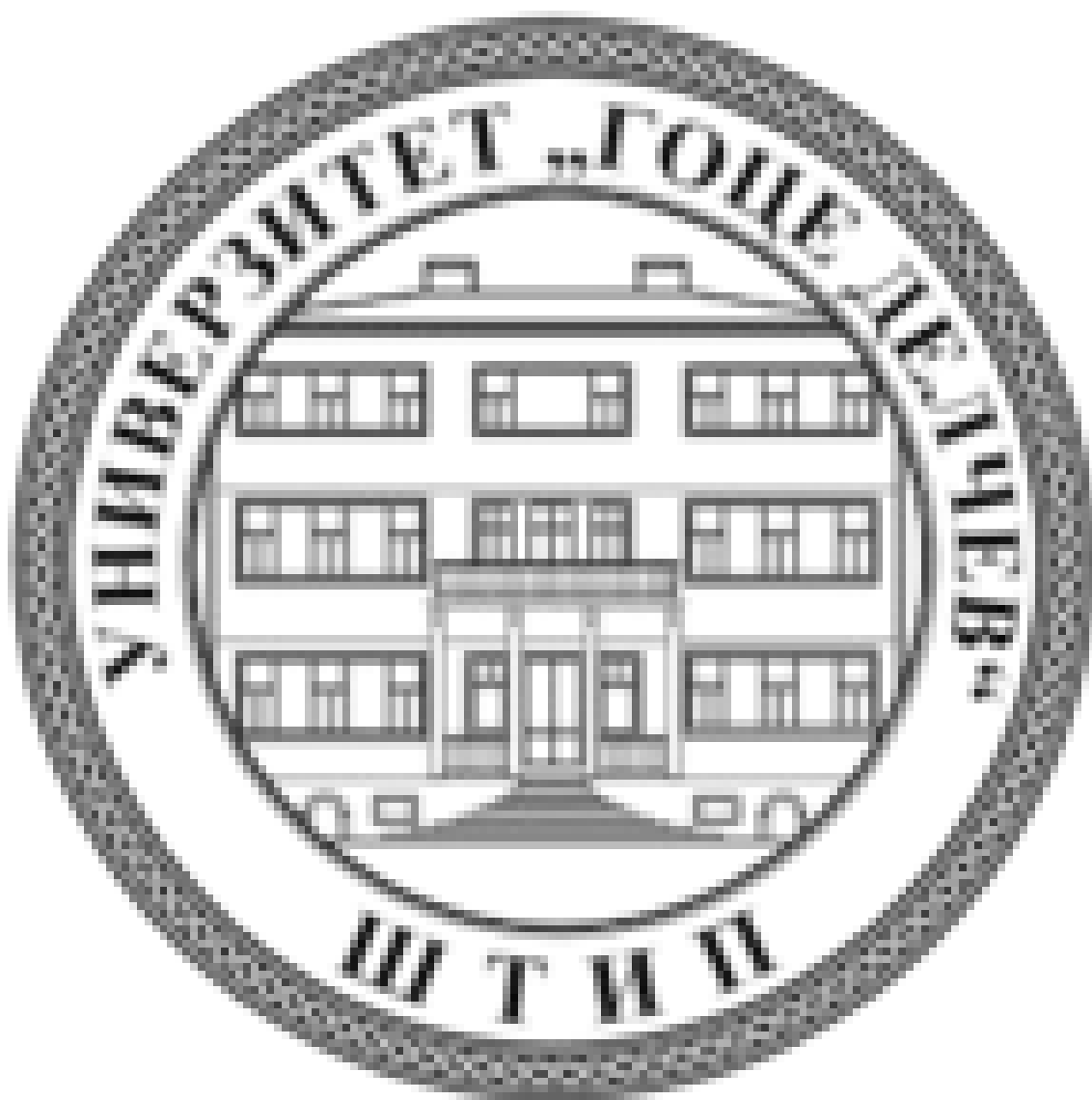


Електронски Пари

Криптовалути



Изработил
Ристе Петров
број на индекс 084129
насока Финансии

Намерно оставена празна страна

Содржина

Содржина	3
Историјат на парите	4
Што е тоа криптовалута?	7
Разлики помеѓу критповалутите и електронските пари	8
Важноста на трансакцискиот систем базиран врз синџир и видови на протоколи за негово спроведување	9
Поделба на критовалутите според технолошки фактори	14
Проблеми со кои се сочуваат синџирите	18
Криптовалута	20
Како се анализира криптовалута? И каков потенцијал може истата да има?	22
..... Технолошка анализа	22
..... Пазарен потенцијал и состојба	23
..... Конкуренција	24
..... Корисници / Конзументи	24
..... Менаџерски тим	24
..... Акционерски склоп/Поседувачи	25
..... Углед, Односи со јавноста	25
Сортирање на критовалутите	26
Децентрализирани Менувачници (DEX)	27
Стабилни коини	27
Незаменливи токени (НФТ)	28
Бирање на централизиран пазар на кој што ќе се тргува со криптовалутин	28
Користени извори	30

Пред да се посветиме внимание на Електронските Пари поточно на најновата иновација во електронските пари би било пожелно да ја погледнеме накратко историјата на парите. Како истите еволвирале и на кој начин се одвивало плаќањето во општеството.

Историјат на парите

Како прва појава на наплата се појавила трампата или размената. Ова и најпримитивната појава на парите, луѓето кои што живееле во племенски заедници ги разменуваале своите производи едни со други со цел да преживеат и истовремено секој да придонесува кон општеството со сопствената специјалност.

Со еволутивниот тек трампата преминала во стандардизирани предмети искористени за размена во одредени општествени заедници т.е се користеле ножеви, кожа, вино како унифицирана вредност за замена и трансакција на производи во општеството.

Со развојот на технологијата дошло до развивање на обработката на металите и така трговијата преминала од стандардизирани предмети искористени за размена кон трговија со користење на метали. На почетокот се користеле не благодарни метали, подоцна се користеле благородните метали.

Благородните метали се појавиле во форма на пенсаторен (нестандардизиран со цели групи метали се вршела размената) и нумерички со создавање на ковани пари во форма на монети со различни финости. Појавата на нумеричката форма на размена со благородни метали го модернизирала начинот на размена и го направила побезбеден за сите вклучени страни во трансакцијата со што и го убрзала текот на економијата. Како главни ковани монети биле златните, но поради нивната голема вредност истите биле заменувани за сребрени или бакарни за да се наплатуваат секојдневни трошоци или помали трансакциски суми.

Книжни пари настанале како резултат на разрешувањето на проблемите кои ги предизвикувале монетите од благородни метали. Благородните метали само по себе имале голема вредност и поради тоа голема била шансата за кражба, со цел да се избегне ова се создале потврдите (како први форми на книжени пари) со кои се заложувале монетите кај златари или во банка и со тие потврди се вршела размената во трговијата место да има размена на самите монети.

Со зголемувањето на економијата и општото богатство истиот проблем кој што ја предизвикал транзицијата од монети кон книжни пари го забрзал развојот кон жиралните пари. Жиралните пари се всушност потврди кои што сопственикот ги има депонирано во одредена банка и истите може да ги искористи без да ги подигне и да ги размени своите потврди со помош на жиралните пари. Само истите потврди ја променуваат сопственоста кон другата засегната страна во трансакцијата, самите потврди остануваат во банката цело време само што се отуѓува сопственоста со помош на жиралните пари. Жиралните пари го убрзале развојот на економијата и од тука почнало развивањето на финансискиот пазар за пари, почнале банките да издаваат кредити и економијата во краток временски период го дуплирала своето богатство. Покрај појавата на жиралните пари кон ова допринело и отуѓувањето на вредноста на книжените пари кон одреден метал туку се засновале на општествената прифатеност да се тргува со одредена валута.

Најголема заслуга за ова ја има доларот кој во 1971 година од страна на претседателот Никсон, со што во следните декади ќе ја промени судбината на парите на глобално ниво.

Денеска парите имаат поткрепа на други валути и економијата е испреплетена во мрежа, ова го овозможува глобалниот прираст на економијата но истовремено овозможува и глобален пад на економскиот прираст. Со оваа промена се овозможува поголемо задолжување, т.е банките се задолжени да задржуваат само мал дел од депозитите, а остатокот да го искористуваат да издаваат кредити без да имаат депозити за истите (се додека се ликвидни).

Како една од последните промени е појавата на електронски пари, со цел да се забрза текот на жиралните пари и да се поефтини процесот на трансакција од банка кон банка во различни економии. Се формира SWIFT (Друштво за светски меѓубанкарски финансиски телокомуникации) преку кој се вршат сите меѓу гранични трансакции на жирални/електронски пари, овој процес е централизиран и доколку од различни фактори настане проблеми во трансакциите текови во SWIFT може да се појават глобални проблеми во трансакциите измеѓу финансиските институции.

Доколку приметивте финансиската размена, со текот на еволутивниот тек преминува од децентрализирана примитивна размена, кон централизирана размена на технолошко развиени жирални пари со централизиран систем (врз кој сите вклучени страни во системот зависат од неговото оперирање). За да се избегнат можните проблеми еволутивно се настанати криптовалутите кои што се децентрализирани платежни средства кои што функционираат со помош на милиони различни компјутери. Истите ги поседуваат главните карактеристики кои што ги поседувале како предност ковните пари кои што го олесниле текот на трансакција и го модернизирале текот на средства во економијата. А тие комперативно се:

Карактеристики	Ковани пари	Криптовалути
Заменливост	Поради хомогеноста, возможно било различни парчиња од ист метал да бидат еднакви по квалитет	Исто како жиралните пари истите може лесно да се разменат и до најситни фрагменти од истата криптовалута.
Деливост	Овие метали моат лесно да се делат и на најситни делови	Скоро сите криптовалуди имаат деливост многу поголема од електронските пари до 6, некој дури и до 20 децимални места
Ковност/	Можат лесно да се коваат во различни форми и да се носат	Потребата од ковност или физички пренос е непотребна. Но истите можат да се коваат доколку има такво барање. Постојат криптовалуди кои што се во физичка форма или се поткрепени со залихи од одреден метал. Покрај ова има можност од ковност/отсликување на шифрите кои даваат пристап кон новчаникот со криптовалуди.
Трајност	Не се распаѓаат	Се додека постои мрежата, т.е има компјутери кои што прават трансакции истите постојат. Исто додека не се изгуби пристап до нив.
Лесна препознатливост	Особено златото лесно се препознава и постојат реагенси кои	Со минимални трансакции и со проверка од страна на мрежата

	што можат да го препознаат	може да се потврди сумата. (се избегнува инфлација и двојно трошење)
Преносливост	Златото има добра преносливост на богатство	Криптовалутите во USB уред од неколку мегабајти може да се пренесе богатство вредно колку цела економија на средно развиена економија.
Корисност	Благородните метали немаат посебна корисност во индустријата.	Криптовалутите се 0 и 1 во компјутерската меморија и исто како електронските/жиралните пари немаат значителна корисност во индустријата.
Постојана вредност	Златото има голема стабилност.	Имам посебен вид на криптовалути кои што се создадени со цел да имаат еквивалентна вредност на друга валута и истите се користат за постојана вредност и намален ризик од волитет.

Што е тоа криптовалута?

Криптовалута според википедија претставува колкција од бинарни податоци кои се дизајнирани да работат како медиум за размена/платежно средство. Етимолошки зборот криптовалута доаѓа од зборовите, “cryptos” – старогрчки за скриено и валута – што во буквален превод означува скрена валута.

Покрај буквалниот превод на овој поим не можеме да кажеме дека сите валути се скриени, и носат со себе потполна приватност. Почетоците во овој технолошки напредок се почнати со ориентираност кон прикривање на идентитетот на сопствениците на самите средства, и од таму доаѓа самото име.

Почетоците на криптовалутите почнуваат со развивањето на криптографската наука, криптографот Давид Чаум во далечната 1982 ги создава криптографските анонимни електронски пари наречени Екеш(еготовина). Неговиот концепт заживнува во 1995 година со неговата фирма ДигиКеш, тој се обидел со користење на криптографска технологија да направи енкриптирани(шифрирани) клучеви кои ќе може да се искористат во банките за да се извршат трансакции без да се знае идентитетот на сопственикот на средствата од страна на ниту една инволвирана страна (банка, држава или друго трето лице). Покрај тоа што системот профункционирал во повеќе банки како Кредит Свис во Швајцарија, Германска Банка во Германија, Банка на Австралија и многу други финансиски институции сепак бил истиснат од конкурентната услуга на кредитни картички. Членувањето во овој систем било бесплатно за корисникот, а трошоците за одржување ги плаќале трговците кои ја нуделе услугата како можност за наплата (на ист модел како што кредитните картички ја наплатуваат својата услуга). По пропастиот во 1998 следува декада на мрачна доба за криптовалутите до основањето на Биткоинот како прва криптовалута основоположник на филозофијата и појавата на криптовалутите на глобално ниво.

Со развитокот на криптографијата, и напредоци во математиката доаѓа до создавање на SHA-256 криптографскиот протокол, овој протокол е од големо значење за светот на криптографија бидејќи е основоположник на заштитата на податоците на глобално ниво и е од исклучиво значење за безбедноста на криптографските клучеви на повеќето криптовалути.

Во 2009 доаѓа до создавање на Биткоинот кои што е создаден благодарение на развитокот на интернетот и развивањето на конектирањето конекција со конекција(peer to peer), наместо со досега раширениот систем на конекција кон сервер и од серверот да се превземаат податоците. Генијалноста на оваа технологија е што се формира информационе систем во кој безбедно може да се запишуваат сите тековни трансакции во форма на синцир притота да нема мешање од трансакциска сметка/новчаник и воедно можноста за двојно трошење. Овој начин на менаџирање на финансиски средства досега не бил возможен и барал централна контрола и различни одбрамбени механизми, воедно и прифаќање на одреден морален ризик од страна на корисниците па и посредниците за не исплата или невозможност за повлекување на средства од страна на посредникот во наплатата (банката).

Разлики измеѓу електронските пари и криптовалутите

Електронските пари според дефиниција на Википедија претставуваат секоја валута, пари, или слична на пари која примарно е менаџирана, складирана или разменувана на дигитален компјутерски систем претежно преку интернет. Како подгрупа спаѓаат и криптовалутите иако сите останати валути се во форма на централизирани дистрибутирани бази на податоци кои се во сопственост на компанија, банка во форма на дигитални документи или во форма на електронски картици.

Покрај тоа што според класификацијата на Википедија криптовалутите претставуваат под група на електронските пари сепак имаме значајни разлики кои што ја менуваат природата на трансакцијата. А тие се:

- структурата – има скоро отсуство од структура т.е нема лица со поголем или помал приоритет, не постои ентитет кои што го контролира самиот систем.

- автономност во споредба со сопствеништво – јавната база на податоци е во ништина сопственост, трансакциите ги извршуваат копачи/одобрувачи, сите одобрувачи/копачи имаат копија од ланецот на трансакции и на тој начин се решаваат проблемите на двојно потрошување и манипулација со истиот.

- саморегулирање наспротив централен администратор – кај дигиталните пари обично сопственикот/менаџерот проверува дали може да се изврши трансакцијата или доколку се направи договор за одложено плаќање самиот менаџер го превзема ризикот. Споредствено кај криптовалутите имаме регулирање од операторите (одобрувачи и копачи) кои раководат со синџирот на трансакции а поради нивната работа (потрошена електрична енергија за да го најдат решението на трансакцијата) добиваат награда.

- леснотија за пристапност – криптовалутите не бараат лиценци, дозволи или пак посредници кои овозможуваат да се користат средствата, секој кој има мобилен телефон или компјутер може да го симне новчаникот на криптовалутата која што сака да ја користи. Доколку неговиот уред му го дозволува истот може да учествува во процесот на саморегулирање. Нема непотребни трошоци за посредници има само трансакциски трошоци кои одат кон регулаторите (копачите/одобрувачи на трансакции)

- транспарентност – споредствено со другите видови на дигиталните пари, криптовалутите се транспарентни во својот софтверски дизајн и код. Секој може да го види, да го копира и искористи за да направи сопствена криптовалута, со помош на оваа карактеристика нонстоп се надградуваат истите се прават нови иновации и се подобрува сигурноста во истите.

- потполна контрола – тој кој што управува со новчаникот/сметката на криптовалутите има апсолутна контрола врз истите, т.е секој сопственик е одговорен за постапките како операциона безбедност, заштита од хакерски напади и долку сака може да ги поништи своите средства. Имам потполен избор за употреба на истите, за помалку софистицираните корисници постојат услуги кои што нудат менаџирање на истите.

Сумирано сите видови на децентрализирани бази на податоци во форма на синџир кои служат како средство за размена може да ги наречеме криптовалутите.

Вакви постојат од околу илјадници до десетици илјадници на различни криптовалути со различна пазарна цена, различни принципи на работа, различен број на единици во оптек од криптовалута, различна цел и различно решение на одреден проблем. Некој од нив имаат финансиски импликации, а некој од нив пак немаат никакви финансиски или пак општествени импликации, со технолошкиот развој се дава можноста да се создадат најразлични видови на криптовалути.

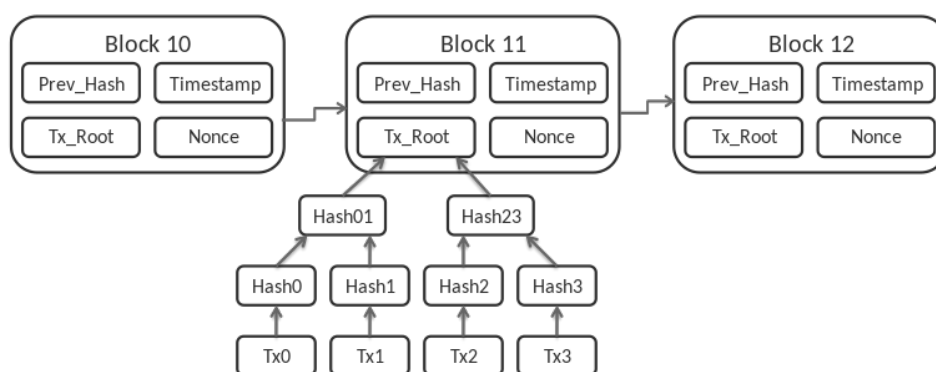
Важноста на трансакцискиот систем базиран врз синџир и видови на протоколи за негово спроведување.

Како што видовме како фирмата ДигиКеш беше истисната од пазарот од својата конкуренција. Тоа се случи поради самиот факт дека тој начин на трансакции беше заснован на поддршка од банките. Т.е и покрај тоа што банките немаа сознание кој колку средства има, сепак истите ги складираа тие пари и ги сервисираа серверите. Сегашните криптовалути го решаваат тоа со децентрализирани податочни бази во форма на синџир од делчиња (blockchain).

За да ги разбереме крипто валутите ќе мораме да ја разбереме технологијата и како истите синџири функционираат. Според дефиницијата од Википедија синџир од делчиња претставува растечка листа со записиси, (наречени делчиња/blocks), кои што меѓусебно се поврзани со криптографија. Секое делче има :

- криптографскиот хеш/шифра/клуч од претходното делче
- печат со датум
- криптографски хешеви/клучеви од сегашната трансакција
- дополнителни метадата податоци (како обработувачот на блокот, наградата за истиот , износите во трансакциите).

Графички приказ на едно делче/block направен од страна на [Matthäus Wander](#).



Синџирот ја покажува состојбата на сите трансакции кои што се извршени, како што видовме во дијаграмот погоре во едно дече имаме повеќе трансакции. Делчињата имаат различен временски интервал на просечно формирање на нови делчиња наречено блоковско време (block - time) на различни алгоритми и при различни фреквенции на трансакции.

Биткоиот има блоковско време (block - time) од 10 минути.

Литекоиот има блоковско време од 2.5 минути.

Документчеин има блоковско време од 2 минути.

ЦПУ чеин има блоковско време од 1 минути.

Етериумот и Кардано имаат блоковско време од 20 секунди.






Чиа има блоковско време од 18.75 секунди или 32 блока секои 5 минути

Шугар чеин има блоковско време од 5 секунди.

Запишувањето на трансакциите се прави со помош на клучеви(hesh) кои се собираат во купчиња клучеви или блокови. Секој клуч покажува кон една трансакција. И доколку го знаеме истиот можеме да провериме дали истата трансакција е извршена или уште е во тек(се однесува на тоа дали уште треба да се изврши одреден паметен договор или пак нема доволно потврдувања на истата трансакција од страна на повеќе обработувачи за да може истата да се потврди како извршена).

Кај некои криптовалути имаме податоци за тоа кои се испраќачите и примачите на трансакциите, кај некој тие се непознати (т.е за секоја трансакција имаме користење на фиктивни адреси за една употреба), кај некои е транспарентен износот кој што се пренесува, кај некои само алгоритмот го знае износот и истот во клучот го маскира со издавање на 4-20 различни износи од кои еден е точниот при што го прави екстремно тежок процесот на проценка за износот.

Bitcoin Transaction 96e8800ba74cd0ecf95f49758c8c902aca436caf91265b0e69b8f1232a3a8b89

Share:     

block, address, transaction Search

Block	452687
Time	2017-02-12 12:38:34
Size	225 (bytes)
Total Input	0.13253788 BTC
Total Output	0.13053788 BTC
Fees	0.002 BTC

← prev tx 1PX6MLDcLUGwczwPRgde3ZJfLbYrJpRHnk -0.13253788 BTC	1AskNdvFmYuGK1Wd7zznFEjctKZX1ZfHVQ 0.11346388 BTC
	1P428y65VzBrfM2sr3VkKNWwoXkxBXERN9 0.017074 BTC wallet: 25920911

Fee: 0.002 BTC
Transaction sum: 0.13053788 BTC

[Light](#) / [Dark](#) | [Advertising](#) | [Privacy Policy](#) / [Disclaimer](#) | Contact: bitinfocharts@gmail.com

Еве како изгледа податоците од еден клуч. Овој клуч има големина од 225 бајти, направена е трансакцијата 12:38:24 на 02.12.2017. Оваа трансакција се содржи во блокот под број 452687.

Од адресата на десната страна се прфрлаат средства кон долната адреса од левата страна во износ од 0.017074 биткоини, а повратот кон адресата испраќач е 0.11346388 биткоини. Цената за извршување на трансакцијата изнесува 0.002 биткоини која се исплаќа на обработувачот.

Податоците се транспернтно доспатни на повеќе пребарувачи на биткоини. Доколку сакате да ја погледнете истата може да ја видите [тука](#).

Mining reward transaction

This is a public transaction summary. You can decode address and amount information with the options below.

Auto-refresh

 508,031 Confirmations Done!	Mining reward 2.04 XMR	Block 2,000,000	Size in KB 0.10
---	----------------------------------	---------------------------	---------------------------

Transaction ID
eae25672906c24ee26d95221476010854a936d50c8bdcd7e7935defc46306c8b

[Get a send receipt](#)

[Verify deposit](#)

Монеро како криптовалута која има енкрипција на трансакциите и износите во трансакциите, и помала транспарентност, истата бара да се внесат клучевите од новчаните на сопствениците кои ја пратиле или примиле трансакциската сума за да ја видат точната сум која што ја испратиле/примиле, единствен износ кој што се гледа е наградата за операторот која и неговата адреса на која се испраќа наградата.

Transaction f7128630fe4db53d19b9a0ed6a44f2aa8e117ae6b80ca6131a3557bd053b8305

Transaction status

- Fee: 0.0000
- Sum of outputs: 5.1089 (IRD)
- Size: 280

From Block

- Hash: [aeaa6f2afdbd6eb31b448f6ddb6719f07189b8c5996d15978fea50ad65a1f35e](#)
- Height: 767471
- Timestamp: 12/5/2021, 7:59:12 AM
- Confirmation: 5 / 20

Inputs

- Amount

Outputs

Amount	Key
0.00000439 (IRD)	2d00e28d00fd82ff3f938780fd8c2e71968c41b0b8eb99e8f367f6610bca66fc
0.00008000 (IRD)	0de662090f846cdf6ad5cfbd681257ce35bfdd4c5295e0ad70783d4ed0ff137
0.00080000 (IRD)	0f07ecc99ea5aca9b3c11edd64a8e060ab633d27664ee718bd0c4972d229921
0.00800000 (IRD)	667831023dd2bbd5087bdd29777e3f763f38863b9178fab55d4f5ca4de74c29f
0.10000000 (IRD)	4f04dce3d1130fd3b88794ff91bb589bea70cd49ba2fd0f1182dec0216014601
5.00000000 (IRD)	5d2bf09dc75509d836cb962aa02f239e41ec46059c5126742a526bdae8b875e6

Криптовалутата Иридиум го користи претходниот концепт на Монеро и покажува повеќе трансакции од кои една е точна, таа не ги покажува примачите и испраќачите на трансакцијата. (најблиску до точен податок што можеме да добиеме е да претпоставивме дека износот на трансакцијата изнесува од негде 0.00000439 ИРД до 5.00000000 ИРД без да имаме пристап до праќачот на трансакцијата или пак примачот на трансакцијата). Како што може да видите оваа трансакција во моментот на пишување истата е во тек. т.е треба уште 15 пати да се потврди од други обработувачи за да истата добие статус како извршена. Трансакцијата е извршена во склопот на 767471, наградата е премала за да биде запишана со 4 децимални места и затоа истата стои како да не постои.

На различни системи имаме различни големи на самите клучеви, т.е секоја трансакција зафаќа различен простор за да се запише истата споредствено со секоја трансакција на некој друг систем. Како што видовме од горната трансакција на биткоин клучот изнесуваше 225 бајти, кај монерото истиот изнесува 0.10 килобајти или 100 бајти, кај иридиум истата изнесуваше 280 бајти. Кај различни системи и алгоритми имаме лимити на големината на делчињата/блоковите (block-size).

Биткоинот до 2010 имал блоковска големина од 32мб, сега има само од 1мб
Документчејн има блоковска големина од 2мб (поради помала големина на трансакцискиот клуч, делчињата/блоковите доспеваат побрзо од Лајткоинот иако имаат помала блоквоска големина)

Кардано има блоковска големина од 2мб, со транцаксиска големина од 8килобајти.

Лајткоинот има блоковска големина од 4мб. (затоа има 4пати побрзо блоковско време дека имаат горе долу иста големина на клучевите за трансакција)

Шугарчејн има блоковска големина од 4мб. (многу помала трансакциска големина има и затоа има брзо блоковско време од 5 секунди.)

ЦПУчејн има блоковска големина до 1000мб (сега за сега трансакциите се во мал обем и нема доволно јака компјутерска моќ која што ќе ја задоволи таа блоковска големина)

Чиа има блоковска големина од минимум на $k=32$ [околу 100гб во стално складиште или $x2$ во моментално скаладиште] (различен систем на обработка, брзината е голема бидејќи нема потреба од процесори, податоците се веќе запишани и не се бараат туку се вчитуваат од хардиските на системот)

Етериумот има модуларна големина на блоковите, т.е големината на блоковите се базира врз принципот на понуда и побарувачка. Единица мерка не е бајт, туку единица мерка наречена гас секоа единица мерка гас е еднаква на 1 гвеи (или 0.000000001 eth), горната граница за максимална количина на гас е варијабилна низ историјата на Етериумот, моментално истата изнесува 15 000 000 гвеи. При услови на зголемена побарувачка трошоците за трансвер се поголеми и самите блокови се поголеми поради ова, исто така и се зголемува тежината за разрешување на математичкиот проблем кој го издава трансакцискиот клуч (хеш). Големината исто така зависи од комплексноста на договорот, обично нормалните трансакции се околу 100-150 (за брзо извршување), 200 (при голема побарувачка на трансакции), доколу имаме паметен договор или издавање на РЦ-20 токени истата цена е 10 до 20 пати поголема поради комплексноста и поголемата компјутерска моќ да се изведе трансакцијата.

Оваа големина ограничува доста работи и е во директен сооднос со блоковското време, колку помала големина на делчињата толку помалку трансакции може да све вметната во едно делче (доколку не се промени граничната големина по трансакција).

Трансакциска големина(вклучува хешови и други метадата податоци) * број на трансакции = блоковска големина

Колку е поголема трансакциската големина толку е потешко, да се решаваат математичките проблеми особено кај алгоритмите што докажуваат работа (Proof of work). Исто така со вклучување на појаки компјутерски единици кои што ја докажуваат работата има тенденција да се истиснат послабите компјутерски единици кои што можат да одобруваат трансакции. (со овој проблем се соочува биткоин и ќе се соочува во иднина).

Со секоја трансакција расте параметар наречен тешкотија на решавање проблем (difficulty), оваа единица означува коефициент кој што ја покажува колкава е тежината за решавање на проблемот за да се добие еден трансакциски клуч (хеш).

Колку повеќе обработувачи/копачи толку поголема тешкотија на решавање на проблем.

Колку повеќе АСЦИ, ГПУ картици толку помала е можноста на решавање на проблемот од страна на процесори.
(има одредени алгоритми кои што ја отежнуваат работата на Графичките Картици и Апликационо Специфичните Кола (ASIC))

Зачувавањето на синџирот во некој валути се врши од страна на главни јазли (masternodes)

Ова е практика кај поновите системи за докажување на работа (proof of work) и кај системите кои работата на доказ на залог (proof of stake).

Главните јазли или Цели јазли служат како информациона база на јазолот, кои што се создаден со цел да не мора секој кој што ќе го симне или создаде новчаникот да мора да го симнува целиот синџир, или пак кај мајнерите да не мора да го имаат целиот синџир симнато (може да користат туѓ главен јазол за да проверуваат трансакции). Кај одредени синџири кои постојат подолго време и имаат голем број на трансакции и блоковската големина е голема истите имаат доста голем обем. Величини на различни синџири во момент на пишување

Биткоин има големина на синџир од 378.53 гига бајти.

Етериум има големина на синџир од 320 гига бајти.

Монеро има големина на синџир од 63.75 гига бајти.

Лајткоинот има големина на синџир од 57.72 гига бајти.

Карданото има големина на синџир од 18.72 гига бајти.

Големината на синџирот со секоја трансакција се зголемува, секоја трансакција или секоја промена на граничната големина трансакциската/блоковската големина влијае на големината на синџирот

Главните јазли кај системите со проверка на работа (proof of work) не се загарантирани со колатерал и обично, потребно е големо вниманија на избирање на главен јазол доколку иститот не се симне за да се одтргне од опасноста сопственикот на јазолот да манипулира со синџирот во сопствена корист. (со оваа проблематика се занимаваат информационите аналитичари).

За да нема манипулација на главните јазли особено кај системите со докажување на залог постои колатерал кој што изнесува прилично голема сума од количината во оптек околу 0.1 до 5% од токениите/валутата во опсег за да се создаде главен јазол (кој што е заклучен се додека оперира главниот јазол), постојат во одредени валути или јадници вакви главни јазли. Управувачите со главните јазли добиваат награда од страна на системот за наградување на копачите (добиваат дел од трансакционите трошоци) бидејќи придонесуваат во безбедноста на самиот систем. Потребен колатерал за основање на главен јазол.

Блек хет има колатерал од 5000 БЛКЦ (0.42% од валутата во оптег)

Заклучени се околу само 16% од целиот (кој што ќе биде во иднина) или моментален 52% оптег на валутата.

Документ чејн има колатерал од 5000 ДМС (0.42% од валутата во оптег)

Заклучени се околу само 8% од целиот(кој што ќе биде во иднина) оптег на валутата.

Деш има колатерал од 1000 ДЕШ (0.189% од валутата во оптег)

Заклучени се околу 17% од целиот (кој што ќе биде во иднина) или моментален 40% оптег во валутата.

Постојата околу триста па и повеќе криптовалути кои даваат награди за основање на главни јазли, бројот на главни јазли се зголемува дневно и моментално има околу 250 илјади главни јазли. Затворен капитал во тие главни јазли изнесува околу \$30 милијарди долари (со калукулран пад од 20% од пред неколу дена) или попрецизно во биткоини 620 илјади Биткоини.

Поделба на криптовалутите според технолошки фактори

Пред да преминеме на разрешавањето на проблемите кои електронските трансакции ги имаат и системите/алгоритмите на кои се докажуваат истите трансакции би сакал да посветиме внимание на начините на поставување на криптовалутите во оптег и воедно инфлационите фактори на криптовалутите.

Како што знаеме секоја валута има своја количина во оптег, истото е и со криптовалутите. Одредени криптовалути имаат ограничена количина во оптег, некој пак имаат неограничена количина во оптег, одредени имаат стабилна инфлациона стапка одредени немаат инфлациона стапка.

Поделбата според ограниченоста на количината во оптег е на:

- Ограничени
- Неограничени

Повеќето познати и ширеко применувани криптовалути имаат ограничена количина во оптег, истата може да биде решение на проблемите како вреднување на истата, може да претставува можност да се користат валутите како заштитници од инфлација (бидејќи истата има ограничен оптег за разлика од жиралните пари). Но истовремено да претставува проблем како големи трансакциски трошоци, иликвидност во времиња на зголемна побарувачка за трансакции, дефлација итн.

Поделба според поткрепеноста на криптовалутата е на:

- Поткрепа врз капитал (стабилни криптовалути)
- Поткрепа врз побарувачка (поткрепата е скоро и не постојана).
- Поткрепа врз услуга (криптовалутата т.е компанијата која што ја издава нуди одредена услуга која ја наплатува преку криптовалутата во оптег).

Стабилните криптовалути кои што ќе ги објасниме понатаму имаат резерви од жирални пари или еквиваленти на истите со кои ја потпираат својата криптовалута во оптег. Овие криптовалути се доста стабилни во совојата вредност и обично се засновани на доларот и имаат еквивалентна вредност на него. (мала нестабилност се јавува при зголемена или намелена побарувачка од нив, нивната вредност опаѓа или расте од 10-20% од вредноста на доларот).

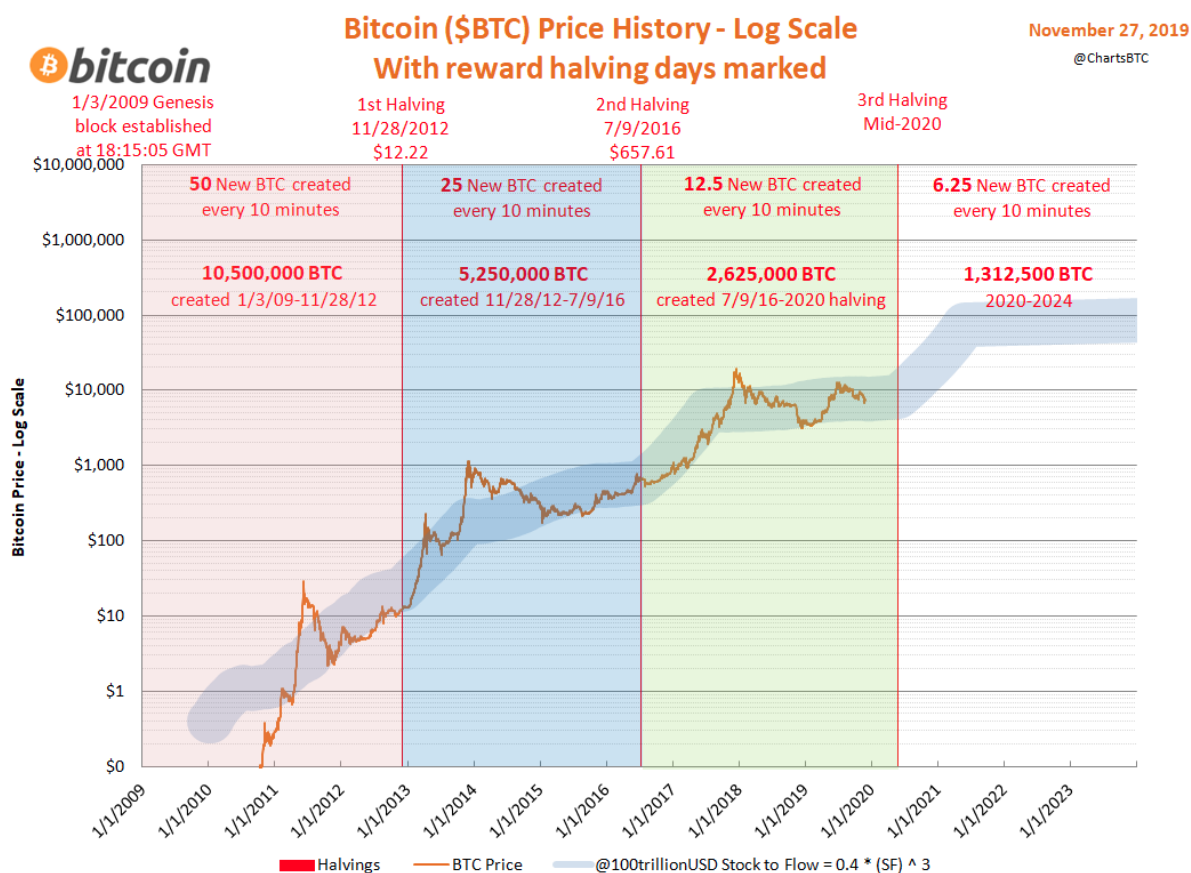
Поткрепата врз побарувачка се наоѓа во скоро сите криптовалути, нивната поткрепа се должи врз идната употреба на истата и технолошкиот напредок кој што го нуди криптовалутата.

Поткрепата врз услуга се обично криптовалути издадени од правни лица кои нудат услуги со наплата на истите услуги преку криптовалутата, но во оваа категорија се наоѓаат широко познатите криптовалути кои што се користат за размена на други криптовалути со нив. Како биткоин, етериум, бајненс коин, унисвап, пенкеик свап, поокоин, курв фанјенс и други.

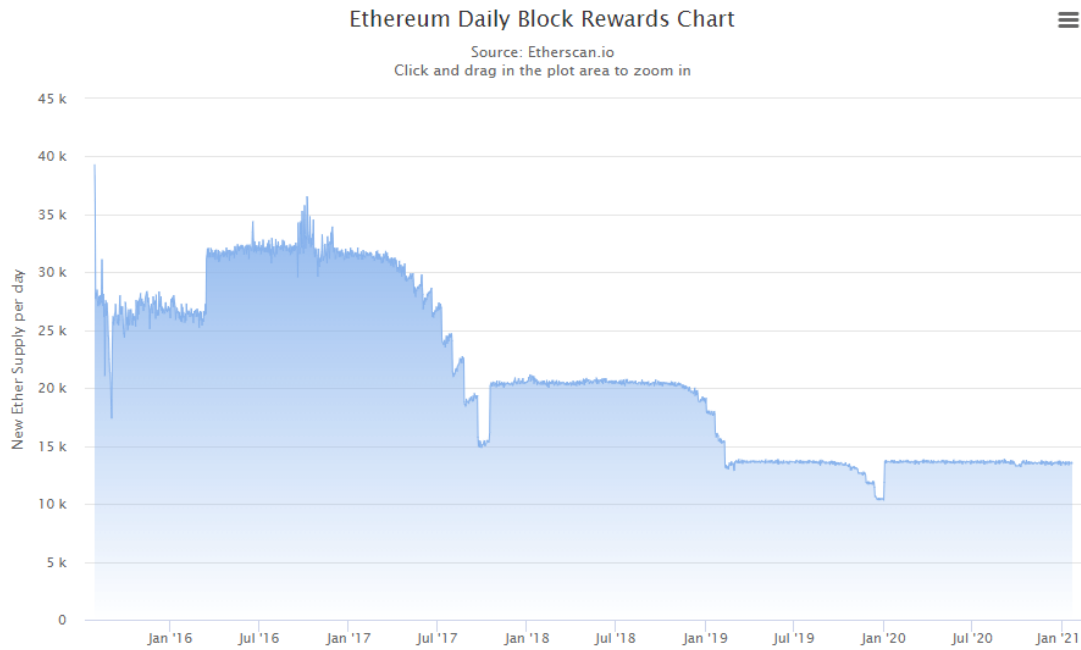
Поделбата според начинот на инфлационата стапка е на:

- Инфлациона стапка поврзана со време
- Инфлациона стапка сврзана со работата на операторите
- Непостоечка инфлациона стапка

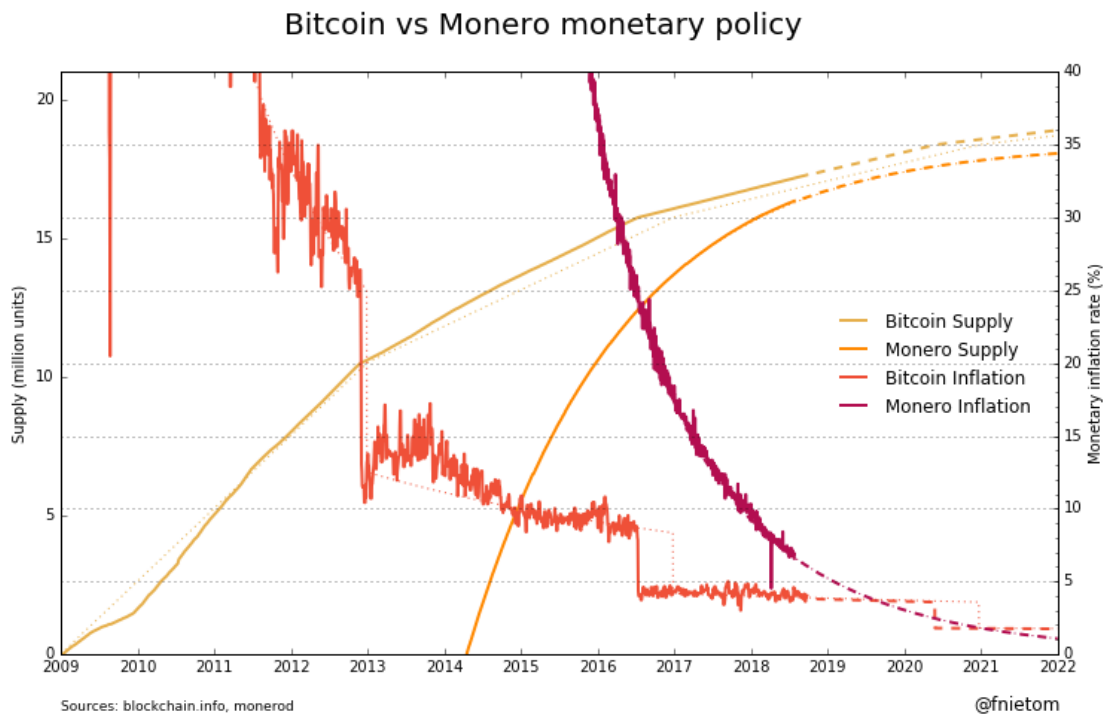
Мнозинството од криптовалутите користат инфлациона стапка поврзана со време, т.е. наградата која што ја добиваат операторите со текот на времето се намалува. Визуализацијата на овој концепт е најдобро објаснета преку графикот направен од твитер корисникот @ChartsBTC



Според податоците е покажана количината во секој четригодишен период колкава количина на биткоини биле создадени во тој период и пропорционално како се движела цената на биткоинот. Не секогаш со растење на количината во оптег расте цената. Моментално системот на биткоин издава награда за решение/создавање на блокот, а корисниците плаќаат за да добиат поповлна позиција на редицата за чекање на изведба на нивната трансакција. Доколку во иднина опстане системот на Биткоин последната награда која што ќе ја издаде истиот ќе биде во 2140 година, од таа дата нанатму инфлацијата ќе биде непостојана и за трансакциите да се извршат ќе треба да плаќаат самите побарувачи на трансакциите.



Од друга страна инфлационата стапка на Етериумот е базирана врз работата на обработувачите, поради ова е и неограничена количината на истиот. Колку поголема побарувачка има за трансакции на екосистемот на Етериум толку е помала инфлационата стапка (т.е колку поголеми се трансакциските трошоци врз корисниците толку помалку системот треба да издава етериуми во системот за да ја наполни количината на гас за да се изврши трансакцијата) Илустрирано горе на сликата.



Графикот создаден од корисникот @fnietom го објаснува хибридниот систем на Монеро заснован и врз временска рамка и врз работата на операторите. Биткоинот споредствено има инфлациона стапка со ирегуларности и на крајот стапката стигнува до нула. За разлика од тоа Монерото има експоненционален тек т.е се намлаува постепено и никогаш не достигнува нула. Со цел да нема конгестија при отсекување и ограничување на оптегот на валутата и зголемувањето на трансакционите трошоци, Монеро користи систем од така наречени опасни трошоци. т.е после Мај 2022 инфлацијата ќе биде фиксна од 0.6 ХМР по делче/блок (едено делче/блок се создава секој 2 минути) или фиксна годишна инфлација од 157680 ХМР. Која постепено на годишно ниво опаѓа но никогаш не стигнува до нула.

Неинфлаторните криптовалуди се обично затворени криптовалуди кои што директно се купуваат преку ПрвичнаЈавнаПродажба, Раздавања (Airdrops) или преку инвеститори и се достапни на секундарните пазари (менувачниците) да се откупат. Овие валуди се строго со ограничен капацитет, освен ако нема измениво натамошниот тек и издавачите/сопствениците на истите не направат моментална инфлација за да проадат поголема количина од истите.

Поделба според начинот на дистрибуција на криптовалутата
Органска дистрибуција (без ICO/ПрвичнаЈавнаПродажба,
инвеститор и претходно копање пред да се отвори синџирот за јавноста)
Полу-органска дистрибуција (со награди за тимот кој ја работел
на криптовалутата)

Неорганска дистрибуција (со ICO ,со претходно копање пред
отварање на синџирот во јавноста и со инвеститори)
Најретки од сите се валутите со Органска дистрибуција, најголем дел од нив се со полу-
органска дистрибуција (тимовите или имаат загаратиран удел или се користат одредени
средства за промоција на истата). Неорганската дистрибуција се јавува најчесто кај
приватните криптовалуди или оние кои што се управувани/создадени од правни лица.

Биткоинот, Етериумот, Документ чеинот се криптовалуди со полу-органска дистрибуција.

Цпу Чејн, Монеро, Иридиум и други се криптовалуди со органска дистрибуција.

Со неорганска дистрибуција се Курв Фајненс, Коинбејскоин, Бајненс коин, Унисвап, Пеинкејк
свап и други криптовалуди.

Проблеми со кои се сочуваат синцирите

Без централен ентитет, и централен систем за управување мора да постои начин на кој ќе се одвиваат трансакциите и воедно да се избегнат проблеми како двојно трошење и можноста да го превземе некој синцирот на трансакции и да прави промени.

Првиот проблем (проблемот на двојно трошење) се решава со проверка на целосниот синцир. Кај скоро сите протоколи овој проблем се решава на истиот начин, т.е за да се изврши трансакцијата операторот (копачот/одобрувачот) го проверува синцирот (без разлика дали е целиот синцир со користење на процесорска моќ, или пак заложува одреден број од своите токени за да се осигура трансакцијата или пак го прегледува одредениот дел од синцирот кој што истиот го има зачувано) и гледа дали има доволно средства за да се изврши трансакцијата, кога ќе може да се потврди трансакцијата и измене блоковското време (има доволно трансакции да се наполни едно делче/блок) истата се запишува во делче(блок). И истата може да се види како што погледнавме горе во сликите кога дискутиравме за трансакциски клучеви.

Вториот проблем се решава на ниво на протокол на обрботка на самиот синцир.

-Протоколот базиран врз докажување на работата (proof of work) е скоро невозможен да се манипулира бидејќи за да се контролира одреден синцир потребно е некој да има мнозинство (повеќе од 51 процентен удел) од целокупниот број на обработувачи/копачи во тој протокол за да може да го промени синцирот со цел да манипулира со состојбата на средствата на самите сметки/новчаници.

-Протоколот базиран врз докажување на залог (proof of stake) е исто така тежок за манипулација бидејќи за да се контролира истиот синцир потребно е некој да има повеќе од 80% од количината валути во оптек и истовремено да контролира 51% од сите главнијазли (masternode). Истото важи и за модифицираниот протокол на докажување на брзина на залог (proof of stake velocity).

-Протоколот базиран врз докажување на простор (proof of space and time/alocation) го избегнува овој проблем со тоа што е потребно некој да го поседува мнозинството од целиот трансакционен синцир и да го манипулира времето на креација на сите тие синцири за да може да го менува и истовремено да ги истисне другите кои имаат копии од истиот во правилен временски интервал.

-Протоколот базиран врз докажување на Активноста (proof of activity) го избегнува овој проблем со истите решенија на докажувањето на работата и залогот. Тој како комбинација од двата, кога ќе се ископа наградата таа не се слева кај операторот туку треба кај другите одобрувачи да се одоброи за да се изврши. Овој систем е малце поскап за одржување поради двојниот процес, но затоа е побезбеден. Бидејќи бара ем да се превземе мнозинството од компјутерската моќ ем мнозинството од валутата во оптек.

-Протоколот базиран врз докажување на горење (proof of burn) работи на сличен принцип како протоколот базиран врз докажување на залогот (proof of stake) само што место да се заклучуваат средствата со цел да се одобри една трансакција, тука се праќаат на трула адреса/новчаник и иститие се “уништуваат”. За самото уништување со добива награда и на тој начин се обезбедува безбедноста, уништувањето може да биде во форма на валутата која

што го применува овој протокол или некоја друга валута, важно е дека треба да се прати одредена сума.

-Принцип базиран врз докажување на поминато време (proof of elapsed time) ги сегрегира обработувачите и доделува задачи и награди за сработената работа на случаен начин. Т.е треба да помине случаен период од време за да добие одреден копач работа. Овој принцип можеме да го замислиме како принципот за докажување на работа само што нема натпревар меѓу обработувачите/копачите туку на секој му се доделува работа на одреден случајно одреден временски интервал. Овој концепт се користи како подконцепт во повеќе концепти како докажување на работа, залогот, место, итн.

Сите овие концепти имаат и позитивни и негативни страни, некои бараат поголеми ресурси, некои пак имаат голем инвестициски праг на учество од страна на обработувачите. Сепак сите овие концепти работат и се успешни во обработката и со помош на нив се автоматизираат и децентрализираат трансакциите.

Криптовалута

Откако осознавме основно како функционираат криптовалутите (т.е како функционираат нивните синџири од делчиња/blockchains) сега да ги спознаеме елементите и како тие влијаат врз динамиката на самата валута. Како воедно можеме да ги искористиме во вредносна анализа на една криптовалута.

Елементи на криптовалута се:

- Цена

Кога ќе погледнеме преглед на една криптовалута, прво нешто што гледаме е нејзината цена или вредност. Таа најчесто е изразена во Долари или пак во биткоици.

Прикажаната цена на страните кои што ги прикажуваат криптовалутите е просек од сите цени понудени на пазарите, многу важен фактор во тоа кога гледаме цена е да видиме валутатата за кои валути можеме да ја замениме. т.е дали идниот пад или пораст на цената ќе биде под влијание на пад на валутатата во која што се менува истата. Има и други елементи кои влијаат на цената.

- (Дилутирана) Пазарна капитализација

Пазарната капитализација ја има истата формула како и кај другите финансиски инструменти. Бројот на единици * пазарна цена = пазарна капитализација.

Дилутираната или разредената пазарна капитализација ја вклучува идната предвидена инфлација или ги исклучува изгорените/уништените единици.

- Волумен

Волуменот ни го покажува целовкупниот број на средства разменети за таа валута на познатите менувачници во времетраење од 24 часа. Истиот ни ја индицира ликвидноста на самата валута, исто така на краток рок доколку водиме евиденција можеме да предвидиме дали одредена валута ќе опаѓа и расте. Најчесто волуменот расте и се намалува циклично со пазарното расположение (мечкино или биковско) освен при ценовно влијателни вести.

Како коефициент за ликвидност се пресметува соодносот на волуменот спрема пазарната капитализација

- Договори

Под поимот договори се подразбира склучените договори/contracts кои ги има криптовалутата, или пак поедноставено. Договорите (паметни договори/smart contracts) претставуваат начини на кои што криптовалутата користи туѓи синџири како синџирите на Етериум, Бајненс, Трон или други валути. (и фактички е подсинџир во нивниот синџир) што помага во намалување на трошоците на краток рок за изнаоѓање на обработувачи и технолошко развојни трошоци, на долг рок со приврзаноста кон други валути може да направи големи трансакциони трошоци или пак да ја осуди на пропаст доколку пропадне системот на обработка на синџирот или пак замре побарувачката на истата криптовалута на која е направен паметниот договор. Доколку гледате големи аспирации во одреден проект и претпоставувате истиот да има голем волумен, присуството на паметни договори може да биде алармантен сигнал за потешкотии во иднина (процес на раскинување или реинтеграција во сопствен синџир)

- Пазари

Овој елемент иако не е поврзан директно со самата технологија на криптовалутата и нејзиното раководење е од исклучетелно, значење. Одлични примери за пазарното значење се доце коиноти и шибата коишто технолошки немаат значителна поткрепа, а истите одкако беа прифатени да бидат тргувани на Пазарниот Гигант Бајненс го зголемија својот волумен десеткратно и со тоа растеше и нивната цена, покрај нивната ограничена практичност. Колку повеќе пазарни места за размена толку подобро, исто така пазарниот волумен и реномето на пазарното место/менувачницата е важно. Политиките кои што ги води истото, односот со корисниците и други фактори кои ќе ги објасниме подоцна.

- Пазарна историја

Според пазарната историја и со согледување на ценовната разлика во минатото може да добиеме ориентациона слика за самата идна цена особено за однесувањето на поседувачите во однос на одредени ценовно-осетливи новости, исто така и цикличните тенденци на крипто пазарот, како истата се однесувала во биковски пазар (биткоин ориентиран пазар) или во мечкин пазар (алткоин ориентиран пазар).

- Поседувачи

Поседувачите и трансакциските аналитики многу добро нија покажуваат структурата, особено кај транспарентните криптовалуди. Со помош на информациониот приказ можеме да ги видиме адресите кои што поседуваат најголем удел (наречени и китови) од истата криптовалута, да видиме доколу истите прават одредени промени. Тие како големи “акционери” и тоа како можат да влијаат на цената и се во способност да направат ценовни шокови, во некои случаи и паника.

- Други Коефициенти

Постојат и други коефициенти како насоченоста на поседувачите (мечкино или биковско), пораст на обработувачи, процентен пораст на самиот главен синџир, концентрација (китовско однесување), обем на трансакции итн. Овие повеќе влијаат и се гледани од страна на техничките аналитичари кои своите продажни и куповни стратегии ги базираат врз пазарното однесување, јас не би го препорачал овој начин на тргување. Иако истите може да ни индицираат краткотрајни промени во сликата или пак да ни навестат за поповолен иден период за купување и продажба доколу имаме некоја слична намера.

Каде можат овие информации да се видат?

Овие информации обично се наоѓаат на крипто листоарите, како што се коинмаркеткап, коинпаприка, коингеко и други. Некој од менувачниците исто така нудат вакви податоци, или пак во одредени случаи истите мора мануелно да се собираат со анализа на интернет. Овие основни елементи ни ја покажуваат општата положба на криптовалутата и не се ни блиску до мерило за купопродажба. Овие се показатели за моменталната состојба и претходниот тек на истата, инвеститорите би ги интересирале идните постапки и иднината на самите криптовалуди затоа овие елементи не се од исклучителна важност во тој сегмент.

Како да се процени купопродежен потенцијал на една криптовалута?

Одговорот е сличен како со повеќето финансиски инструменти, со многу истражување, анализи. Колку подобро познавање имате за криптовалутата и технологијата позади неа толку подобро. Или да го цитирам Сун Цу.

“Ако го знаеш непријателот и себе си, ти нема да се плашиш од исходот од илјада битки. Ако се знаеш себе си а не го знаеш непријателот, тогаш за секоја добиена битка ќе поднесеш пораз. Ако не се знаеш себе си ниту пак непријателот тогаш секоја битка ќе заврши со пораз.”

Или метафорично ако го замислиме крипто пазарот како едно воено поле, ние доколку си ги знаеме нашите финансиски приходи и го знаеме непријателото или туѓото нешто (криптовалутата во која инвестираме) ќе можеме, да оствариме максимален финансиски приход (ќе победиме) над другите кои ќе сакаат истата да ја купат во погрешен момент.

Секако ова не значи дека треба да организираме измами од типот на пумпање и исфрлање, но во секој случај доколку ја осознаеме на подлабоко ниво криптовалутата од повеќе информациона извори, ќе знаеме да направиме правилна одлука барем во 50% од одлуките кои што ќе ги направиме.

Како се анализира криптовалута? И каков потенцијал може истата да има?

Како можеме да ја гледаме Криптовалутата како финансиски инструмент? Тоа е доста едноставно, се додека истата има некаква значајна примена во вистинскиот свет и пазарот има побарувачка да ја купи истата, истата има одреден потенцијал. Иако финансиските инструменти имаат регулативи и стандарди, сепак криптовалутите вонглавно се докажаа како сличен еквивалент како нив. Тие претставуваат амалгам од финансиско средство слично на хартиите од вредност кое што ни докажува одредена инвестираност во тој трансакциски начин и истовремено ние како акционери во тој проект можеме транспарентно да допринесеме кон истиот да прерасне во нешто поголемо, без проблеми на иликвидност како што се соочуваат стартап правните лица. При анализата на криптовалутите ќе гледаме слично како што би анализираше една компанија или еден проект и ќе ставиме акцент на:

- Технологијата која што ќе се капитализира
 - Концепт на извршување на синцирот
 - Состојба на обработувачи
 - Трансакциони трошоци и општествено влијание
- Пазарниот потенцијал и состојба
- Конкуренцијата
- Корисници/Консументи
- Менаџерски тим
- Акционерски склоп/Поседувачи
- Углед, Односи со Јавноста, Заедница

Технолошка анализа

Да дефинираме што претставува и опфаќа технологија, под технологија се подразбира целото функционирање на криптовалутата како истата работи или еквивалент за ова во бизнис секторот ни претставувал бизнис планот со балансите на успех, состојба, готовински тек итн.

Обично криптовалутите немаат вакви извештаи, туку истите податоци се распрчкани наоколу, како прво нешто што гледаме се научни/технолошки дела или на англиски наречени *whitpaper*. Во користена литература има цитирано неколку технолошки дела од криптовалутите кои што ги споменав кога давав пример кога ги објаснував карактеристиките на синцирите кои што може да ги погледнете. Тие се долги во просек од околу 10-30ина страни, некој од нив навлегуваат во математички калкулации и објаснувања на изворниот код, некој пак изгледаат во форма на бизнис брошури.

Сепак тие ни даваат првична слика за технолошкиот развој, понатака доколку имате познавање од информациона технологија и програмирање можете да погледнете во изворниот код, некој од криптовалутите користат елементи од различни криптовалути, некој пак се комплетни копии од одредени криптовалути само што менаџерската политика им е различна менаџерска политика. Како што се Биткоин Кеш и Етериум Кеш (кои се директни одцепувања /forks кои се создадени поради спорни теми како блоковска големина, трансакциска брзина, распределба на оптег на количина од криптовалутата итн.)

Овие две анализа зафаќаат голем временски период и може да потраат од неколку часа па се до стотици часови работа, исто така доколку немате познавање може да ги користите различните форуми на кои се дискутира за технологија и криптовалути и да увидите туѓи мислења за изворниот код или пак за менаџерската политика.

Со оваа постапка ќе ги видите предностите и слабостите на самата криптовалута и навистина ќе ги запознате границите и ќе можете да дадете свој став за менаџерската политика и како акционер/поседувач соодветно да влијаете кон промените.

Како друг елемент од технолошката анализа би претставувала анализата на структурата на обработувачи. Покрај тоа што е важна технологијата, сепак таа технологија не би можела да постои без обработувачите. Ова се гледа со анализа на така наречените базени за копање/одобрување и структурата на заеднички/одвоени главнијази,

Обработувачите (без разлика дали се копачи или одобрувачи) истите ни претстауваат трудот на самата криптовалута, со нивна структурна анализа ќе можеме да ја видиме нивната моќ која што ја имаат врз самиот синџир нивниот удел и на еден начин ако сме заинтересирани и ние да се “вработиме” во некоја криптовалута ќе процениме кон кој “синдикат” е подобро да се зачлениме или пак дали е подобро да останеме сами и да не учествуваме во тие базени на обработувачи.

Исто така со оваа анализа се гледа и моќта на самата мрежа, можеме да претпоставиме како може да се одрази зголемувањето на волуменот и недостатокот од компјутерска моќ врз трансакционите трошоци и блоковското време. Или пак да размислуваме кон намалување на трошоците со темпирање на трансакциите во периоди на мрежно успорување.

И како последни елементи од технолошката анализа ќе ги разгледаме општествените влијанија од технологијата и самото функционирање. Со зголемување на обемот одредени концепти како концептот на докажување на работа (proof of work) влијаат на глобалната потрошувачка на енергија, цените и побарувачката на процесорите на глобално ниво. Индиректно влијаат врз загадувањето, со што може технолошки да биде неодржливо во иднина или пак да биде одбивно за многу идни инвеститори, треба да се земат и овие фактори во предвид.

Пазарен потенцијал и состојба

Според елементите кои што ги погледнавме претходно, колку и да е совршен проектот технолошки без да може пазарно да се пласира и истот да капитализира од неговото јавно пазарно појавување истиот нема да опстане од повеќе причини, затоа и многу од проектите одаваат неколку проценти од нивниот оптег кон крипто менувачниците или истите ги продаваат па ги инвестираат во трошоци за лиситирање на менувачниците.

Како што споменав погоре, многу технолошки трули проекти како доџе коин и шибџа успеа да направат големи профити со помош на доста познати менувачници, како добар пример за ова е Squid Game криптовалутата која се појави на унисвеп и со листирањето на Коинмаркеткап и користењето на општествената приклонестот и фаворизација на истоимената серија успеа да направи ценовен шок. Т.е многу мал број на корисници успеаа да ја кренат цената на енорно високи суми и отпосле истата да ја столчат до самата земја. (од неверојатни 522 долари за единица Сквид гејм до 0.0025 долари за истата единица Сквид Гејм, која потсеќа и на завршетокот на приказната во истоимената серија).

Доколку се наоѓате во состојба на инвеститор со поголем удел може да влијаете на менаџерскиот тим за да ја смените насоката или да вложите делови од капиталот со цел да го подобрите пазарниот потенцијал со подобра пазарна поставеност во споредба со другите проекти.

На тема менувачници и пазари ќе посвети подоцна внимание.

Конкуренција

Конкуренција во буквална смисла представуваат сите други инвестициони можности (или сите други можности поврзани како опортунетен/можностен ризик), но во смисла на технологија и ако ја гледаме криптовалутата како една компанија/проект истата има потесен круг на конкуренти.

Чист пример ако погледнеме криптовалутата Бајненс Коин, истата е во категоријата на финансиски криптовалути истата за разлика од валутите на другите менувачници не издава дивиденда. Таа ја нуди услугата која што ја нуди Етериум само на подобар начин со помали трансакциони трошоци, т.е со помош на пазарната позиција како еден вид на монопол и менувачница со голем обем нуди услуга со користење на паметни договори преку кој ќе се тргува со други криптовалути истите да се продаваат со нивната криптовалута. На овој начин бајненс коин им откина од пазарниот удел на биткоин (преку кој се тргуваат вонглавно валути со сопствен синџир) или на етериум (преку кој се тргуваа коини зависини од паметни договори, но поради големите трансакциони трошоци многу од нив почнаа да мигрираат кон Бајненс и Трон).

Корисници / Конзументи

Со едноставна анализа на технологијата може да претпоставиме кои можат да бидат идните корисници на истата, т.е во иднина кога проектот ќе го достигне нашиот праг на потенцијал на истиот на кого ќе може да му го продадеме нашиот удел во него. Исто така на овој начин ќе можеме да ја претпоставиме највисоката цена која што може да ја постигне истата. Ова се истражува со истражување на социјалните медиуми, најразличните форуми на кој што се дискутира за криптовалутата која што ја гледаме и создаваме една стереотипна слика за просечниот конзумент на истата, со тоа го оценуваме нејзиниот потенцијал.

На пример, Подруго се вреднува одредена криптовалута наменета кон банкарскиот сектор која решава банкарски проблеми во однос со трансакции и трансакциски трошоци наспротив криптовалута наменета за препродажба на НФТ(незаменливи токени).

Менаџерски тим

Менаџерскиот тим најчесто се состои од самите програмери на криптовалутата, но во одредени случаи имаме извршни директори кои раководат со менаџерската политка на криптовалутата. Во одреден случаи особено кај DEX(децентрализираните менувачници) имаме демократско раководење нешто слично како во акционерските друштво со што поседувањето на токениот на менувачницата дава права за гласање (кое бара истата да се заклучи на одреден период).

Така да важно е да се установи менаџерската политика која што може да ја уништи или да ја воскресне криптовалутата и да се видат тактиките за алокацијата на средствата кој што ги поседува проектот и како ќе го воспостават билансот на бенефити кон сите засегнати страни. (козументи/муштерии, акционери/инвеститори, обработувачи/труд/вработени и општеството)

Акционерски склоп/Поседувачи

Во основните елементи увидовме дека од голема важност се поседувачите и анализата на истите и како китовите можат да влијаат на цената. Затоа е важно да се знае распределбата од каков вид е, (органиски, неорганиски, полуорганиски) и дали истата има значителни промени. Да се знаат интересите на сите поседувачи и нивните ставови за менаџерската политика и иднината која ја гледаат во проектот како целина и дали се тие исти со нашите.

Овој процес е малку тежок поготово кај валутите кои што имаат намалена транспарентност и зголемена безбедност, но сепак може да се постигне и во услови на потполна приватност како кај монето (каде што имаме фиксен менаџерски тим составен од развивачи кон кој тешко се стапува во контакт [но сепак не е невозможно] и може да се издејстуваат одредени промени во менаџерската политика, сепак не е возможно да се дознае структурата на поседувачи).

Углед, Односи со јавноста

Угледот подразбира јавното мислење за криптовалулата и проектот како целина, како општеството истиот го перцепира и го гледа. Ова влијае значително врз пазарната цена исто па дури и повеќе од ценовно влијателните новости. Пример за ова се доде коиноот и шибата кои ги искористија популарните смешни слики наречени мимиња и со користењето на социјалните мрежи помогнаа да проасне цената повеќекратно и истовремено да го привлече вниманието на милиони луѓе без разлика на нивниот технолошки напредок. Исто така Односите со јавноста имаат голема улога и реакциите на ценовно влијателните новости се важни, адаптацијата на општествените збиднувања и маркетинг стратегиите играат важна улога. Обично инвеститорите ја превземаат улогата на промотори и се лица на истата, но кај поцентрализираните проекти има депармент наменет за оваа цел. Затоа е важно да се истражи влијанието кое што криптовалулата го прави врз пазарото и пазарното мислење за истата.

Сортирање на криптовалути

Откако дознавме како се врши анализата и се мери потенцијалот на една криптовалута би сакал да ја направам распределбата на криптовалути и технолошките појави кои што произлегоа од криптовалути.

Поделбата на истите е огромна по категории (секој автор прави свои категории)

Според протокол се делат на:

- Докажување на точност
- Докажување на залог
- Докажување на простор/време

Според синџир се делат на:

- Сопствен синџир
- Етериум синџир (сите РЦ20 и други поддоговорни

валути)

- Бајненс синџир (сите нови мемикоини)
- Кардано синџир
- Трон синџир
- Солана синџир

Според намена се делат на:

- Општо разменски (Биткоин, Лајткоин)
- Договорни (Етериум, Бајненс, Кардано, Трон, Солана и др)
- Финансиски
 - Централизирани (Бајненс, Гравио и др.)
 - Децентрализирани (Курв, Пенкејк, Суши свап)
- Друга распределба по сектор
 - Транспорт
 - Веб 3.0
 - Видео
 - Канцеларски, комерцијални решенија
 - Метасвет (визуелизација и симулација)
 - Видеоигри
 - Обложување
 - Продажни
 - Податочни
 - Медиумски
 - Интернет на нешта
 - Недвижности
 - Маркетинг
 - Приватност
 - Стабилни коини
 - Енергија
 - Здравство
 - Децентрализирани Менувачници (Декс)
 - Незаменливи токени (НФТ)

Повеќето од овие категории по сектор самите по себе се објаснуваат, ќе навлезме во категориите кои што не се самообјасливи и се овозможени со користење на технологијата која што ја понудија криптовалути и нивната децентрализираност.

Децентрализираните Менувачници (DEX)

Децентрализираните менувачници работат на сличен принцип како што работат централизираните, само што сопствениците го делат профитот со понудителите на ликвидност во самата менувачница. Со помош на Децентрализираните менувачници се намалуваат трошоците, без да се намали профитот на понудителите на ликвидност. Принципот на понуда на ликвидност работи на тој начин што се нуди ликвидност од две валути во одреден базен и во однос тоа колку тој базен е понестабилан во едната валута (поради операциите и размената) толку е поголема процентната камата за вложените средства.

Ризикот да се намали цената постои во секој случај и обично Децентрализираните Менувачници работат врз основа на стабилни коини кои не им варира номиналната цена, а пазарната се менува поради дестабилизирање од страна на побарувачката и понудата. Овој проблем го решаваат со тоа што даваат поголем процентен принос на понудувачите на ликвидност кои што ги депонираат своите средства во децентрализираните менувачници. Обично нема период на кој што се заклучуваат средствата и каматата се пресметува на годишно ниво и се исплаќа на денот на исплаќање. Има и некој кои што ги заклучуваат средствата на одреден временски интервал.

Пионер во оваа услуга е Курв коин кој има понапреден алгоритам од Јунисвап со поефективно распоредување на каматите и пониски трошоци. 50% од профитите одат кон каматите кои ги наградуваат понудувачите на ликвидност во форма на токениот кој што го издава Курв. А 50% одат кај акционерите кои што ги заложиле претходно добиените Курв коинови за да гласаат во менаџерската политика на Менувачницата. Самата менувачница е раководена од акционерите и според гласовната одлука, дел од останатите средства ги распределуваат како стимул на одредени нови базени кои не се активни или пак ги распределуваат средствата како дивиденда измеѓу поседувачите на заклучени Курв коини. Одредени менувачници како Суши Свап немаат систем за гласање сеуште, а некој како Курв (кралот на стабилните коини), Унисвап (првиот познат Декс) и Пеинкејк свап (најголем број на коини се разменуваат на овој Декс) имаат пак систем за гласање и менаџерска политика.

Стабилни коини

Ги споменаваме на самиот почеток и делумно навлеговме во нив. Истите ја имаат функцијата за стабилизирање на добивки и да се избегне ризикот од девалвација при мечкино време. Најголем дел од нив ги издаваат финансиски институции или пак менувачници кои се користат истовремено за размена на коини на истите менувачници. Како исклучок е Тетер кој претставува правно лице кое има инвестирано 62.8 милијарди долари кои се распоредени пола во готовина и готовински еквиваленти, а половина се распоредени во хартии од вредност и други финансиски инструменти. Најчесто истите се користат како заменска единица и се последна врата за излез на добивка од крипто во жирални пари. Во одредени држави каде што тргувањето со криптовалута е дозволено истото се прави легално и се плаќа данок, според моето искуство во Државата постојат огласници преку кој се тргува со истите, се разменуваат под рака или пак во последниве неколку месеци се отвараат менувачници кои ги даваат парите на рака и средствата им се префрлаат на нив.

Незаменливи токени (НФТ)

Незаменливите токени се технолошки напредок кои со помош на криптографија се овозможува да се продаваат одредени интелектуални и уметнички дела и со помош на неа истите да се докажат дека се во сопственост на одредено лице. Обично овие коини функционираат на различни платформи со помош на паметни договори или пак имаме посебни валути наменети за истите. Овие токени имаат голема примена во светот на дигиталната уметност, видео игрите (продажба на скинови и одредени предмети[слично како во екосистемот на Стим]), дигитални патенти и слично. Како најголем напредок за популаризација во ова поле е интеграцијата на Твитер и можноста да се покажуваат и продаваат овие незаменливи токени.

Бирање на пазар на кој што ќе се тргува со криптовалути

Како последен елемент би го посветил тргувањето на Централизираните менувачни, такви постојат ијадници. Овие карактеристики ги нема кај децентрализираните поради немањето потреба да се прави акаунт на истите, само се поврзува новчаник и се прави трансакција. Критериуми кои би требале да ги запазите кога бирате централизирана менувачница на која ќе тргувате.

- Барање за идентификација (KYC) – повеќето големи менувачници бараат идентификација поради законите против прикривање даноци и перење пари. (ова може да предизвикува проблем доколку купувате криптовалути наменети за приватност со што си ги издавате идентитетот и коинот кој што ќе го префрлите на вашата адреса ќе биде асоциран со вашиот идентитет)

- Трансакциски трошоци за купопродажба – на различни менувачници различни валути имаат различни трансакциски трошоци познати како maker fees.

- Трансакциски трошоци за повлекување или депонирање средства – обично се само за повлекување средства и може да бидат поголеми од средствата потребни за трансфер од адреса на адреса.

- Лимити на количина со која може да се тргува – одредени менувачни забрануваат тргување со премали или преголеми суми на средства да се оградат од ризикот за пазарна манипулација.

- Реномето на менувачницата – доколку првпат тргувате на одредена менувачница депонирајте мала сума која нема да ви значи доколку истата ја изгубите поради измама, хакирање на менувачницата или други системски грешки. Исто така прочитајте за угледот на менувачницата дали има тенденција да прави серверски одржување во периоди на енормна пазарна активност, дали има индикации за претходно губење на средства на истата, дали претходно била хакирана, дали нивниот тим за поддршка е услужлив, дали лица од вашата држава имале проблеми со повлекување на средства во жирални пари (Оние кои што ја нудат таа услуга) и други проблеми.

Ви благодарам на вниманието, се надевам го зголемивте знаење за самите криптовалути.

Сите информации се од информативен карактер и се слободно достапни.

Електронски Пари - Криптовалути(т.е Делото кое го користи овој Договор.)
<https://github.com/a0ris0to0te0l/--->
Ристе Петров(сопственик) (C) 2021 Ристе Петров riste.084129@student.ugd.edu.mk

Ова Дело е слободно, вие можете да го разделувате, користите/извршувате и/или да го менувате под условите и одредбите на МНФ договорот за користење на слободни дела објавена на <https://github.com/kaladont/mnf>

Вие треба да сте добиле примерок на МНФ договорот за користење на слободни дела заедно со ова Дело, во спротивно, копија од договорот може да добиете на <https://github.com/kaladont/mnf> (официјална)

Со читање на овој текст вие ги прифаќате условите и одредбите на овој договор и сте должни да ги почитувате условите и одредбите на договорот. Вашите права но и правата на Авторот се Апсулативни и под никакви услови не се променливи. Доколку ги прекршите условие и одредбите на договорот вашите права како Корисник се одземаат.

Оваа програма/Дело се разделува со надеж дека ќе биде корисна, но БЕЗ БИЛО КАКВА ГАРАНЦИЈА, подеднакво ни без толкувана гаранција на КОМЕРЦИЈАЛНА ВРЕДНОСТ И ПРИКЛАДНОСТ ЗА ОДРЕДЕНА УПОТРЕБА.

Видете го МНФ договорот за користење на слободни дела за повеќе детали.

За да ја видите автентичноста на овој документ погледнете на <https://github.com/a0ris0to0te0l/--->, во него ќе се наоѓа хешотот кој што ќе биде истовремено поставен како начин на кој што ќе може да направите ревизија на пдф верзијата од овој документ, на криптовалути Документчеин направен за истата намена.

Користени извори

1. Основи на Финансии - Проф д-р Марија Гогова Самоникова. ISBN 978-608-244-746-9
2. Дигитални пари - https://en.wikipedia.org/wiki/Digital_currency
3. Критповалути - <https://en.wikipedia.org/wiki/Cryptocurrency>
4. Синџир од делчиња - <https://en.wikipedia.org/wiki/Blockchain>
5. Кардано блок тајм - https://www.reddit.com/r/cardano/comments/80wltj/block_time/
6. Чиа - <https://manuals.plus/chia/chia-network-consensus-explained>
7. Иридиум - <https://www.ird.cash/>
8. Иридиум Технолошки Проспект - <https://www.ird.cash/wp-content/uploads/2018/06/Iridium-Coin-Whitepaper-v3.pdf>
9. Биткоин - <https://bitcoin.org/bitcoin.pdf>
10. Masternodes online - <https://masternodes.online/>
11. CoinMarketCap - <https://coinmarketcap.com/>
12. Етериум - <https://ethereum.org/en/whitepaper/>
13. Солана - <https://solana.com/solana-whitepaper.pdf>
14. Кардано - <https://docs.cardano.org/introduction/>
15. УСДЦ - <https://f.hubspotusercontent30.net/hubfs/9304636/PDF/centre-whitepaper.pdf>
16. Унисвап - <https://uniswap.org/blog/uni>
17. Тетер - <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>
18. Монеро - <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>
19. Деш - <https://docs.dash.org/en/stable/>
20. Документчеин - <https://documentchain.org/files/documentchain-whitepaper-en.pdf>
21. Proof of Work - <https://www.investopedia.com/terms/p/proof-work.asp>
22. Proof of Stake - <https://www.investopedia.com/terms/p/proof-stake-pos.asp>
23. Proof of Stake Velocity - [https://wiki.reddcoin.com/Proof_of_Stake_Velocity_\(PoSV\)](https://wiki.reddcoin.com/Proof_of_Stake_Velocity_(PoSV))
24. Proof of Space and Time - <https://xchscan.com/kb/how-does-proof-of-space-time-work/>
<https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp>
25. Proof of Activity - <https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp>
26. Proof of Burn - <https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp>
27. Proof of Time - <https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp>
28. Squid Game - <https://coinmarketcap.com/currencies/squid-game/>
29. Тетер - <https://www.theverge.com/22620464/tether-backing-cryptocurrency-stablecoin>
30. Твитер и НФТ - <https://phemex.com/academy/what-are-twitter-nfts>
31. Curve - <https://resources.curve.fi/>
32. Uniswap - <https://uniswap.org/blog/uni>
33. Sushiswap - <https://sushi.com/>
34. Pancake swap - <https://pancakeswap.finance/swap>