zelcash

innovative | intuitive | intelligent

white paper version two

Таблица със съдържание

Представяне

Блокчейн технологията ще промени света по начини, които не бихме могли да си представим преди пет години. MarketsandMarkets прогнозират годишен ръст от най-малко 61,5% през 2021 г., а докладът на Световния икономически форум прогнозира, че до 2027 г. 10% от световния БВП ще се съхранява на технология, отнасяща се до блокчейна. [1], [2]

Прозрачността, неотменимостта и премахването на нуждата от трети страни в блокчейна, намалявайки таксите, повишават сигурността и премахват риска за отсрещната страна. Той предлага опростеност: Операциите се добавят към една публична счетоводна книга, избягвайки объркване, хаос и главоболия, обикновено свързани с наличието на множество счетоводни книги.

Може би най-важното е, че блокчейна дава право на хората, като им осигурява повече контрол над техните транзакции и взаимодействие с информация и финансови сделки (да не говорим за техните собствени данни).

Ясно е, че блокчейна предлага огромен потенциал за промяна на неприкосновеността на личния живот и сигурността - и в идеалния случай - за преобразуване на глобалната икономика.

Но само в идеалния случай, на този етап. Липсата на достъпност и използваемост забавя възприемането. Проблемът със скалируемостта е основен. Другите предизвикателства включват атаки насочени към отказ от достъп до услугата (DDoS), срив на борси, липса на изходи във фиатни пари и особено за обикновения потребител – загадъчната система от hex (шестнайсетични) адресите. Резултатът: гъсто населени екосистеми, уязвимости в сигурността и високи - понякога непреодолими - бариери пред навлизането.

Както е посочено в този документ, планираме да разгледаме - дори да решим - тези въпроси.

Нашата платформа осигурява интуитивно, безпроблемно преживяване, улесняващо транзакциите между блокчейните в прост и изчистен интерфейс както за потребителите, така и за разработчиците. Със Zel ние създадохме една всеобхватна и стандартизирана среда, която позволява на разработчиците да съсредоточат усилията си върху решения, разположени на блокчейна. Това ще спомогне за свободното създаване на децентрализирани приложения (Dapps) и интелигентни договори, които са отворени за всички.

Изразената визия и решенията, описани в тази Бяла книга, представляват първите стъпки към разрушаването на бариерите, задвижването на глобалното възприемане на блочейна и извършването на разкъсващата трансформация.

[1] "Blockchain Technology Market-Global Forecast to 2021" MarketsandMarkets research *Blockchain Daily News*
[2] Deep Shift Technology Tipping Points and Societal Impact --World Economic Forum www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Мисия, визия и цели

Екипът на Zelcash е основан от хора, които мислят, че технологията може да направи велики неща за развитието на човечеството. Вярваме във визията за децентрализиран свят, за подобряване на състоянието на всички. Като екип сме си поставили за цел да станем лидери в развитието на фронт-енд блокчейна и развитието на неприкосновеността на личния живот. Нашата общност е това, което ще движи напред проекта, с вдъхновението от други в пространството. Нашата цел е да бъдем лидери в бранша и да позволим на технологията да стимулира проекта заедно с участието на общността. Zelcash има за цел да създаде необходимите инструменти за разработчиците, за да разширят впечатляващата сила на блокчейн технологията, водена от нашия силен екип и общността, за предоставяне на достъп до мощна технология, достъпна за всички.

Крайната цел, към която се стреми Zel е да бъде напълно децентрализирана и скалируема световна мрежа от компютърно-изчислителни мощности, мрежа, която позволява на разработчиците да използват безпрецедентната сила на интернет, за да осигурят лесен за използване пренос на стойност към хората, които не са обвързани с банките, тези които бяха забравени от традиционните парични институции и да разшири своята дейност чрез на пръв поглед безкрайния потенциал на блокчейн технологията.

Преглед

Целта на тази статия е да предостави подробна информация за технологиите и функциите на Zel, които са излезли на пазара или предстои да бъдат представени. Искаме този документ да бъде ясен и достъпен за всички, като в същото време гарантира, че са обсъдени ключовите технологии. Статията няма да представи задълбочени технически подробности за все още непредставените продукти, докато Zel Technologies не ги представи или е близко до представянето им в публичното пространство. Това ще гарантира, че разработеното от Zel Technologies не е копирано преди представянето.

Въпреки че някои от продуктите и услугите на Zel (като ZelTreZ) са с затворен код, кода им ще бъде инспектиран от независима трета страна. Екипът на Zel твърдо вярва в отворения код; където можем, ще гарантираме, че нашият софтуер и технологиите се разпространяват с отворен код, ведно с техническите характеристики.

И накрая, този документ не е предназначен като техническа справка или проспект, а като средство за демонстриране на това, което сме постигнали досега и за да дискутираме нашата визия и планове, докато работим по реализирането на истинския потенциал на Zel. В този дух, моля, обърнете внимание на следния отказ от поемане на отговорност:

Отказа от поемане на отговорност: Предстоящи изявления

Информацията в тази бележка е чисто описателна и не е задължителна. Моля, обърнете внимание, че тази статия съдържа прогнози, изявления за намерение, обсъждане на планове, оценки или друга информация, която може да се счита за поглед към бъдещето. Доколкото тези изявления представляват нашата преценка и очакване за това, което е за в бъдеще, това не е предложение или подкана за закупуване на продукт, стока, услуга или сигурност. Всички изявления са предмет на рискове и несигурности, които биха могли да накарат действителните резултати от развитието на ZelCash да се различават съществено. Никаква информация в този документ не е прегледана или одобрена от регулаторен орган.

Освен това възнамеряваме да използваме блокчейна на Zel като платформа за разработки с отворен код, допринасяйки към технологиите, за които е издаден лиценз, за напредъка на обществото, като не се фокусираме единствено върху печалбата на всеки, който е свързан с проекта. Ето защо не приемайте за чиста монета изложеното, особено във финансово отношение, върху тези бъдещи твърдения, които са предмет на промени.

Тази Бяла книга и нейните предходни и бъдещи издания са и ще бъдат достъпни на zel.cash/whitepaper. Забележка: Тази статия ще се актуализира често, понякога без предупреждение. Моля, потвърдете, че версията, която четете е текущата.

1.0. Bitcoin

Месец януари, 2009г. беляза излизането на бял свят на Bitcoin на Сатоши Накамото. Като първата валута без централизирана подкрепа или емитент, която не е физически подплатена, тя представлява радикална революция в начина на функциониране на финансовите системи. Може би много по-важна от обикновената транзакция на стойност е самата технология, на която се основава.

Блокчейнът, разработен също от Накамото, позволи използването на разпределен и децентрализиран консенсус. Чрез премахването на централизиран емитент или контролиращ орган, "дигиталните пари" биха позволили да се сключат сделки между партньори, без консенсус или потвърждение от доверена трета страна.

Bitcoin не бе първата електронна парична единица; B-money на Dei, както и други са съществували преди Bitcoin. Техният проблем беше постигането на консенсус. Трябваше да има механизъм, който да противодейства на един участник с нечисти помисли, опитващ се да извърши „двойно харчене” в мрежата. Чрез използването на доказателство за извършена работа, проверяващо блоковете в блокчейна на Bitcoin - по подобен начин на Hashcash на Adam Back - може да се постигне консенсус между свръзките, което позволява потвърждаване на транзакциите.

Оттогава блокчейнът се развива. Разработването на различни проекти - най-вече "Ethereum" - показа нови възможности и използване на блокчейна, разширявайки своя потенциал.

1.5 Zcash

Zerocash (2014 г.), който по-късно стана проекта Zcash (2016), използваше zk-SNARKs (Zero-knowledge Succinct Non-interactive ARguments of Knowledge), за да доведат до напълно анонимни транзакции между потребителите. Изграден върху Bitcoin, Zcash е доразработен на база Zerocash, с корекции в сигурността и настройки, както и подобрена функционалност и производителност. По същия начин, по който Bitcoin стана първата широко възприета електронна валута, Zcash стана първата широко възприета анонимна електронна валута.

Също така, Zcash започна борбата срещу централизацията на миньорството, породено от асиците под алгоритъм SHA-256, които бяха ударили по мрежата на Bitcoin; това (може би) позволи на мрежата да стане централизирана. Въвеждането на алгоритъма Equihash, алгоритъм, засягащ основно големината на паметта на

графичните чипове, явяващ се докзателство за извършена работа в областта на миньорството, доведе до връщане обратно към децентрализирания добив с процесори и графични карти. Макар, че наскоро беше разработен асик под алгоритъм Equihash 200,9 на Zcash, някои проекти поддържат миньорството отново децентрализирано, чрез консенсус, произхождащ от разработването на модифициран Equihash алогоритъм и програмируем алгоритъм (ProgPOW) като доказателство за извършена работа, както и чрез нови концепции като например доказателство за успешно извършена работа.

zk-SNARKs позволяват извършването на операция - например транзакция, излъчена в блокчейн мрежа, а произходът на транзакцията, сумата и получателя на транзакцията - да бъдат напълно прикрити от обществото.

Постоянното развитие на Zcash, като скорошното подобрение „Overwinter” в мрежата и работата по Z-транзакциите в мобилния (олекотен) портфейл, води до подобрения, които осигуряват анонимност в търговията по подобен начин на фиатните пари, но с удобството на цифровата валута и с разликата, че не е емитирана или контролирана от централен орган.

3.0 Zel

Ethereum също разшири възможностите на децентрализираните приложения и използването на блокчейна, позволявайки на разработчиците достъп до отворена платформа за разработване на приложения, интелигентни договори и много други.

От Бялага книга на Ethereum:

> *Това, което Ethereum възнамерява да предостави е блокчейн с вграден пълноправен програмен език на Turing, който може да се използва за създаване на "договори", които биха могли да бъдат използвани за кодиране на произволни функции за промяна на състоянието, което позволява на потребителите да създават някоя от описаните по-горе системи , както и много други, които все още не сме си представяли, просто като напишем логически свързано няколко реда код.*

С тази си визия Ethereum е бил движеща сила в много аспекти на развитието на блокчейна и индустрията на криптовалутите. Тя носи потенциала за свят, в който повечето - ако не и всички системи - могат да се възползват от технологията на блокчейна и характеристиките, произтичащи от нея. Независимо дали става въпрос за монетизиране на активи или възможност за използване на средства от фондове за първично предлагане на монети, тя е дала възможност на потребителите да създадат нов интернет, който не бихме могли да си представим преди няколко години.

Независимо от това, проблемите с скалируемостта - и опасенията за това как Ethereum ще се справи с тях - продължават. Ограничени до около 15-20 транзакции в секунда, просто е твърде бавно тази визия да се превърне в реалност.

Както ще очертаем в тази Бяла книга, Zel има за цел да реши проблема със скалируемостта и накрая да превърне визията на Ethereum в реалност. Създадохме екосистема от продукти и приложения за постигането на тази цел, съсредоточена върху достъпността и използваемостта.

2.0 Ethereum

Технологиите на Zel работят в симбиозни взаимовръзки помежду си и с технологии, простиращи се извън екосистемата на Zel. Zel е проектиран като отворена система в партньорство с технологии със затворен код. Вижте Раздел 4.0 за специфичните основи на Зел.

4.0 Основни функции на Zelcash

На повърхността си Zelcash е цифрова валута, която може да се копае, базирана на технологичните основи на крипто-валутата Zcash (известна преди като Zerocash), която се основава на Bitcoin. Zelcash използва zero-knowledge доказателство за първи път замислено в цифровите валути от Zcash, но се използва и от много други проекти, свързани с поверителността. Този факт осигурява сравнително голяма мрежа от разработчици на различни екипи, осигуряващи подобрения в протокола във времето, за да се укрепи основната функционалност на блокчейн технологията и основата на zero-knowledge протокола.

За разлика от Bitcoin - чиито претенции за анонимност са били опровергани през последните години - Zcash гарантира анонимност на потребителя чрез протокола zk-SNARKs (описан в раздел 4.2). С анонимността на крайните потребители на една транзакция, която е основен принцип на първоначалната визия на Bitcoin, подобренията и общото развитие на идеята за поверителност трябва да бъдат приветствани както от притежателите на този вид монети, така и от потребителите. Zel избра да използва характеристиките за поверителност на Zcash, за да наложи тази визия за анонимност и да увеличи възприемането на такава вид основна характеристика, въведена чрез голяма, скалируема мрежа.

Zelcash предлага икономически стимул за мрежата ни, състояща се от децентрализирани свръзки – ZelNodes, да предложи напълно скалируема, децентрализирана мрежа за развитие на блокчейна. Този стимул се създава чрез част от наградата за блок и евентуално чрез различни икономически модели като такси за транзакции или тарифи за операции в децентрализираните приложения (Dapps), които да подкрепят нашата визия за мощна и децентрализирана мрежа от свръзки, която позволява самостоятелни блокчейнове, приложения, тоукъни, интелигентни договори, и още много други.

4.1 T-транзакции

Транзакциите обикновено са записани върху блокчейна на Bitcoin. Те се извършват между адреси, известни като прозрачни адреси или t-адреси, получени първоначално от Bitcoin. Те се използват най-често всеки ден между портфейли и борси. Това е така, защото те изискват по-малка изчислителна мощност за изпълнение на транзакцията и могат да се изпращат от мобилни устройства и други преносими устройства.

4.2 Z-транзакции

Z-транзакциите са защитени или поверителни. Те се препращат между Z-адреси, известни също като защитени адреси. Zelcash ги е онаследил от Zcash и следователно се възползва от всички технически постижения и развития, които екипът на Zcash прави по отношение на развитието на Zcash и протоколите му, като подобренията на мрежата на хард форка Overwinter.

Ако се изпраща от един или повече защитени адреси, стойността на транзакцията (ите) се запазва поверителна. Само когато има прозрачен адрес на крайния получател, монетите ще бъдат разкрити (и транзакцията вече не е поверителна). Това ще покаже получената стойност само на този конкретен адрес в блока. Първоначалните адреси или входящия адрес заедно с изпратената стойност остават поверителни, когато са защитени по такъв начин. Протоколът на Zcash описва подробно този процес:

Стойността в Zcash е или видима, или защитена:

• Трансферите с видима стойност работят по същество като Bitcoin и имат същите свойства за поверителност.

• Защитената стойност се разбира от бележки, които определят сумата и ключа за плащане. Ключът за плащане е част от адрес за плащане, който се явява мястото, на което могат да се изпращат бележки. Както при Bitcoin, това се свързва с частен ключ, който може да служи за изпращане на бележки до адреса; в Zcash това се нарича ключ за разходване.

Всяка бележка има криптографски-асоциирана възможност за изпращане на бележки и уникален занулителя (така че съотношението е 1: 1: 1 между бележки, предаване на бележки и нулификатори). Изчисляването на занулителя изисква съответния частен разходен ключ. Невъзможно е да се съпоставят предаването на бележка със съответния занулител, без да е известен поне разходния ключ. Неизпратена валидна бележка в даден момент върху блокчейна е такава, за която предадената бележката е била публично достъпна на блокчейна преди този момент, но занулителя не го е допуснал.

Транзакцията може да съдържа видими входове, изходи и кодове, които работят като Bitcoin [Bitcoin-Protocol]. Също така съдържа поредица без никакви или няколко JoinSplit-a. Всеки от тях описва трансфер на JoinSplit, който приема видима стойност и до две входящи бележки и възпроизвежда видима стойност,

както и до две изходни бележки.

Занулителите на входящите бележки са разкрити (предпазвайки ги да бъдат изпратени отново) и действията по предаването на изходните данни, означава, че бележките ще се разкрият (позволявайки им да бъдат изразходвани за в бъдеще). Всяко описание на JoinSplit включва и доказателство за изчисление от тип zk-SNARK придружено със звук, което доказва, че всички от следните по-долу притежават, макар и с незначителна вероятност:

• Баланса на входящите и изходящите стойности (индивидуално за всеки JoinSplit).

• За всяка входяща бележка с различна от нула стойност, някои с наличие на задължение за бележка за нея самата.

• Доверителят знае частните разходни ключове на входящите бележки.

• Занулителите и ангажиментите за бележки са изчислени правилно.

• Частните разходни ключове на входящите бележки са криптографски свързани с подпис върху цялата транзакция, така че транзакцията да не може да бъде променяна от страната, която не е знаела тези частни ключове.

• Всяка изходна бележка е генерирана по такъв начин, че е невъзможно нейния занулител да взаимодейства с занулителя на друга бележка.

Извън zk-SNARK (защитени адреси) се проверяват също така дали занулителите за входящите бележки вече не са били показани (т.е. те вече не са били изразходвани).

Адресът за плащане включва два публични ключа:

1. разходен ключ, свързан с този на бележките, изпратени до адреса, и

2. предавателен ключ за шифърна асиметрична схема за криптиране.

"Шифърен" означава, че шифровите текстове не разкриват информация относно за кой ключ са били криптирани, освен за притежателя на съответния частен ключ, който в този смисъл се нарича ключ за преглед.Този уникален ключ се използва за комуникация с кодирани изходящи бележки към блокчейна до получателя им, който може да използва ключа за преглед, за да сканира блокчейна за бележките, адресирани до него и след това да декриптира бележките.

В основата на свойствата на Zcash за поверителност е следното: Когато се изпраща бележката, продавачът доказва само, че действието за него е било разкрито, без да разкрива какво е точно. Това означава, че изпратената бележка не може да бъде свързана с транзакцията, в която е създадена.

От гледна точка на конфликтност, наборът от опции за дадена бележка – възможността за проследяването ѝ - включва всички предишни бележки, които отсрещната страна нито контролира, нито знае, че са били изпратени. Това се различава с другите предложения за поверителни платежни системи като CoinJoin или CryptoNote, които се основават на преплитане на ограничен брой сделки и поради това имат по-малки възможности за проследяване на бележките.

Занулителите са необходими, за да се избегне двойното харчене: Всяка бележка има само един валиден занулител, така че опитът да се изпрати бележка два пъти би разкрил отново занулителя, което води до отхвърляне на повторната транзакция.

4.2. Доказателство за извършена работа

Откакто Накамото подобри работата на Hashcash на Adam Back, той създаде система за валидиране, която да разчита повече на криптографско хеширане, отколкото на доверие в централизирана система. Изхождайки от използването на алгоритъма SHA-256 от страна на Накамото за Bitcoin, Litecoin въведе алгоритъма Scrypt, последван от Dash и Ethereum, използвайки съответно алгоритмите X11 и Ethash. Последните разработки (разширявайки се върху идеята за X11, които са последователност от хеширащи алгоритми, при които изходът на един става вход за следващия) дойде с развитието на алгоритмите X13, X15 и X17.

Bitcoin е предназначен да бъде добиван от компютърни процесори (CPU), отнасящи се както до хеширане, така и до гласуване чрез процесори. След това, обаче бяха разработени усъвършенствани устройства като графичните процесори (GPU). Тъй като стойността на Bitcoin се увеличи и стимулът за добив стана по-голям, в изключително важен се превърна програмируемия хардуер, като програмируема логическа матрица (FPGAs), която да се използва за добив на Bitcoin. Те имат предимство пред обикновените процесори и графичните процесори. След разработването на FPGAs дойде времето на миньорски хардуер с определена цел, специфично разработени за приложенията интегрални схеми (ASICs), които от скоро доминират мрежата на Bitcoin, което значеше, че стана нерентабилно да се копае с процесори, както когато GPU миньорството навлезе, както и, че същата съдба може да споходи и GPU-тата благодарение на FPGAs.

Въз основа на идеята за свързване на множесвтво алгоритми заедно в последователност, която беше въведена за първи път в X11, скоро се появиха алгоритмите X13, X15, X17. Те работят по подобен начин, но с повече алгоритми, което означава, че е трудно за машините, които са предназначени да копаят под тези алгоритми.

Zelcash се базираше на основата на Zcash с неговите технологии за анонимност и ползите, които му спечелиха. Но тъй като много криптовалути са базирани на Zcash и използваха техния метод на доказателство за извършена работа и консенсус (PoW), стана икономически изгодно да се създаде ASICs за алгоритъма Equihash 200, 9. Много от криптовалутите като BTCZ, BTG, SAFE и други мигрираха към различен набор от N и K параметри, алгоритъм Equihash 144, 5 и започнаха да показват устойчивост срещу производителите на ASICs.

Екипът на Zel Dev беше определил да замени Equihash 200,9 с X16R за алгоритъм за добив на Zelcash. Развитието бе в ход, включвайки zk-SNARK в хеш алгоритъма, както и да се стартира тестова мрежа, но се появиха достоверни слухове, че

FPGAs/ASICs са били разработени за X16R, които биха могли да бъдат 100-1000x по-ефективни в добива с GPUs.

Въпреки, че се борим срещу ASICs, последните разработки в хардуера на FPGA представляват друго потенциално предизвикателство. Въпреки че CPU миньорството беше идеализирано, разбираме, че по-голямата част от миньорското общество в момента използва графични процесори и в края на краищата всички ние имаме някаква привързаност към графичните процесори. Така, че целта е да се намери противодействие на ASICs и се да се опитаме да запазим добива от GPUs.

Развитието на алгоритъма X16R за Zelcash беше преустановено. Количеството работа за импортиране на анонимността в X16R бе твърде голямо, а и противопоставянето на ASICs не толкова осезаемо.

Поради тези причини Zelcash ще промени алгоритъма за хеширане с променен алгоритъм Equihash с N и K параметри съответно 144 и 5, също като това, което направиха останалите анонимни монети. Това ще бъде "възпиращ лост", за да останем устойчиви спрямо ASICs и FPGAs и ще ни спечели известно време да се разкрие по-голяма част от бъдещия път на развитие. Решения се разработват постоянно, за да поддържа смисъла от миньорството с GPU и по този начин да се запази масива от децентрализирана екосистема на миьорските мощности. Една такава идея е progPOW (програмируемо доказателство за извършена работа), което ще бъде проучено и обсъдено от екипа на Zel през идните седмици. Ще бъде направено задълбоченото описание на бъдещите алгоритми и стратегии в бъдещите издания на тази Бяла книга.

Тъй като целта на Zel е да създаде децентрализирана мрежа, има смисъл да се запази разпространението на Zelcash сам по себе си, което на свой ред позволява създаването на мрежата на ZelDev, децентрализирано и възможно най-разпространено. Ние ще продължим да прилагаме нашата позиция да бъдем устойчиви срещу ASICs. Смяната на алгоритъма на доказателство за извършена работа ще бъде завършена до края на юли 2018 г.

И накрая, нашият алгоритъм за трудност ще се движи от стария Digishield V3 към LWMA на Zawy. Zawy's Linearly Weighted Moving Average (LWMA) носи много по-голяма последователност в таймингa на блока и се настройва много по-бързо от Digishield V3 при увеличавение на хеш мощностите. При нашите тестове, LWMA на Zawy е повече от десет пъти по-бърз при пренасочването към нов блок, отколкото това на Digishield V3. Новият алгоритъм относно трудността ще помогне

да се намали силата на атаките срещу хеш мощностите и timestamp атаките, тъй като Zel изкарва на пазара повече продукти и вероятно това ще доведе до повече хеш мощност в мрежата, докато проектът нараства. Този ход ще бъде направен и като част от надстройката на мрежата на Zelcash през месец юли 2018 г.

4.4 Награда от блок

По време на старта, Zelcash имаше забавен старт от 5 000 блока, след като фондът за разработки е бил осигурен от блок 5,000 нататък наградата за изкопан блок е била 150 Zelcash, която се разпределя на 100% за миньорите, извършващи доказателство за работа. С развитието на подходите към ZelNode-вете ще променим това, за да се погрижим да стимулираме собствеността на потребителите върху ZelNode и ще настъпи промяна в наградите. Това ще се ръководи от екипа и ще бъде решено от общността през следващите няколко седмици, последвани от излизането на тази статия.

Намерението на корекция в системата за наградите от блок ще бъде, за да осигури стойност както за миньорското общество, базирана на доказателство за извършена работа, така и за собствениците на ZelNode. Тази скала ще има възможност да се „плъзга" и по този начин се коригира, ако е необходимо, за да се осигури подходящ модел за възнаграждение за всички.

Наградата на блока ще бъде намалена наполовина на всеки 2,5 години, започвайки от датата на първоначалния блок.

4.5 ZelNodes

Концепцията за ZelNode-вете се появи от дискусия за това как потенциално да се разширят платформите за децентрализираните приложения и интелигентни договори и мрежа като например тази на Ethereum. Проекти като Lisk, Neo и други са могли да го направят. Въпреки това те са изправени пред риска да се отдалечат от децентрализацията, а вместо това - само предлагат предимствата на блокчейн технологиите по донякъде достъпен начин.

Ethereum е децентрализиран, така че се сблъсква с проблемите на скалируемостта, както изглежда и всички децентрализирани мрежи. С децентрализирани приложения (Dapps), като Crypto Kitties, които поставят мрежата на Ethereum на колене, резултатът е скъпи транзакции, които са бавни и

увеличават разходите за взаимодействие с интелигентните договори, които работят в мрежата.

Това не е само въпрос на разходи; това може да предизвика засечки в DAO и много други приложения, които работят в мрежата, което я прави неприемлива в свързания свят, в който живеем. Чрез създаването на стимулирана мрежа, подобна на DASH, Zelcash ни позволява да създадем една наистина децентрализирана и разпределена мрежа от свръзки. Това би позволило скалируемостта на мрежа, подобна на Ethereum, с много по-висока производителност на транзакциите. Използвайки ZelChains (странични блокчейнове), позволяващи повече транзакции в секунда.

Това е необходимо, ако трябва да преминем към децентрализиран интернет. Ethereum понастоящем не може да отговори на тези изисквания. Uber дава пример в реалността: С 12 превоза в секунда мрежата ще се задръсти, което означава, че конкурент като Lyft няма да може да работи в същата мрежа. Въпреки че визията на Виталик Бутерин е за потенциално 1 милион транзакции в секунда (TЗС), в момента тя е 15-20. С концепции като раздробяване, което е в процес на разработка, обаче е възможно Ethereum да успее да постигне тези числа.

Ние не сме склонни да хвърлим произволно число без безспорни доказателства, но на теория - в концепцията на ниво доказателство за извършена работа - мрежата на Zel ще може да достигне по-висока ТЗС от Ethereum за по-малко време. Със скалируемостта, постигната от ZelNode-вете, можем теоретично да съответстваме като ТЗС на мрежата на VISA. Имайте предвид, че това предположение за над 1000 ТЗС е точно това - предположение. Бихме искали първо да да докажем нашата технология, преди да „хвърлим" числата, които подлежат на промяна и въпреки това смятаме, че това е консервативна оценка.

Няма да спекулираме с истински ТЗС, докато основната мрежа не бъде пусната и добре тествана с месеци, за да можем да посочим реалистичен брой, който не е хиперболизиран или не е бил подложен на тестове.

4.6 Иконимика на ZelNode-вете

Стимулирането на свръзките, използвани за обезпечаване на мрежата на монетата и обработване на транзакции, са в основата около създаването на DASH - цифрова валута. Оттогава много проекти са добавили платформата на Masternodes (MNs) като средство за стимулиране на притежателите на монети, за заключване на количеството монети и за активизиране на размяната и миньорството. Някои проекти успешно са успели да интегрират MNs, докато някои по-нови валути с минимална сума са използвали привлекателността на MNs и тяхната огромна нереалистична възвращаемост, за да спечелят бърз растеж в общността и повишаване на капитала, което може да доведе до измами, разводняване на пазара, спад във възвръщаемостта на инвестициите и др. За да бъде създадена стабилна и децентрализирана мрежа за развитие на MN, наречена ZelNodes относно този проект, обезпеченията и възнагражденията трябва да бъдат реални и считани за дългосрочна инвестиция.

ZelNodes ще бъде сктруктура от свръзки на три нива, изискваща три различни нива на обезпеченост и хардуерни спецификации на системата, както и ще осигури три степени на награда. Наградите от ZelNode ще бъдат разпределени между притежателите на свръзки от частта от всеки изкопан блок в съотношение 25% за ZelNodes (свръзките), 75% за миньорите. Също така ще има скала, която може да бъде променяна за бъдещ растеж и стимулиране, което означава, че съотношението може леко да се коригира, ако е необходим за поддържането на голяма децентрализирана мрежа за компютърно-изчислителна мощност (виж

раздел 4.5 в случай на употреба). ZelNode също ще изисква високи възможности, поради което е необходим много стабилен ъптайм за получаване на наградата от свръзката; необходимият процент на ъптайм ще бъде публикуван близо до датата на пускането на ZelNode-вете.

Предполагаеми системни изисквания за хардуер за Zelnode:

Вид спецификация	Zelnode Basic	ZelNode Super	ZelNode BAMF
CPU	2 vCores	4 vCores	8 vCores
RAM	4GB	8GB	32GB
Storage (SSD)	50GB	150GB	600GB
Bandwidth	2.5TB	4TB	6TB

Засега трите ZelNode нива са наречени ZelNode Basic (с най-ниско ниво на необходима обезпеченост), ZelNode Super и ZelNode BAMF (изисква се най-високото ниво на обезпеченост). Всяко ниво на ZelNode има изисквания за VPS системата, което се означава по-скъпо ниво на обслужване на VPS. Всички ZelNode-ве ще имат изискване за актуализиране, така че изискванията за време и спецификация на системата ще бъдат тествани от Zel, за да се осигури съответствие с правилата и че разпределението на наградата е заслужено.

Предполагаема обезпеченост и структура на възнагражденията:

Ниво	Обезпеченост [Zel]	Награда % (от 25% за всеки блок)
ZelNode Basic	10,000	15%
ZelNode Super	25,000	25%
ZelNode BAMF	100,000	60%

Широкият обхват на размера на обезпечеността позволява на голям брой хора да участват в системата на ZelNode-вете, ако пожелаят, и нелинейното скалиране на обезпечението/наградата е необходимост, така че например 10 ZelNode Basic-а да не могат да печелят повече от 1 ZelNode BAMF.

Икономическият модел е разработен с прогнозна цена на монетата Zel от $ 1 USD до края на 2018 г. Като дългосрочна инвестиция разходите, свързани с

управлението на ZelNode, са сравнително незначителни и се приема, че са променливи по природа, подобно на спекулативните печалби от миньорството с графични карти, където мигновената печалба не е единствено изискване на инвеститора.

С възможността леко да променя съотношението на наградата от блока, увеличавайки го или намалявайки го, екипът на Zel има известна способност да поддържа определен брой свръзки в мрежата чрез увеличаване на наградата, ако общият брой свръзки спадне под прага или чрез намаляване на наградата в обратния случай. Тази функция ще бъде използвана изключително рядко и се смята за "последна инстанция" за поддържане на ZelNode-вете в мрежата на Zel.

5.0 Двоен икономически модел

Zelcash е механизмът на транзакцията за платформата Zeldev. Процесите, таксите и услугите ще бъдат пряко свързани с инфраструктурата на ZelDev и ще изискват монетата Zelcash; все пак изследваме възможните дългосрочни развития около "двойния икономически модел". Тъй като децентрализираните борси и приложения се развиват, трябва да се развият и визията за икономика, базирана на услугите, както и валута основана на структурата.

Осъзнаването на необходимостта от стабилна мрежа от миньори, свръзки и разработчици ще затвърди Zelcash и платформата Zeldev. Тъй като развитието на децентрализираната борса (DEX) и DApps стои на преден план, необходимостта от финансиране и поддръжка на разработчиците е от съществено значение. Разбирайки, че това е нещо, което трябва да се обмисли, създаването на Фондацаията е от ключово значение за ангажиране на общността около моделите за дългосрочно финансиране.

6.0 Zel Technologies

Zel Technologies работи над различни проекти и приложения в допълнение към Zelcash. Всички те живеят и си взаимодействат в отношения на симбиоза в екосистемата на Zel.

Проектът се основава на идеята за създаване на децентрализирана блокчейн мрежа, състояща се от блокчейн, подобен на този на Ethereum, с по-висока

производителност на транзакциите, благодарение на консенсуса, който се установява между операторите на ZelNode-ве. Напускайки главния блокчейн, подобен на Ethereum, блокчейна на "ZelDev" ще бъде разположен върху ZelChains. ZelChains ще работят като странични вериги в среда от тип Lisk, позволяваща на тези блокчейнове да комуникират помежду си, ако те го изискват, но и да могат да се справят с по-високата производителност на транзакциите и да се възползват от работата на истинската децентрализирана мрежа.

Това препраща Zel към следните важни теми:

• да разреши проблемите със скалируемостта, пред които е изправен Ethereum и подобни проекти; както и

• да се позволи децентрализираните приложения, интелигентните договори, децентрализираните оракули, системите за гласуване и т.н. да бъдат разработени по скалируем начин.

С този напън (започнат от Сатоши Накамото) ние се отделяме от централизирания интернет, който всички ние познаваме от преди няколко години (и все още използваме и днес) към децентрализирания интернет и свят.

Останалите проекти като ZelTreZ, ZelPay, Zel ID и др. ни позволяват да създадем тази екосистема за разработване на технологии за в бъдеще.

6.1 ZelTreZ

ZelTreZ се появи от желанието на екипа за по-добра платформа на портфейла от това, което се предлагаше в пространството с отворен код. Zel се замисли за разработването на олекотен портфейл и такъв, явяващ се „пълноценна свръзка”, който просто включваше Zelcash. Той е създаден така, че да дава възможност на потребителите да избират кои опции са им необходими. От началото на тази разработка ние започнахме да осъзнаваме потенциала на платформата и като такава идеята се разви и процъфтя в това, което е днес всъщност. Сега ZelTreZ е портфейл с множество активи, който предлага както олекотена версия, така и

„пълноценна свръзка” като опции за потребителите.

Проектиран за лесна употреба със свеж и лек потребителски интерфейс, ZelTreZ се превръща в портал за света на криптовалутите. Понастоящем се поддържат ZEL, BTC, LTC, ZEC, ETH, BTCZ, RVN, BNB и HUSH, като нови проекти се публикуват на всеки две седмици заедно с актуализации и подобрения в сигурността. ZelTreZ използва криптиране, за да държи потребителите в безопасност; това ни позволява да създаваме профили, без да съхраняваме информация за потребителя на отдалечен сървър. Тъй като развитието на Zel продължава, изпълнението на ZelDev ще покаже нашата децентрализирана мрежа за разработка чрез ZelTreZ с помощта на ZelDex, нашата децентрализирана борса, която ще бъде предлагана в рамките на платформата ZelTreZ.

Освен че е магазин за DApps, той също е и портал за разработчици и студенти, които могат да научат за развитието на блокчейна и да започнат да използват платформата на ZelDev за разработване на собствени DApps и приложения за блокчейн. Понастоящем е достъпен за Windows, Linux и MacOS, ZelTreZ ще бъде имплементиран към уеб приложението, като приставка за Chrome, Android и iOS, позволявайки вход от различни профили и устройства, без да се съхранява информация на нашата инфраструктура.

6.2 Zel ID

Zel ID е система за удостоверяване, предназначена да даде възможност на потребителите да поддържат пълен контрол над цифровата си идентичност. Тя потенциално позволява на потребителите да съхраняват собственост, здравни досиета и друга информация в децентрализирана, криптирана мрежа, а не на хартия или на централизирани сървъри; това ще даде на потребителя контрол върху информацията и поверителността, която липсва в настоящия цифров свят.

Zel ID се задвижва от същите концепции за сигурност, представени от Authparty - базирана на Bitcoin/Counterparty система за удостоверяване, разработена от члена на екипа на Zel Матю Райхард. Zel ID постига удостоверяване със zero-knowledge метод чрез използване на подписи, генерирани от публичните и частните ключове на вашия портфейл. Това на практика отрича необходимостта

от 2FA (двоен подпис за удостоверяване), тъй като удостоверяването изисква достъп до портфейла ви. Вашият портфейл, в този случай ZelTreZ, ще бъде толкова важен, колкото мобилен телефон или интернет връзка.

Уникалните идентификационни данни за самоличност, наречени "Персони", се генерират и използват за удостоверяване чрез zero-knoweledge метод на трети страни или доставчици на услуги.

Zel Registry предоставя API достъп до протокола за удостоверяване Zel ID. Чрез генерирана „Персона" се създава нова идентичност, наречена "Единица", и се прикрепя към Персоната. По този начин доставчика - трета страна, удостоверяваща се чрез ID на Zel, ще има три нива на обособяване спрямо истинската ви идентичност, допускайки различни „Персони", като същевременно предоставя възможност за анонимност.

6.3. ZelPay

Един опростен, но жизненоважен софтуер като ZelPay може да се използва в терминалите в магазините, както и в уеб приложенията. Целта на ZelPay е да осигури на потребителите лесна употреба и прозрачност и да предложи на бизнеса липса на такси или 1% такса от транзакциите.

Ползата от ZelPay е уеднаквено приложение, което предлага лесна употреба както в магазина, така и онлайн и дава на собствениците на бизнеси достъп до по-високи нива от аналитични данни и подробности за продажбите, за да им помогне да развият и разраснат бизнеса си. ZelPay ще бъде създаден, за да позволи на бизнеса да приема не само всички криптовалути в ZelTreZ, но също така потенциално и фиатни валути в един блокчейн на материализирани активи, който е едно към едно, подплатен с USD, GBP, EUR, YEN или злато и други активи Това би позволило по-свободна и по-лесна търговия с по-високи възможности в процесите на транзакции в системите, отколкото предлаганите от други криптовалути решения.

ZelPay ще предложи опции като NFC технология и QR-код, за да улесни

безконтактното плащане чрез мобилното приложение ZelTreZ, както и плащанията за електронна търговия, използвайки подобен метод, който позволява безпроблемен и бърз опит както за клиентите, така и за търговците.

Хипотетично изпълнение за ZelPay и други приложения на блокчейна:

Вече видяхме приемането на павилиони за самообслужване в магазините за хранителни стоки, премахвайки необходимостта от множество служители. Вместо това само трябва да се гарантира, че машините работят правилно, а ЕГН-то на тези, които купуват алкохол се проверява. За да извлекат ползи от тази идея, роботизираното пазаруване се тества от Amazon и други компании, като тези системи вече са били приложени в някои градове.

Това се постига чрез процес, който звучи сложен, но всъщност е толкова естествен и лесен, колкото и използването на смартфон. Купувачът сканира QR код, за да влезе в магазина; това е неговата количка. Когато купувачът влезе, той избират желаните от него неща и ги поставя в „проверка на сметка". Тя чете RFID кодовете, които се намират върху продуктите, генерира друг QR код или позволява NFC плащане, а купувачът има право да си тръгне с покупките. Тази система може да бъде подобрена, но това е отличен пример как технологиите подобряват опита на клиентите и намаляват разходите на бизнеса.

6.4. ZelDev

ZelDev ще бъде проектиран около разработчиците, за да работи възможно най-лесно с блокчейн. Ще постигнем това, като дадем на разработчиците достъп до ZelSDK (Software development kit) и BDK (base derivation key), което ще позволи лесното възприемане на блокчейна в бъдещите или вече съществуващи проекти. Ще има някои шаблони в ZelChains, които ще помогнат на разработчиците да започнат отнякъде и ще позволят на разработчиците да си взаимодействат чрез Javascript. Също така, шаблони на интелигентни договори заедно с шаблони за токъни ще бъдат на разположение и ще позволят интелигентните договори да бъдат написани на Javascript. Това намалява бариерата за навлизане на разработчиците, тъй като Javascript е най-широко използваният програмен език. За да се справят с транзакциите на токъни, те ще бъдат разпределени в отделни

блокчейнове, които когато е необходимо, ще комуникират с основния блокчейн на ZelDev. Това също така позволява по-високи възможности за обем на транзакциите и например може да намали влиянието, когато определен блокчейн е в поддръжка.

Техническите характеристики относно платформата на ZelDev и продуктите, пряко свързани с нея, ще бъдат оповестени по-късно.

6.5 ZelChains

Основният блокчейн на ZelDev заедно със ZelChains (странични блокчейнове) са блокчейновете, които ще извършват процесите в мрежата на ZelNode-вете. Това ще позволи истинска децентрализация по скалируем начин, тъй като ще бъде гарантирано, че наличните изчислителни ресурси от общия брой ZelNodes ще са обезпечени в мрежата на Zelcash. Това дава възможност за отваряне на други преки пътища за ресурсите, ако една или повече ZelChains се наситят и драстично се увеличи общия брой възможни транзакции в секунда, които Zel може да обработва.

6.6 ZelDex – Децентрализирана борса

Понастоящем най-големите борси за криптовалути са централизирани. В повечето случаи потребителят не притежава своите частни ключове към портфейлите на борсата и като такъв не притежава криптовалутата, която е в тяхната "сметка за обмен".

Въпреки, че централизираните борси в момента предлагат много по-добър опит, както и повече транзакции в секунда, децентрализираните борси се подобряват. С новите борси, които предлагат на потребителите контрол над техните частни ключове, ние сме в началото на революцията във борсовия пазар. Основният проблем, който затруднява възприемането на децентрализирани борси, е въпросът за скалируемостта, дължаща се отчасти на тяхната инфраструктура.

ZelDex ще бъде изградена на върха на мрежата на ZelDev като демонстрация на възможностите й. Интерфейсът ще бъде проектиран така, че да е лесен за навигация, но достатъчно цялостен за напреднали потребители. С интегрирането й директно в ZelTreZ, както и като самостоятелна платформа за уеб и мобилни устройства, ZelDex се стреми да бъде първата децентрализирана борса с масово възприемане в пространството.

Също така, отворените API входове ще позволят на разработчиците да използват ZelDex в своите приложения за обмен на тоукъни и валути.

6.7 ZelDapp - Магазин за децентрализирани приложения

Магазинът за приложения ZelDapp ще бъде основно хранилище за децентрализирани и някои централизирани приложения, с по-занижени изисквания за достъп, с някои правила и разпоредби, които да гарантират законност. Магазинът за приложения е разработен така, че да позволява на разработчиците достъп до голяма база от потребители решено чрез преплитане на различни платформи. ZelTreZ се явява възможност за тестване на тези децентрализирани приложения, които работят вътре, позволявайки по-бърз достъп и време за разработка, без да се налага да чакате одобрение от определени компании.

ZelDapps се различават от другите предложения, че не е необходимо да сте експерт. Структурата ще бъде достъпна чрез лесен SDK (software development kit), който вероятно ще бъде базиран на Javascript и евентуално други езици при разработването на платформата. Използването на изключително популярен език за програмиране осигурява лесен достъп до инструментите за разработка и достъп до широк кръг от програмисти - професионални такива, както и любители.

В Zel Technologies ние вярваме, че хората трябва да могат да общуват свободно и без ограничения. За тази цел ще бъде създаден месинджър като първо децентрализирано приложение. След това той ще последван от платформа за социални медии, която позволява на хората да изразяват своите мнения без цензура (в рамките на закона).

Таксата в магазина на ZelDApp ще бъде съвсем малка или без наличие на такава. Тя ще бъде замислена така, че да бъде свободен и отворен пазара, за да може разработчиците да достигат до потребителите.

7.0 Водещ принос към Бялата книга

Основател- Майлс Менли
Партньор и разработчик- Луми Ибиши
Партньор и водещ разработчик- Тадиъс Кмента
Водещ съветник- Даниел Келър
Мениджър на проекта и съветник- Паркър Хъниман

Дарение: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

От деня, в който бе създаден, биткойн завинаги промени финансовата свобода за тези, които избират различния път. Технологията е великият лост, на всички, които създават бъдещето, поздравяваме ви!

-Екипът на ZEL

8.0 Бъдещето на Zel

Zel ще бъде постоянно развиваща се екосистема. Екипът е посветен на промяната в промяната в света да извлече ползи от блокчейна и криптовалутите. За тази цел Zel ще се ангажира активно с нови и нововъзникващи технологии, проекти и разработки за развитие. Ние вярваме, че пространството ще се нуждае от лидери, които да въведат нови технологии и бихме искали да бъдем на преден план.

Вървейки напред, екипът на Zel ще:

- да продължи да разработва нови технологии, основани на модела Zelcash, както в проекти с отворен, така и в проекти със затворен код
- да си сътрудничи с другите в сферата, за да сме сигурни, че проектът ще е в челните редици на крипто сферата
- развива и насърчава общността около платформата на Zel, която ще ръководи ценностите и резултатите от бизнес модела.
- Разработване и насърчаване на благотворителна дейност на фондация "ZEL" за подобряване на останалите възникващи технологии.

9.0 Речник

Altcoin—Криптовалута, която не е биткойн

ASIC (application-specific integrated circuit)—Силиконови чипове специално разработени, за да изпълняват една единствена задача (копаене на криптовалута). В случаитес с биткойн, те са разработени да извършват хашинг процеси под алгоритъм SHA-256 и да копаят нови биткойни.

Cross-chain technology—Позволява на два блокчейна да обменят информация и крипто активи по едно и също време

DASH—Вид криптовалута базирана на софтуера на биткойна, който предлага анонимност; познат преди като XCoin (XCO) и Darkcoin.

Fiat money-- Валути с минимална или никаква вътрешна стойност, но определени като законно платежно средство от правителството, като например книжни и монети.

JoinSplit-- данни, включени в транзакция, която описва JoinSplit трансфер, т.е. трансфер със защитена стойност. Този вид трансфер на стойност е основната операция, специфична за Zcash, извършена като транзакция.

Litecoin (LTC)—Криптовалута, създадена от бивш служител на Google Чарли Лий през 2011. Предоставя възможност за по бързо изпълнение на процесите на по-ниска стойност.

NEO—Отнася се към криптовалутите и до първия блокчейн на Китай с отворен код. Точно като Ethereum, тя може да изпълнява „интелигентни” договори или денцентрализирани приложения , но в някак си централизирана среда.

Overwinter fork—Първият и единствен за сега хард форк на Zcash, отнасящ се до мрежата и подобрения в представянето й по други точки, за да подсили протокола за следващите подобрения.

Multi Signature (multisig)— Адреси с множество ключове позволяват на няколко страни да изискват повече от един ключ за разрешаване на транзакция. Тези адреси имат по-голяма устойчивост от кражба.

Private Key—Частен ключ е низ от данни, което дава контрол на потребителя до

публичния ключ и адреса, за да разреши транзакция на криптовалути.

Proof of Stake (PoS)—Алгоритъм, който възнаграждава участниците, които разрешават сложни криптографски задачи, за да постигнат децентрализиран консенсус. PoS потребява по-малко енергия отколкото PoW.

Proof of Work (PoW)—Алгоритъм, който възнаграждава първия човек или група хора (басейн), който/които разреши/ат компютърно-изчислителна задача, за да постигне децентрализиран консенсус.

Z-cash—Една от първите криптовалути, насочени към поверителността

Zel ID-- Система за разпознаване, която създава онлайн профил на потребителя, Система за разпознаване, която създава онлайн профил на потребителя, които да бъдат използвани във всеки аспект на живота и във всяка система, която изисква верификация и валидиране на самоличността в реалния живот.

ZelChains—Помощните „вериги”, които ще вървят на мрежата на Zelcash, за да осигурят използваема компютърно-изчислителна мощ и скалируемост за разработчиците на денцентрализирани приложения.

ZelDev—Платформата за децентрализирани приложения на разработчиците да взаимодействат с блокчейна на Zelcash и ZelChains чрез лесни за използване SDK (software development kit) и BDK (Base Derivation Key).

ZelDex—Децентрализирана борса създадена от Zelcash, за да управлява децентрализираната мрежа чрез ZelTreZ, както и чрез самостоятелен уеб портал, ZelDex ще бъде използван като флагман на технологията на ZelDev.

ZelNodes—Мрежа, състояща се от няколко нива на компютърно-изчислителна мощност изпозвана от разработчиците на децентрализирани приложения (Dapp) и разпространението на тоукъни, която е стабилна, скалируема и напълно децентрализирана.

ZelTreZ—Фронтенд платформата на Zelcash, ZelTreZ е мултифункционален криптиран портфейл, в който ще бъде разположен Dex, управляващ портфейлите чрез ZelNode-ве (пълноценните свръзки) и съдържащ Dapp Store.

zk-SNARK—Поверителен протокол, въведен за първи път в криптовалутите от Zcash, който позволява защитени транзакции да осигурят анонимност на крайните

потребители. (Вж. Бялата книга на Zcash за техническо обяснение)

Източници

[1] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system

[2] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Zcash Protocol Specification Version 2017.0-beta-2.5.

[3] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. (2014) Zerocash: decentralised Anonymous Payments from Bitcoin

[4] Vitalik Buterin and the Ethereum Project: A Next-Generation Smart Contract and decentralised Application Platform, Ethereum

[5] Tron Black and Joel Weight: X16R ASIC Resistant Design

lEIKa