena/hrvatska/ethereum-ima-snazan-ekosustav-i-s-razlogom-je-druga-najvecakriptovaluta-136774
22. Mnif, E.; Jarboui, A. COVID-19, bitcoin market efficiency, herd behaviour. Rev. Behav. Financ. 2021, 13, 69–84.
23. Nerdwallet (2023) Cryptocurrency, Explained: A Guide for Beginners; https://www.nerdwallet.com/article/investing/cryptocurrency
24. Nick Szabo, „Smart Contracts“ (1994): https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
25. Okoba, G. (2023). Solidity for Beginners: understanding the features of Solidity.https://coinsbench.com/solidity-for-beginners-understanding-the-features-of-solidity-53adc9a19d1e
26. Solomon, M. G. (2019). Ethereum for dummies. John Wiley & Sons.
27. State of the DApps [online]. State of the DApps, 2021: https://www.stateofthedapps.com/dapps
28. Stroukal, D. (2018). Can Bitcoin become money? Its money functions and the regression theorem. International Journal of Business and Management, 6(1), 36-53.

29. Szabo, N. Formalizing and Securing Relationships on Public Networks. First Monday, 2,9. (1997), str 1, https://doi.org/10.5210/fm.v2i9.548
30. Taipale, S. Intergenerational Connections in Digital Families; Springer: Berlin, Germany, 2019.
31. The Investopedia Team (2024). What Are Smart Contracts on the Blockchain and How Do They Work? https://www.investopedia.com/terms/s/smart-contracts.asp
32. Token Tracker [online]. Etherscan, 2020: https://etherscan.io/tokens
33. Top Accounts by ETH Balance [online]. Etherscan, 2020: https://etherscan.io/accounts/c
34. Umar, M.; Su, C.-W.; Rizvi, S.K.A.; Shao, X.-F. Bitcoin: A safe haven asset and a winner amid political and economic uncertainties in the US? Technol. Forecast. Soc. Chang. 2021, 167, 120680.
35. Unalan, S.; Ozcan, S. Democratising systems of innovations based on Blockchain platform technologies. J. Enterp. Inf. Manag. 2020, 33, 1511–1536.
36. Vigna, P., & Casey, M. J. (2015). Cryptocurrency: how Bitcoin and digital money are challenging the global economic order. (No Title).
37. Vogels, E.A. Millennials Stand Out for Their Technology Use, But Older Generations Also Embrace Digital Life. 2019. Available online: https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/
38. Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P.: A survey on consensus mechanisms and mining strategy management in blockchain networks. (2019)
39. Werkheiser, B. (2023). What is Solidity? https://www.alchemy.com/overviews/solidity
40. WHAT IS ETHEREUM 2.0 AND WHY DOES IT MATTER? [online]. EC-Council, 2021: https://blog.eccouncil.org/what-is-ethereum-2-and-why-does-itmatter/
41. Yermack, D. (2015). Is Bitcoin a real currency? An economic appraisal. In Handbook of digital currency (pp. 31-43). Academic Press.
42. Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. (2020).

43. Проф. д-р Зоран Колев, Криптовалута – злато на интернет, Статија во „е-Банкар“ број 9, https://www.abit.edu.mk/News2e53.html?IdNews=153&IdLanguage=1&IdRoot=1