Домашно 2 по Блокчейн – Burstcoin – Proof of capacity (PoC) – блокчейн консултантски анализ

*Техническите подробности и доказателствата за числата, посочени тук, идват скоро в бъдещи публикации, но това е преглед на предимствата на Proof of Capacity като алгоритъм за копаене.*

*В съзнанието на много хора, занимаващи се с криптовалута, има два алгоритъма за копаене: доказателство за работа и доказателство за залог. Удивително обаче и за щастие за мен и всеки друг, който открива Burst при сегашната му абсурдно ниска пазарна капитализация, повечето хора не са чували или не са обмисляли сериозно друг основен алгоритъм, който има по-голям потенциал от който и да е от другите два, Proof of Capacity.*

*Първата реакция на много хора е, ако търсите нов алгоритъм, тогава защо не изберете вариант на Proof of Stake? Изглежда като очевиден избор, вие напълно елиминирате гладното за енергия оборудване за копаене от уравнението. Въпреки това, Proof of Stake има няколко ключови проблема с него. И тези, които осъзнават тези проблеми, приемат, че доказателството за работа е единственият алгоритъм с потенциал.*

*Първо, позволете ми бързо да обясня как работят различните доказателства. Всички блокчейн алгоритми работят чрез свързване на блокове, които съдържат всички транзакции, извършени през определен период от време. На копачите се плаща, защото тези блокове съдържат такси за транзакции, както и първоначални транзакции. Всички транзакции се извършват по подобен начин във всички тези мрежи, но проблемът е начинът, по който тези блокове са свързани заедно.*

*В мрежа с доказателство за работа всеки хешира последния блок плюс произволно число, което е създал, докато намери валиден хеш, който отговаря на определени критерии. Тези хешове доказват, че е била изразходвана много работа за създаването на блока и следователно майнерът, който го е създал, трябва да е похарчил много пари за оборудването си за копаене.*

В мрежата Proof of Stake оборудването за копаене не е важно. Копаещите добиват приблизително частта от блокове, която съответства на процента от монетите, които контролират.

*С доказателство за капацитет частта от блокове, които миньорът получава за копаене, съответства на количеството пространство на твърдия диск, което копачът е отделил за копаене за мрежата. На пръв поглед изглежда приблизително същото като Proof of Work, използвайки твърди дискове вместо оборудване за копаене.*

*Отново ще навляза в повече подробности и ще докажа тези числа в бъдещи публикации, но има изчисления, които да ги подкрепят. Това е само бърз преглед.*

*Доказателството за капацитет има няколко предимства пред доказателството за работа и доказателството за залог.*

*Енергийна ефективност*

*Най-голямата причина Proof of Capacity да побеждава Proof of Work е, че Proof of Capacity е много енергийно ефективен, като използва приблизително 30 пъти по-малко енергия за изразходван долар, отколкото за миньор Proof of Work. Това е справедливо сравнение, тъй като миньорите ще похарчат определена сума пари, за да постигнат определена възвръщаемост на инвестициите при подобна мрежа, която има подобни транзакции и блокови награди.*

*Лесно копаене за обикновените хора*

*Копаене за монета Proof of Work изисква ASIC за копаене. ASIC са скъпи, шумни, консумират енергия и в някои случаи изискват допълнителни системи за охлаждане. Това не е нещо, което обикновен човек ще купи, но всеки вече има твърд диск.*

*Да бъдеш ASIC Proof означава, че всеки ден хората могат да копаят за мрежата и да бъдат също толкова ефективни, колкото хората, които купуват луксозно, скъпо оборудване, опитвайки се да спечелят предимство един пред друг... защото тези хора също ще купуват твърди дискове и всякаква технология, която позволява лесно копаене също ще предложи предимство на фирми и хора, които се нуждаят от евтини технологии за съхранение и повечето хора също трябва да притежават такова оборудване, ако редовно архивират компютъра си, както е силно препоръчително.*

*Ако погледнете Litecoin, когато беше устойчив на ASIC, макар че не и ASIC Proof, както изглежда Proof of Capacity, ще видите, че имаше огромен наплив от хора, които купуват допълнителни графични карти за копаене за Litecoin. Коефициентите са, че Burst ще създаде подобни вълнения и ще доведе до хората да купуват допълнителни твърди дискове. В момента вашият среден миньор копае с 12,5 TB, ако анализирате копачите за Burst.ninja. Което изглежда вероятно ще остане стабилно, тъй като нови копачи се присъединяват към осигуряването на монетата.*

*Енергийна ефективност*

*Proof of Stake наистина използва малко по-малко енергия, но Proof of Capacity използва само приблизително 25% повече енергия като Proof of Stake за мрежа с подобен размер поради ниското потребление на енергия от твърдите дискове в сравнение със свързания компютър, който трябва да се използва за копаете в еднакво голяма и децентрализирана мрежа за доказателство за дял.*

*Подрязване на блокчейн*

*Proof of Stake има някои сериозни проблеми, когато става въпрос за съкращаване на своя блокчейн. В среда на доказателство за работа или доказателство за капацитет можете да вземете тези доказателства и да ги използвате, за да докажете, че дадена верига от заглавки на блокчейн е валидна. В Proof of Stake тези блокчейн хедъри се правят с помощта на Proofs, които разчитат на блокчейна, който трябва да бъде създаден. Ethereum предложи решение за подрязване на блокчейн, но то е рисковано и погрешно, тъй като разчита на това, че най-малко 66% от миньорите остават онлайн през цялото време. В по-късна публикация в блога ще покажа защо това е недостатъчно и няма да работи.*

*Доказателството за залог не може да бъде толкова безнадеждно*

*В система за доказателство за работа или доказателство за капацитет можете да намерите блокчейн, който е имал повече работа, отколкото останалите, използвани за създаването му. И можете да покажете, че тези копачи са се съгласили коя верига е правилната. В монета Proof of Stake няма начин да докажете, че копаете по правилната верига по недоверен начин.*

*Единственият план, който съм чувал досега и който може да помогне, е корпорации като Walmart и McDonalds по същество да „гласуват“ коя верига е правилната и след това да разчитат на мнозинството, за да спечелят. Това е така нареченото „икономическо клъстериране“, което Nxt обсъжда. Така че по същество се доверяваме на корпорациите да осигурят блокчейна... което изглежда противоречи на целите на повечето хора, интересуващи се от криптовалута. И тъй като този вид споразумение е податливо на проблема с византийските генерали, това означава, че трябва да вярваме, че над 2/3 от страните по споразумението са честни. С тези гласове, това оставя веригата както с 51% атака върху блокчейна, така и с 33% атака върху броя на гласовете. Този метод е много по-сложен както за разработчиците за писане, така и за клиентите за използване и по-труден за доказване на правилността.*

*Другият начин за постигане на известно безнадеждност, което помага на този проблем с определянето на правилния генезис блок, е да се добави Proof of Work към уравнението, подобно на това, което прави Peercoin, където Proof of Work първоначално се използва за създаване на монети, но след това се намалява и заменен с Proof of Stake. Но в този случай това безнадеждност относно това кой генезис блок е правилен е толкова силно, колкото и компонентът Proof of Work, оставяйки монетата широко отворена за 51% атака срещу компонента Proof of Work чрез създаване на фалшиви вериги и с компонента Proof of Stake не осигурява допълнителна защита срещу този тип атака.*

*Доказателството за залог разчита на ключовете на миньора да останат в тайна*

*Два проблема с потенциално компрометирани ключове на миньора:*

*1) За да копае, миньорът трябва да съхранява личния си ключ на компютър за копаене за мрежата, свързана с интернет. Това директно противоречи на идеята за най-добра практика за сигурност за криптовалута като цяло, където притежателите трябва да държат ключовете си офлайн и на сигурно място.*

*2) Възможни са атаки с исторически ключ, когато миньорите продават частните си ключове дълго след като са изпразнили акаунтите си и ключът иначе е безполезен. Поддръжниците на Proof of Stake твърдят, че това не е проблем поради децентрализираните контролни точки, които не позволяват блокчейнът да бъде върнат назад достатъчно, за да се случи това. Векторът на атаката, който това пропуска, е, че такава атака може да се случи с помощта на разклонения на блокове в продължение на една година, което завършва с милиони фалшиви разклонения, изградени от различни блокове, и как може нов копач, който току-що се присъединява към мрежата за първи път, да знае по недоверчив начин коя вилица е правилната?*

*Други предимства на доказателство за капацитет*

*Доказателството за капацитет е по-децентрализирано*

*Ползата от възможността обикновените хора да копаят изгодно е, че мощността за копаене е по-децентрализирана, като се има предвид, че за обикновените хора е изгодно да копаят. Добивът вече не е концентриран в ръцете на миньори, които са похарчили милиони за специализирано минно оборудване. Може да се случи, че гигантските центрове за данни ще започнат да използват допълнителното си свободно пространство за копаене, но въпреки това, докато обикновените клиенти все още могат да бъдат печеливши от копаене, това няма да им попречи да копаят. Освен това тези гигантски центрове за данни ще печелят приблизително същата възвръщаемост на инвестициите като клиентите. Нека си признаем, в система с доказателство за работа, ако започнете да използвате дори своя графичен процесор за копаене, но ASIC са 1000 пъти по-ефективни от гледна точка на разходите, средният ви потребител дори няма да опита да копае. Тъй като те никога няма да спечелят блок и едва ще помогнат за защитата на мрежата или ще направят пари за това, така че какъв е смисълът?*

*По-лесен метод за привличане на нови клиенти в сравнение с други алгоритми*

*Като съпротива срещу ASIC и като се има предвид, че всеки ден хората ще са по-склонни да копаят, означава, че те могат лесно да бъдат запознати с монетата. Винаги ще има „безплатен“ начин за хората да печелят Burst, просто като копаят за мрежата. Това е чудесен начин да накарате нови клиенти да се присъединят към мрежата. След като накарате клиентите да държат малки количества от монетата, те чувстват известна лоялност и е по-вероятно да станат дългосрочни потребители, както сами купуват повече от монетата, така и насърчавайки другите да използват монетата.*

*Енергоемката част от копаене е извършването на изчисленията, но с монета Proof of Capacity като Burst, компютърът извършва изчисленията веднъж, след което всичко, което прави по време на копаене, е да чете няколко мегабайта от твърд диск на всеки няколко минути и проверява всеки път, когато се измъкне, вместо да работи чрез тежки изчисления.*

*Някои твърдят, че миньорите просто ще купуват повече оборудване, за да стигнат до точката, в която сумата Burst, която печелят, е равна на сумата, която харчат за електричество, така че те все още харчат същата сума за електричество. Този аргумент обаче не взема предвид първоначалната цена на оборудването за копаене, която трябва да се амортизира през целия живот на оборудването. Колкото по-енергийно ефективно е оборудването спрямо цената му, толкова по-енергийно ефективна е цялостната система.*

*Имайте предвид, че дори тези ASIC, които са оценени като най-енергийно ефективни (въпреки че не са толкова ефективни, колкото твърд диск), обикновено изискват охладителни системи, които не са включени в техните оценки за енергийна ефективност.*

*Най-важното обаче е, че като се има предвид, че Burst coin е доказателство за ASIC, това означава, че ще имате много повече хора, които ще копаят от компютрите си през времето, когато компютрите им така или иначе са включени и тези копачи ще бъдат печеливши и имат по-малък риск от влагайки парите си в минно оборудване, което не може да бъде препродадено. Това по същество е безплатна енергия, що се отнася до Burst, тъй като тези копачи биха използвали същото количество енергия, независимо дали копаят или не.*

*Бърз анализ на енергийната ефективност на Proof of Capacity срещу Proof of Work, нека сравним две „копаещи машини“. Имайте предвид, че това, което поддържа мрежата сигурна, е колко пари са отишли за закупуване на оборудване за копаене.*

*Машина за копаене на биткойни*

*SP35 Yukon Power [1]*

*Цена: $2,235*

*Консумирана мощност: 3650 W*

*Консумация на енергия за изразходван долар: 1,63 W/$*

*Разрушена машина за копаене*

*Твърд диск Seagate Barracuda 7200.14 [2]*

*Цена: $101,99*

*Средна консумация на енергия: 5,50 W*

*Консумация на енергия за изразходван долар: 0,05 W/$*

*Вашият среден майнер вероятно ще използва това устройство на доста средно ниво на мощност, което означава:*

*1,63 W$0,05 W$= 32,6*

*Това означава, че биткойн копачите използват приблизително 33 пъти повече енергия, отколкото копаене на допълнителен твърд диск за Burst.*

1.Сигурност -оценка X /1-10/