Институт по Математика и Информатика

Българска Академия на Науките

Секция Математически Основи на Информатиката

Живко Стефчев Желязков

Платформи за Интелигентни Договори

Автореферат на дисертация

за присъждане на образователна и научна степен доктор

в професионално направление 4.6. „Информатика и компютърни науки“

Научен ръководител: доц. Христо Костадинов

София, 2025 г.

Въведение

Целта на тази дисертация е да се разработят подходи, които да адресират няколко широко разпространени предизвикателства, включително стимулирането на научните изследвания, внедряването и текущата поддръжка на бизнес софтуерни системи в реални оперативни среди и генерирането на доказуемо случайни числа. Решенията са реализирани с помощта на разпределена архитектура, базирана на блокчейн [1-10], която отговаря на изискванията на съвременния софтуер за доставка и внедряване на бизнес софтуерни системи. Основна част от дисертацията (Глава 3) обхваща етапите от жизнения цикъл на разработване на системи (SDLC) [11-14], като се обръща специално внимание на фазата, свързана с внедряването на софтуера от крайните клиенти, както и на последващите актуализации на софтуерните версии. Значението на този процес изисква той да се извършва по надежден начин, с минимално прекъсване на бизнес процесите и пълна проследимост на отговорностите на всеки участник. Архитектурата на блокчейн-базираните системи предвижда автоматизиране на стъпките, свързани със специфични отговорности и ключови показатели за ефективност (KPI), чрез интелигентни договори, така че засегнатите страни да бъдат уведомявани своевременно. Важно място заема и анализът на сигурността и надеждността на процесите, гарантирани от блокчейн протоколи, базирани на криптографски алгоритми.

Блокчейн технологията е сравнително нова технология, а началото ѝ често се свързва с криптовалутата Bitcoin [15-18]. За разлика от криптовалутата обаче, това, което интересува разработчиците на блокчейн софтуер, са предимствата на самата технология с нейните характеристики като дистрибутивност, сигурност, надеждност и качествено нови архитектури на комуникация между участниците в бизнес процесите. Тези характеристики я правят много подходяща като основа за разработената блокчейн система. Поради съвременния си характер и актуалност, в момента съществуват десетки варианти на блокчейн платформи с привидно много сходни, но същевременно доста различни характеристики. Това изисква подробно разглеждане на популярните налични платформи и избор на най-подходящата, която да отговаря на изискванията на всеки процес.

Важна част от дисертацията е разработването на прототип, който демонстрира как основните модули, връзките между тях и комуникационните протоколи решават поставените цели за дадената архитектура. Прототипът в глава 4 е изграден върху блокчейн платформата EOSIO/Antelope [19-21], която е с отворен код и се отличава с бърза,

мащабируема и сигурна обработка на транзакции. За съхранение на големи данни се използва InterPlanetary File System (IPFS) [22-24] - ново поколение децентрализирана разпределена мрежа за съхранение, наречена Interplanetary File System. IPFS използва адресиране на съдържание, за да идентифицира уникално всеки файл в глобално пространство от имена. Файловете, качени в IPFS, се разпределят на множество компютри и им се присвоява хеш стойност, която позволява на потребителите да ги локализират.

След добива на първия биткойн през 2009 г. и въвеждането на Ethereum [25–27] през 2015 г. като блокчейн платформа, поддържаща интелигентни договори, множество индустрии са придобили увереност в надеждността и предимствата на тази технология. Това е предизвикало вълна от нови софтуерни архитектури, които коренно променят конвенционалните бизнес модели и сектори. Известни примери включват застраховане, здравеопазване, банково дело, финанси и други, всички характеризиращи се с участието на множество участници във всеки процес, където транзакционната информация трябва да се съхранява постоянно и да остане защитена от неправилно използване. В тези контексти надеждната и проследима комуникация между участниците е от съществено значение и в много случаи е необходимо наличието на арбитражна организация за разрешаване на спорове, свързани с отговорност и обезщетение.

Именно релевантността и основните характеристики на блокчейн технологията – нейното разрушително въздействие върху традиционните индустрии и способността ѝ да се справя със сложни сценарии с високи залози – позволяват проектирането на качествено нови архитектури, основани на блокчейн платформи.

Структура на дисертацията

Дисертацията е разделена на въведение и шест глави. Дисертацията съдържа 135 страници, 48 фигури, 3 таблици, 57 цитирани литературни източника и 2 приложения. Публикувани са 2 публикации по дисертацията, всички от които са доклади от международни конференции.

Първата глава предоставя общ преглед на DLT технологиите, техните ключови характеристики, видове и класификации. Обяснени са концепциите, които се използват по-нататък в дисертацията. Описани и анализирани са основните елементи на функционирането на DLT, както и как се осигурява сигурността на комуникацията и как се постига консенсус. Направени са основни заключения въз основа на проучени литературни източници и са формулирани насоки и функционалности, които са от значение за проектирането на предложените нови блокчейн системи.

Обоснован е изборът на блокчейн платформа и технологични средства за внедряване на системата. Описани са характеристиките на различните съществуващи платформи и е анализиран анализ на това как техните специфики биха могли да отговорят на предизвикателствата в различни области.

Глава 2 описва разпределена система за стимулиране на научните изследвания. Базирана е на EOSIO технология и позволява на различните страни да задават специфични задачи, които други страни да решават, и да предоставят стимули под формата на блокчейн токени.

Глава 3 представя традиционната област на SDLC с нейните ключови сценарии, участници в процеса, както и предизвикателства при внедряването и актуализирането на софтуера. Предизвикателствата са описани и по отношение на изискванията към новата SDLC система, която би трябвало иновативно да преодолее трудностите, свързани с типичните стъпки за актуализиране на софтуера. Най-съществената част, представена в Глава 3, е дефинирането на иновативния блокчейн дизайн на SDLC и анализ на това как той преодолява съществуващите класически SDLC предизвикателства.

Глава 4 описва архитектурата на практическа система за генериране на доказуемо случайни числа и резултатите от изграждането на прост, но стабилен прототип, базиран на иновативната архитектура, като описва подробно средата, в която работи: интерфейси, интелигентни договори, модули и агенти, комуникационни протоколи и др.

Глава 5 описва приноса на дисертацията и научни публикации по дисертацията.

Последната глава 6 обобщава резултатите от разработването на трите сценария, описани в глави 2, 3 и 4, и анализира различните сценарии, успешно решени от иновативните архитектури. Демонстрирани са предимствата, особено в областите на проследимостта, сигурността и надеждността на резултатите.

Глава 1. Преглед и анализ на технологиите на разпределения регистър (DLT)

Блокчейн е най-разпространеният вид технология за разпределен регистър (DLT), която се състои от нарастващи списъци със записи, наречени блокове, които са сигурно свързани помежду си чрез криптография. Всеки блок съдържа криптографски хеш на предишния блок, времеви печат и данни за транзакцията. Времевият печат доказва, че данните за транзакцията са съществували, когато блокът е бил създаден. Тъй като всеки блок съдържа информация за предишния блок, те ефективно образуват верига, като всеки блок е свързан с тези преди него. Транзакциите в блокчейн са необратими, защото веднъж

записани, данните във всеки блок не могат да бъдат променяни със задна дата, без да се променят всички следващи блокове.

Блокчейнът се съхранява в разпределена мрежа, където всеки участник в мрежата има копие на веригата на своя компютър. По този начин няма едно-единствено, специфично главно копие и няма риск от повреда, загуба или манипулиране на информация. Участниците в мрежата са равнопоставени (peer to peer) и следват специфичен протокол за валидиране на нови блокове. Веднъж валидиран и записан, никой блок не може да бъде променен без одобрението (консенсуса) на останалите участници във веригата блокчейн.

Идеята за блокчейн се появява за първи път през 1982 г., когато криптографът Дейвид Чаум представя дисертация, озаглавена „Компютърни системи, създадени, поддържани и доверени от взаимно подозрителни групи“ [28], в която описва дизайн за разпределена компютърна система, която може да бъде създадена, поддържана и доверена от участници, които не се познават. Година по-късно той публикува статията „Слепи подписи за непроследими плащания“ [29], в която подробно описва нова форма на криптография, която според него може да позволи автоматизирана платежна система, в която трети страни не могат да видят информацията за плащането. Идеята зад блокчейн технологията е доразвита през 1991 г., когато изследователите Стюарт Хабер и У. Скот Сторнета представят изчислително практично решение за маркиране на цифрови документи [30], така че те да не могат да бъдат датирани със задна дата или фалшифицирани. Системата използва криптографски защитена верига от блокове за съхраняване на документи с времеви печат, а през 1992 г. в дизайна са включени дървета на Меркел [31], което го прави по-ефективен и позволява комбинирането на множество документи в един блок.

Концепцията за Proof-of-Work, която е ключова за функционирането на блокчейн, датира от 1992 г., когато Мони Наор и Синтия Дуорк се опитват да се справят с проблема със спама по имейл. Концепцията е предназначена да обезкуражи спама, като изисква от изпращачите на имейли да извършат някои изчислителни упражнения, преди да изпратят имейл. Подробно описание е публикувано в статията „Ценообразуване чрез обработка или борба с нежеланата поща, напредък в криптологията“ [32].

През 1997 г. Адам Бак разработва протокол, наречен Hashcash [33], по-усъвършенствана концепция за предотвратяване на спам по имейл. Самият Hashcash вече включва решение за двойно харчене, включващо така наречената концепция за „защита от двойно харчене“. Интересното е, че тези първоначални концепции самите по

себе си не са били наричани Proof-of-Work.

През 1999 г., две години след концепцията на Адам Бак за Hashcash, беше публикувано академично есе от Ари Джуелс и Маркус Якобсон, озаглавено „Протоколи за доказване на работа и хлебен пудинг“ [34]. Тогава за първи път се появи терминът „доказателство за работа“ (PoW).

През 2004 г. Хал Фини разработи концепцията за „повторно използваемо доказване на работа“ (RPOW), която се основава на концепцията на Адам Бак за Hashcash. Като такава, тази концепция все още се счита за важна част от развитието на дигиталните пари и основен предшественик на Bitcoin.

В края на 2008 г. архитектурен документ, въвеждащ децентрализирана peer-to-peer система за електронни пари, наречена Bitcoin, беше публикуван на криптографски форум от лице или група, използващи псевдонима Сатоши Накамото. „Bitcoin: Peer-to-Peer система за електронни пари“ на Сатоши Накамото съдържа първото подробно описание на Bitcoin/блокчейн. Документа описва концепция за надеждно изпълнение на финансови транзакции в разпределена мрежа, базирана на криптографски алгоритми.

На 3 януари 2009 г. първият блок Bitcoin е добит от Сатоши Накамото, който получава награда от 50 биткойна. Първият получател на Bitcoin е Хал Фини, който получава 10 биткойна от Сатоши Накамото в първата в света транзакция с Bitcoin, която се състоя на 12 януари 2009 г.

През 2013 г. Виталик Бутерин, програмист и съосновател на Bitcoin Magazine, заявява, че Bitcoin се нуждае от скриптов език за изграждане на децентрализирани приложения. Неспособен да постигне консенсус в общността, Виталик започва да разработва нова разпределена изчислителна платформа, базирана на блокчейн, Ethereum, която включва скриптова функционалност, наречена интелигентни договори. Интелигентните договори са програми или скриптове, които се имплементират и изпълняват в блокчейна на Ethereum. Те могат да се използват за извършване на транзакция, ако са изпълнени определени условия.

1.1. Връзка между блокчейн технологията и DLT

Много често DLT и блокчейн се използват като едно и също определение за разпределени цифрови бази данни и разликата между тях остава неразбрана. Основата е концепцията за разпределена база данни между много сървъри, без нужда от централен сървър, като по този начин се гарантира надеждност и сигурен достъп до базата данни, както и, разбира се, други важни

характеристики като автентичност, сигурност и др. И макар определението за DLT да е точно както е описано по-горе, блокчейн е специфично и най-популярно приложение на това определение. Казано по-просто, връзката в този случай е като плод - ябълка. Понякога е по-лесно да се опише ябълка и след това да се обобщи какво е плод. Може да се каже, че блокчейн направи DLT популярен термин след навлизането на Bitcoin на пазара през 2009 г. Оттогава, поради различни сценарии и бизнес нужди, са дефинирани различни подтипове на DLT, които се различават по начина, по който се прилагат.

DLT е определение за криптирана и разпределена база данни, която служи като регистър, в който се съхраняват записи на транзакции. В основата на DLT е иновативен подход към база данни, при който криптографията се използва за всяка актуализация на транзакцията и проверката става възможна в конкретната разпределена мрежа. В зависимост от това как е реализирана тази дистрибутивност, в зависимост от това как информацията е структурирана и валидирана, наблюдаваме няколко вида/подмножества на DLT. Блокчейн е най-разпознаваемият вид DLT. При него транзакциите се добавят в блокове, които са последователно свързани чрез криптографски хеш.

Преди да опишем предимствата и недостатъците на всеки подтип DLT, е необходимо да разгледаме по-подробно основните концепции и етапи на работа на DLT. В следващата глава, наред с приликите на основните етапи на валидиране, разпространение и съхранение на информация, ще бъдат обсъдени някои от съществените разлики между различните подтипове. Това ще ни позволи на по-късен етап да оценим кой подтип е подходящ за решаване на конкретен бизнес сценарий.

1.2. Types of blockchain

Блокчейн платформите могат да бъдат изградени по различни начини, с различни права за възлите в мрежата, различен достъп до мрежата и различни механизми за консенсус. В зависимост от това могат да бъдат дефинирани различни видове [35] блокчейни, както е описано на Фигура 8.

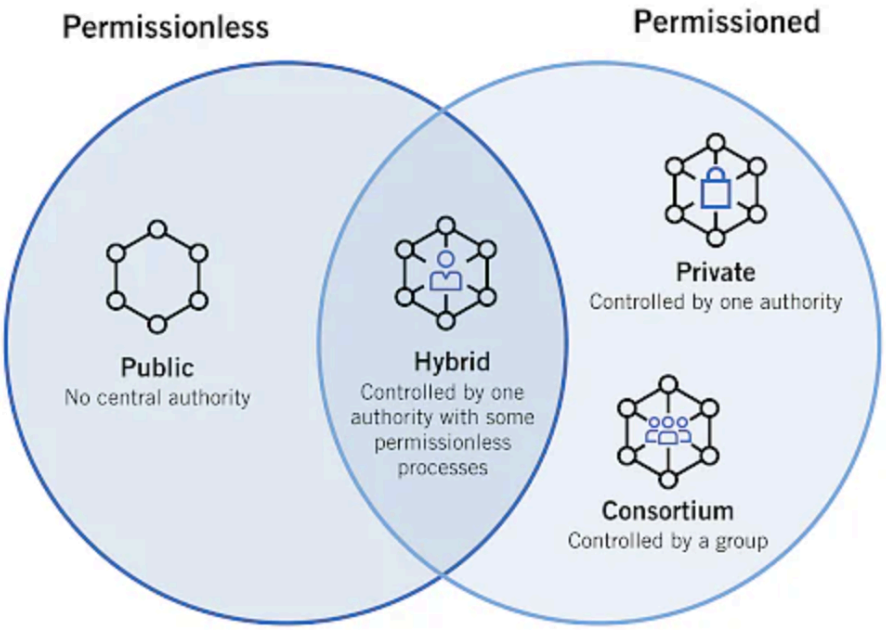

Figure 8 Types of DLT

Публичен Блокчейн

Публичният блокчейн е децентрализирана мрежа, към която всеки може да се присъедини и да участва. Публичните блокчейни позволяват на всички възли да имат равен достъп до блокчейна, което позволява добавянето на нови блокове данни и валидирането на съществуващи блокове данни. Популярни публични блокчейни са Bitcoin, Ethereum и Litecoin. Те се използват най-вече за обмен и добив на криптовалути.

Предимства: Доверие, сигурност, прозрачност.

Недостатъци: По-бавни транзакции, по-висока консумация на енергия за постигане на консенсус.

Частен блокчейн

Частните блокчейни са централизирани и се управляват от лице или организация, която решава кой може да има достъп до блокчейна и да бъде добавен като възел. Транзакциите в частен блокчейн не са публично видими, а се проверяват чрез процес на консенсус между членовете на мрежата. Въпреки че функционалностите му са като на публична блокчейн мрежа, що се отнася до peer-to-peer свързаност и децентрализация, частният блокчейн има значително по-тесен обхват. От съображения за поверителност на данните, както и за споделяне в мрежа на корпоративно ниво, частният блокчейн е предпочитаният тип. Друг пример за неговото използване е B2B (бизнес към бизнес) обмен на виртуална валута, базиран на Hyperledger.

Предимства: Скорост, поверителност.

Недостатъци: Изграждането на доверие е по-трудно, проблем с мрежата може да ограничи достъпа на възлите до ключова функционалност.

Хибриден блокчейн

Хибридните блокчейни съчетават характеристиките както на публични, така и на частни блокчейн мрежи. Този тип блокчейн често се използва в бизнес приложения, където множество организации трябва да споделят данни сигурно. Хибридният блокчейн може да споделя определена информация публично, като същевременно запазва друга информация поверителна. Това позволява по-голяма сигурност и прозрачност, като същевременно се запазва известна степен на поверителност. Пример за това е управлението на веригата за доставки, където подизпълнителите могат лесно да се присъединят към частен/корпоративен блокчейн с множество публични блокчейни.

Предимства: Изграждане на екосистема, сигурност, поверителност.

Недостатъци: Сложна мрежа за изграждане и поддръжка.

Консорциумен Блокчейн

При този тип група компании или организации управляват процеса на предоставяне на разрешение за достъп до блокчейна. Те са по-децентрализирани от частния блокчейн, което осигурява по-голяма сигурност. Предварително дефинирани възли управляват процедурите за консенсус в консорциумен блокчейн. Този тип блокчейн има валидаторен възел, чиято основна функция е да инициира транзакция, да я получи и да я валидира. Участващите възли могат да изпращат или получават транзакции. Пример в тази категория е платформата Corda, използвана в областта на финансите и банковото дело.

Предимства: Скорост, изграждане на екосистема, поверителност.

Недостатъци: Сложност за изграждане и поддръжка на мрежата.

1.3. Популярни блокчейн платформи

Figure 9 Popular blockchain platforms

Ethereum е една от най-популярните и широко използвани блокчейн платформи. Тя е и първата платформа, която позволява на разработчиците да пишат нови приложения, които могат да бъдат конфигурирани и изпълнявани на нея. Създадена през 2015 г., тя въвежда и една от уникалните концепции на блокчейн, а именно интелигентните договори. Интелигентните договори (известни също като интелигентни договори) са вид програма, която съдържа команди и състояние/контекст. Всеки интелигентен договор работи на определен адрес на платформата. Това им позволява да изпращат транзакции и да имат баланс. Всички тези операции се извършват на виртуалната машина на Ethereum (EVM).

Разработчиците разработват и изпълняват децентрализирани приложения (dapps) на EVM. Това са цифрови приложения или програми, задвижвани от интелигентни договори, които работят на блокчейни, а не на централизирани сървъри. Те изглеждат и се усещат като обикновени мобилни и уеб приложения. Разликата обаче се състои в начина, по който работят, и техните ключови характеристики:

- dApps не е необходимо да се управляват от централен сървър. Това ги прави устойчиви на цензура и измами;
- dApps са с отворен код;
- Всички данни и записи, генерирани от dApps, се съхраняват в непроменлив, публичен блокчейн;

- dApps предоставят награди на валидаторите.

Интелигентните договори на Ethereum са написани на езика Solidity. Ethereum е без разрешение и е отворен за обществеността. Неговият механизъм за консенсус първоначално е proof-of-work, но по-късно е преминава към proof-of-stake. Ethereum има криптовалута, наречена Етер (Ether). Етер се използва за плащане, за създаване и иницииране на транзакции в блокчейна на Ethereum.

Hyperledger Fabric е блокчейн с разрешение, разработен от Hyperledger Hub (Linux Foundation) и е насочен към предприятия, които искат да използват, интегрират или изграждат решения и приложения, базирани на блокчейн. Hyperledger Fabric е подобен на Ethereum не само по отношение на вида DLT, но и по своята модулна архитектура. Тази модулност дава на Fabric вид конфигурируем интерфейс, където човек може да избере предпочитаните услуги, като например консенсусен алгоритъм, видове интелигентни договори и др. Интелигентните договори на Fabric могат да бъдат написани на Go, Java и JavaScript.

EOSIO е високопроизводителна блокчейн платформа с отворен код, стартирана през 2018 г. от Block.one. EOSIO предлага бърза, надеждна и високо сигурна платформа за изграждане на блокчейн приложения. EOSIO поддържа интелигентни договори, написани на езика за програмиране C++. Разработчиците избират платформата EOSIO за своите блокчейн проекти, защото тя е: бърза и ефективна, лесно конфигурируема, сигурна, съвместима и фокусирана върху разработчиците.

Corda е блокчейн платформа с отворен код, създадена от R3 Consortium през 2015 г. Corda първоначално е проектирана за финансови институции, но оттогава се е разширила, за да обслужва допълнителни области като здравеопазване, застраховане, цифрови активи и финанси.

▪ Corda е DLT с разрешение и поддържа функционалност за интелигентни договори. Интелигентните договори на Corda могат да бъдат написани на Java или Kotlin.

▪ Платформата няма функция за добив, така че някои транзакции никога не се виждат от повечето възли. С други думи, транзакциите на Corda не са отворени за всички възли. Corda има конфигурируем консенсус, което означава, че има много алгоритми за консенсус, от които да избирате.

▪ Консенсусът за валидност проверява дали транзакцията е приета от договорите на всяко

състояние и вход и дали транзакцията има всички необходими подписи.

▪ Уникалният консенсус съгласува стойността, ако входните данни за транзакцията са уникални и не са били използвани в други транзакции.

Quorum е блокчейн платформа с отворен код, базирана на Ethereum. Основана около 2016 г., тя е проектирана да обслужва финансовата индустрия и да позволява на предприятията да „използват Ethereum за своите блокчейн приложения с висока стойност“.

Quorum наскоро беше придобита от ConsenSys на JP Morgan. Много компании са я внедрили в бизнеса си, включително Microsoft, JP Morgan, Covantis, Южноафриканската резервна банка, SiaChain, Komgo и други.

Quorum е с разрешения, но също така позволява персонализиране въз основа на нуждите на клиентите. Освен това Quorum поддържа както публични, така и частни мрежи, както и интелигентни договори. Точно както в Ethereum, интелигентните договори в Quorum са написани на Solidity, което прави много лесно преминаването от Ethereum към Quorum. По-нататък в тази глава са дадени подробни сравнения между няколко платформи за интелигентни договори, за да се избере платформата, която е най-подходяща за решаване на специфични предизвикателства при разработването на приложения и която ще бъде основата за новите приложения на платформата за интелигентни договори.

1.4. Предимства и ключови характеристики на DLT

Благодарение на използването на p2p мрежи, криптографски функции и консенсусни алгоритми, DLT предоставя следните предимства:

- Децентрализация - информацията е винаги достъпна, защото всеки компютър в мрежата има копие на регистъра.
- Прозрачност - информацията за транзакциите се съхранява в публичното пространство. Тези данни не могат да бъдат променяни.
- Неограниченост - теоретично регистърът може да бъде допълван със записи до безкрайност.
- Достъпност - всеки има достъп и може да пише, разбира се, това е валидно за определени видове DLT.
- Надеждност - проверка на информацията чрез консенсус, както и невъзможност за промяната ѝ по всяко време след запис в регистъра.
- Сигурност - използват се надеждни криптографски механизми за валидиране и защита на

информацията.

- Информацията може да бъде анонимна или поименна - отново поради използваните криптографски функции (публичен-частен ключ).
- Автоматизация - благодарение на интелигентните договори изпълнението може да бъде автоматизирано, например, в случай на закъснение на полет, парично обезщетение може автоматично да се преведе на пътниците.
- Ефективност - поддържането на регистъра и превеждането на транзакциите не изисква високи инвестиции.
- Скорост – транзакциите се извършват мигновено в зависимост от избора на DLT.

Всички тези качества на DLT могат драстично да променят настоящите бизнес процеси, правейки ги по-ефективни, достъпни и надеждни. Промяната в някои бизнес сценарии може да бъде от огромен мащаб и да доведе до качествено ново преживяване за потребителите. Пример за това би бил процесът на регистрация на автомобил или вписване на имот в регистъра. Следващата глава разглежда приложенията на тези функции в някои от най-широко използваните бизнеси и услуги.

1.5. Приложимост на DLT в бизнеса

Поради ключовите си характеристики, блокчейн приложенията имат голям потенциал и вече се използват в много индустриални сектори [39-49]. Те осигуряват по-добро качество на продуктите, по-голяма удовлетвореност на потребителите, намаляват разходите, повишават прозрачността и справедливостта и подобряват пазарната ефективност. Блокчейн позволява ефективно съхранение на данни за транзакции, клиенти и доставчици в прозрачен, непроменлив онлайн регистър.

Блокчейн и DLT са успешно приложени на практика в много области като: вериги за доставки и логистика, здравеопазване, търговия на дребно и електронна търговия, финанси, недвижими имоти, медии, NFT пазари, тежка промишленост и производство, музика, трансгранични плащания, интернет на нещата, игри, поверителност, правителство и гласуване, реклама, създаване на оригинално съдържание, автомобилостроене.

Общ преглед на използваемостта на блокчейн в бизнеса е показан на Фигура 12.

Figure 12 Blockchain Applications

1.6. Избор на DLT платформа

За да изберем подходяща платформа, ще бъде направим подробно сравнение на два публични блокчейна: Ethereum и EOS и два корпоративни блокчейна: Hyperledger Fabric и R3 Corda.

Ethereum: Ethereum е първата блокчейн платформа, която поддържа интелигентни договори. В момента използва консенсусен механизъм за доказателство за залог (PoS). Средното време за създаване на блок е 12 секунди, а общата пропускателна способност е около 15 транзакции в секунда в световен мащаб. Ethereum съдържа абстракционен слой с вграден език за програмиране, пълен по Тюринг, което позволява на всеки да пише интелигентни договори и децентрализирани приложения, където може да създава свои собствени произволни правила, формати на транзакции и функции за преход на състояния. Езикът за интелигентни договори е Solidity, клонинг на Java script, проектиран специално за изпълнение на интелигентни договори на Ethereum. Отличителна черта на Ethereum е, че неговите интелигентни договори са непроменими по дизайн. Този подход е предназначен да гарантира, че цялата обработка на данни е с фиксирана цена от самото начало и не може да бъде променена в нечия полза по-късно. Съществуват методи като надграждащ се прокси модел, които позволяват актуализиране на логиката.

EOSIO/Antelope: EOSIO е блокчейн платформа от трето поколение, базирана на делегирано доказателство за дял (DPoS). В DPoS всеки притежател на EOS може да гласува за доверени производители на блокове. Ще бъдат избрани общо 21 производители, които ще отговарят за обработката на транзакциите чрез хеширането им в блокове. Блоковете ще се произвеждат точно на всеки 0,5 секунди и точно един производител е оторизиран да произвежда блок във всеки даден момент. Протоколът DPoS позволява на мрежата да обработва транзакции в рамките на секунди и без такси. Необходими са по-малко възли за проверка на транзакциите, така че блоковете могат да се произвеждат много по-често, без да се изисква много енергия за работата на мрежата. Обработката на транзакциите обаче консумира малко количество мрежови ресурси. Вместо да плащат, инициаторите на транзакции трябва да наемат ресурсите (по-специално CPU и NET), които искат да използват, като залагат EOS токени. Използването на ресурси ще се изчиства всеки ден и ресурсите, които вече не са необходими, могат да бъдат върнати по всяко време, за да си върнете EOS. Този модел за лизинг на ресурси елиминира таксите за транзакции, така че потребителите ще могат безплатно да прехвърлят токени и да използват всички видове dApps на EOS.

Hyperledger Fabric: Hyperledger Fabric [50-52] е част от общността с отворен код Hyperledger. Предоставя се от IBM и е под егидата на Linux Foundation и е проектиран специално за корпоративна употреба. Няма собствена криптовалута. Интелигентните договори на Fabric се наричат верижен код и обикновено се разработват на Golang. Верижният код на Fabric е единственият начин за достъп или промяна на данни в Hyperledger Fabric. Съществуват концепции за Ledger, State DB и Side DB. Например, достъпът до „леджера“ на Hyperledger Fabric дава достъп до всички транзакции, които са се случили в миналото, независимо от текущото състояние на включените обекти (като „изтрити“). Базата данни за състоянието се изгражда отново за всеки възел въз основа на информацията от Ledger и съдържа само текущото състояние на обектите и не включва обекти, които са зададени като „изтрити“. Side DB е хранилище за данни извън веригата, които все още могат да бъдат предавани и валидирани от Hyperledger Fabric, но не са част от неговите блокчейн структури. Технически, всеки Fabric канал е отделен блокчейн със собствен верижен код и потребители.

R3 Corda: Corda [53] е DLT без блокчейн, създаден от R3 Consortium предимно за използване във финансови институции. Той има подобрена мащабируемост в сравнение с всеки класически блокчейн благодарение на своята иновативна архитектура. За разлика от Hyperledger Fabric, консенсусът в Corda се постига на ниво транзакция (без блокове) и винаги включва взаимодействие с един или повече възли от така наречения нотариален клъстер, за да се гарантира уникалността на транзакцията. Транзакциите в Corda по подразбиране са видими само за участващите страни и има възможност за проследяване на пълната история на средствата при поискване. Интелигентните договори на Corda обикновено са написани на езика Kotlin. По дизайн интелигентните договори на Corda (както и интелигентните договори на Hyperledger Fabric) не са гарантирано детерминистични. Следователно, отговорност на разработчика на интелигентни договори е да избягва писането на вероятностни алгоритми, за да избегне сложни атаки срещу системата. За подобряване на процесите, Corda може да предложи най-добра мащабируемост под натоварване и конфигурируем консенсус, базиран на нотариален клъстер. Неговият модел на сигурност по отношение на видимостта на данните е най-сложен, така че е много по-труден за тестване и анализ. Като се има предвид производителността, когато е правилно конфигурирана, Corda може да бъде най-добрият избор за корпоративна DLT. Corda може да поддържа сложна система с много участници за процеси, работещи под високо натоварване.

Сравнение на DLT

Потребители решават да използват дадена система въз основа на ползата, която тя им носи, нейната използваемост, първоначалните разходи и разходите за поддръжка. Други водещи характеристики за избор на платформа са функционалност, производителност, надеждност, сигурност, мащабируемост. И накрая, размерът на екосистемата, която използва платформата, също е важен, дали тя се подобрява постоянно, дали са написани много нови функционалности и дали средата за писане на нови приложения е лесна и интуитивна за работа.

Сравнението между четирите DLT подчертава разликите, които вече съществуват между различните технологии. Използването на корпоративни DLT (HL Fabric и R3 Corda) изисква значителни разходи за инфраструктура, които да бъдат създадени и поддържани от участващите страни. Това включва разпределението на ресурси както за хардуер, така и за софтуер, както и персонал, отговорен за системните актуализации и промените в конфигурацията. Някои качества на услугите, като висока достъпност и възстановяване след бедствия, следване на най-добрите практики за сигурност и др., трябва да бъдат планирани и внедрени от всички участници. За организационно разпределена система тези разходи могат да бъдат значителни, ако се внедряват по начин, който не разчита на доверие в други участници в процеса.

Използването на публични DLT (Ethereum и EOSIO), от друга страна, гарантира доверие между всички участници, тъй като е базирано на публична p2p мрежа. Инфраструктурата на публичните DLT вече е създадена и поддържана от други страни, което дава предимство в цената и по-лесна поддръжка. DApps, работещи на публични DLT, могат да се консумират директно дори от мобилни устройства. Тези свойства на публичните DLT им дават решаващо предимство пред корпоративните DLT, когато става въпрос за обслужване на разпределена SDM система.

Общите разходи за управление на dApps на Ethereum и EOS се основават на доста различни модели. Ако се анализират всички разходи за всеки участник в процедурата, е очевидно, че използването на Ethereum непременно добавя ежедневни разходи, поради което потребителите продължават да плащат за използването на dApp, тъй като всяка стъпка от внедряването и особено използването на dApp струва определено количество газ. От друга страна, ежедневните разходи за използване на EOSIO dApps са до голяма степен възстановими. CPU и NET, използвани за осъществяване на повиквания към EOS

интелигентни договори, се възстановяват с течение на времето и дори ангажираните ресурси могат да бъдат намалени, ако вече не се използват напълно. Цената на RAM се заплаща за първоначалното внедряване на dApp и се използва за съхраняване на всички данни, събрани от dApp и неговия потребител. Ценовият модел на EOS е по-гъвкав в сравнение с Ethereum и позволява различни модели на разходи и оптимизации. Като допълнително предимство, времето за създаване на блок е значително по-кратко, което позволява по-бързо реагиращи приложения.

Изброените прилики и разлики, както и ключовите характеристики, са обобщени в Таблица 1.

	Ethereum	EOS (Mainnet)	HL Fabric	R3 Corda
Type of DLT	Public	Public	Permisioned	Permisioned
Consensus Type	Proof of Work	Delegated Proof of Stake	Configurable per channel	Notary service + UTXO
Smart Contract Type	Immutable	Mutable/Immutable/BP	Mutable	Mutable
Smart Contract Programming Language	Solidity	C++	Golang	Kotlin
Legal Binding Agreement	- - -	Ricardian Contracts	- - -	Ricardian Contracts
Deployment Cost for dApp Publisher/Operator	Gas price for deployment	Cost: RAM (code + data)	(Distributed) Infrastructure	(Distributed) Infrastructure
Maintenance Cost for dApp Publisher/Operator	- - -	Cost: RAM delta (+/-)	Maintain (Distributed) Infrastructure	Maintain (Distributed) Infrastructure
Motivation to run DLT	Miner's reward per block (inflation)	Block producers' reward (inflation)	Infrastructure maintained by involved parties	Infrastructure maintained by involved parties
End user joining	Free	~ Free minimum RAM, CPU, NET	Restricted	Restricted
End user costs	Gas cost per dApp call	Practically free / Replenishable resources	- - -	- - -
On-chain data visibility	All persistent dApp data is visible globally	All persistent dApp data is visible globally	Full visibility per Fabric channel	Only participants see transactions. Transaction proof may be shared.
Scalability	Limited due to PoW used	Improved due to DPoS and limited number of BPs	Each channel is separate blockchain	Excelent, Native sharding support
Consensuis	Proof of Work	Delegated Proof of Stake	Configurable per channel	Verify: Required signers Unique: Notary service
Security	Top 3 Mining pools control 64% of hashrate	Top 21 Block Producers votable each 63 sec.	Customizable per scenario	Notary service
Transactions per Second	About 15 transactions per second globally	Limited to 4000 TPS for Mainnet	Configurable per channel	N/A
Block producing time	~ 15 seconds	0.5 seconds	Configurable per channel	N/A

Table 1 Comparison between selected DLTs

През 2022 г. Ethereum официално премина към консенсусен механизъм Proof of Stake (PoS) като сигурен и енергийно ефективен начин за валидиране на транзакции и добавяне на нови блокове към блокчейна. Въз основа на анализа, като се вземат предвид всички

важни характеристики, EOSIO е по-подходящ избор на платформа за разработване на прототипи на разпределени приложения. Наред със скоростта, доверието, произтичащо от публичния тип, както и популярния език (C++), използван за писане на интелигентни договори, има друг водещ фактор за избора на EOSIO/Antelope/Vaulta, а именно удобната среда за писане на dApp приложения.

Глава 2. Стимулиране на изследванията, базирано на платформа за интелигентни договори

2.1. Въведение

В тази глава ще опишем децентрализирана система, базирана на публичен блокчейн, за стимулиране на измерими и доказуеми постижения в различни области на изследването.

Нека помислим за един практически пример от областта на медицинските изследвания: Сгъването на протеини е физически процес, чрез който протеиновата верига придобива своята естествена триизмерна структура. Първичната структура на протеина, като линейна аминокиселинна последователност, напълно описва съдържанието на протеина. Вторичната протеинова структура е първата стъпка от процеса на сгъване, за да може протеинът окончателно да се сгъне в своята естествена структура. Вторичната структура се състои от набори от алфа спирали, бета листове и връзки между тях. Крайната им еднопротеинова структура се достига, след като третичната структура фиксира вторичните структури в триизмерното пространство. Четвъртичната структура описва образуванията на вече сгънати протеини, сглобени в по-големи структури. Преминаването от детерминистичната първична структура до крайната триизмерна протеинова структура отнема от микросекунди и минимизира свободната енергия на Гиб на структурите. Тъй като пълната информация за протеина е низ от аминокиселини, намирането на естествената протеинова структура може да се определи като проблем с енергийната оптимизация (фиг.16). Когато имаме стабилен нискоенергиен разтвор, който не отговаря на очакванията ни и не съответства на наблюдаваната на практика структура, можем да предположим, че структурата на естествения протеин е различна.

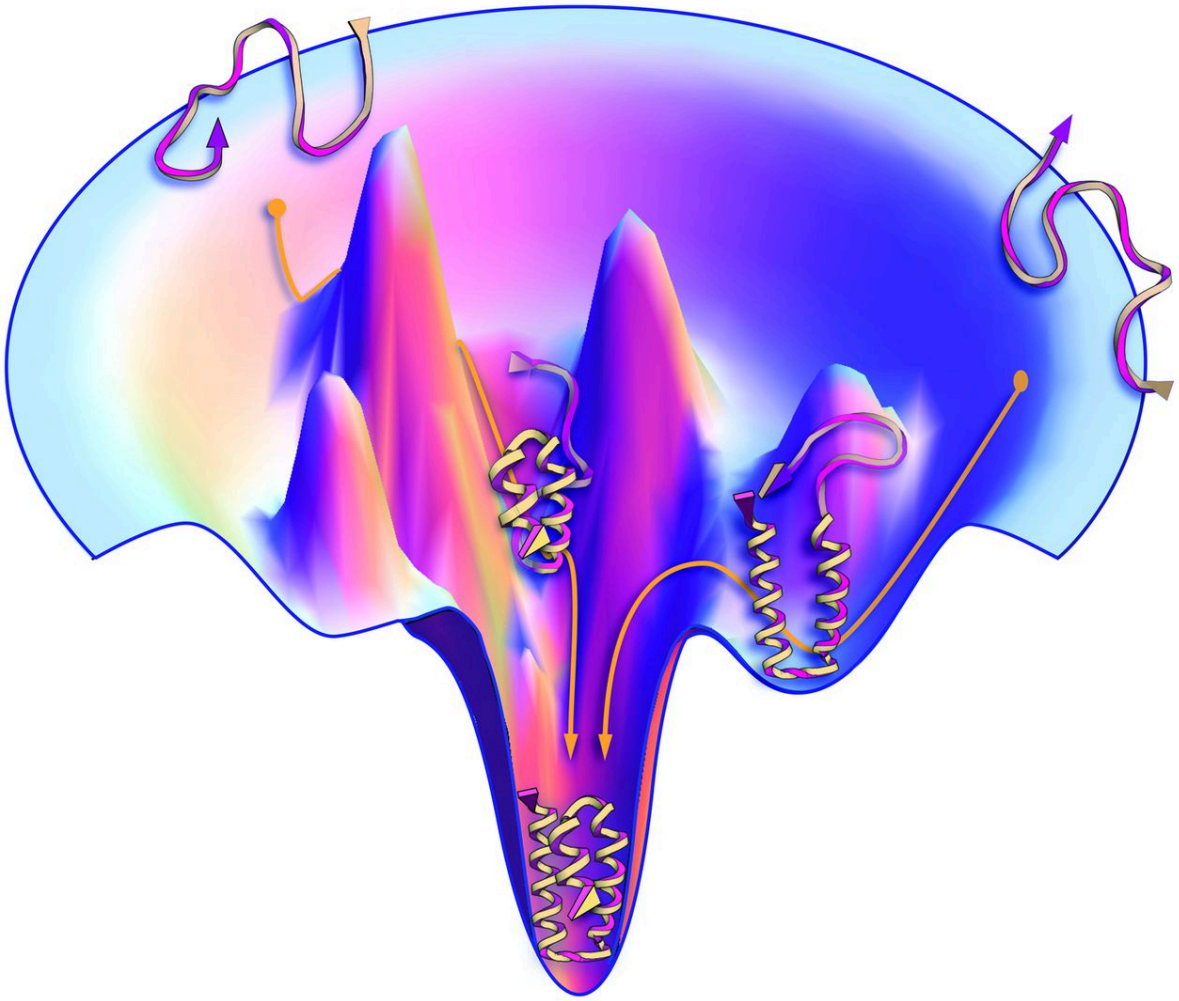

Figure 16 Optimizing Gibbs energy during protein folding

Задачата за търсене на съответстваща структура, която минимизира енергията на Гибс на протеина, може да бъде важна стъпка в изследването на различни протопатични заболявания като болестта на Алцхаймер, болестта на Паркинсон, амилоидоза и много други. Въпреки че това изчислително предизвикателство е лесно за формулиране, то е трудно за решаване и ефективността на предложените решения е лесна за сравнение въз основа на техните изчислени стойности на енергията на Гибс.

Класификация на задачите за стимулиране

Някои от типовете задачи са дадени в Таблица 2. Задачите, които са зададени за системата, могат да варират по определена продължителност – те могат да бъдат зададени в системата за неопределен интервал или да имат предварително определена продължителност. Задачите с неопределено време присвояват пълната си награда при първия достъп до решение, съответстващо на определените параметри, до системата. Задачите с ограничено време са по-гъвкави. Те могат да присвоят наградата на първото подходящо решение или могат да изчакат всички подадени заявки да се натрупат и да наградят само най-доброто след края на периода на състезание.

ID	Task Duration	Private results	Allow Contributors	Allow Cancelation	Typical tasks	Examples
1	Infinite	No	Yes	No*	Theoretical	Counterexample for a hypothesis
2	Infinite	No	Yes	Yes	Research	Protein folding (improvement)
3	Fixed	No	Yes	Yes	Research	Protein folding (initial), Space travel (public)
4	Fixed	No	Yes	No	Practical	Divisor of a big number (public)
5	Fixed	Yes	No	No*	Practical	Divisor of a big number (secret), Space travel

Table 2 Responsibilities and SLA

В някои случаи споделянето на резултатите от печелившото решение може да не е желателно поради причини, свързани със сигурността или финансови причини. Например, ако силата на ключ за сигурност се тества чрез възнаграждаване на евентуални успешни атаки, това може да не е желателно. Също така, сложна задача, като например план за космическо пътуване, може да доведе до отрицателни финансови последици, ако специфични параметри (дати на изстрелване, доставки) станат публични твърде рано. За този вид задачи подаването на решения трябва да е възможно във форма, в която само Доставчикът на награди може да прочете решението. Този подход ще изисква допълнително договаряне между доставчика на решението и Доставчика на награди. Един от ефектите на това усложнение е, че тези сценарии не трябва да позволяват допълнителни вноски с награди, тъй като никой Доставчик на награди няма да има достъп до печелившото решение поради неговия частен характер.

Един много важен аспект от жизнения цикъл на задачата е ситуацията, когато не се печели награда. Това се случва, когато задачата е анулирана или достигне края на активния си период, без да бъде подадено валидно решение. В този случай натрупаната награда трябва да бъде върната на *Доставчика на награди* и на всички *Подпомагащи наградите*.

2.2. Архитектура на системата

Предлаганата система (фиг. 17) се състои от няколко основни елемента, които ще я осигурят за работа. За прототипа избрахме EOSIO като публична блокчейн технология.

Управлението на потребителите е ключов модул, който следи блокчейн акаунти, представляващи участници във веригата, и техните връзки с поддържаните рамки за задачи, задачи, награди и подадени решения. В много случаи има опция за акаунт, който все още не е известен на системата, за изпълнение на операции. Например, това може да е анонимен участник в задача или

изследовател, чието първо взаимодействие със системата е получаване на награда за намиране на решение на един от дефинираните проблеми. В тези случаи не се изисква регистрация на потребител, за да се използва системата, но блокчейн акаунтът ще бъде добавен към данните за управление на потребителите след взаимодействието, независимо дали е успешно или не. Сътрудничеството във веригата е опция за няколко лица или организации да определят ясни граници на наградите, като дефинират как ще се разпределят наградите при успех. Сътрудничеството във веригата е изцяло незадължителна функция, чието предназначение е най-вече да споделя видимостта на участниците за постижението. Ако става въпрос само за парично възнаграждение, това може да се постигне изцяло извън веригата, стига партньорите да си доверяват взаимно за това.

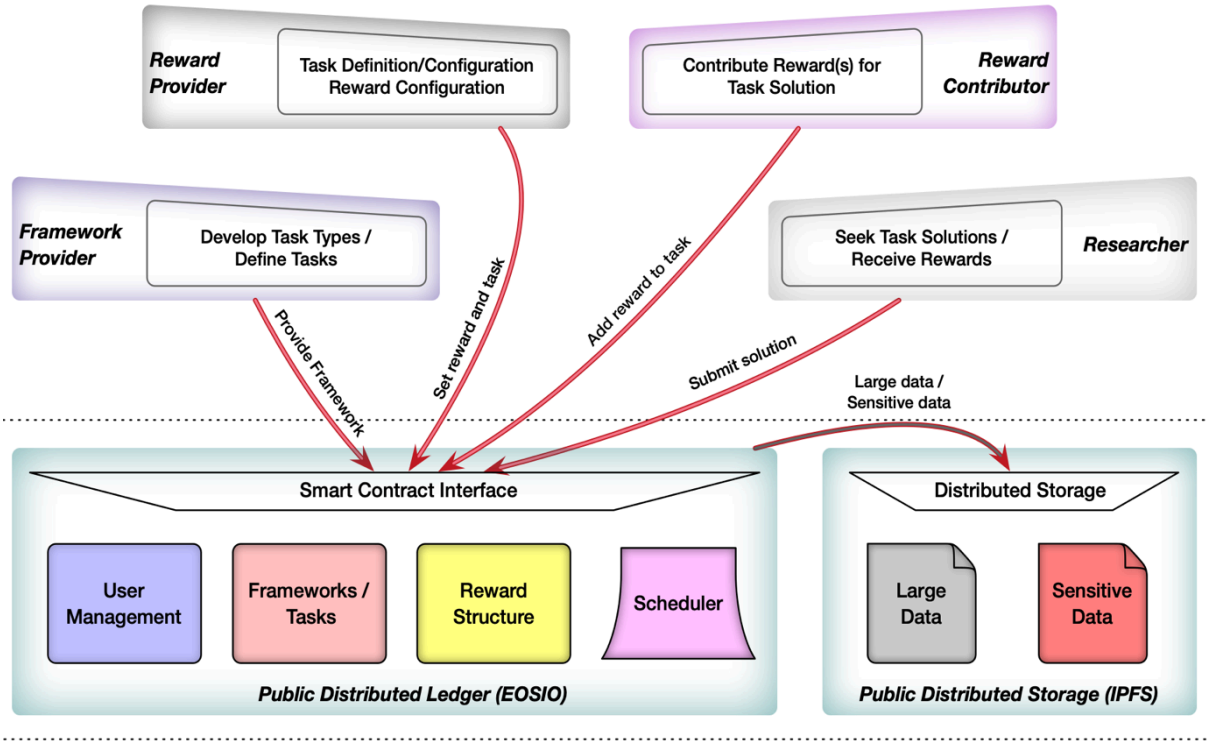

Figure 17 Main actors and interactions for the system

Рамките за задачи са набор от публични блокчейн компоненти, които са отворени за принос от разработчици.

Основните части за принос са компонентите за валидиране и интерфейсите за задачи.

Компонентите за валидиране се предоставят и поддържат от доставчиците на рамки. Важно е те да са стабилни и без грешки, тъй като могат да се използват за дълги периоди от време. Всякакви промени в интерфейса им трябва да са до голяма степен обратно съвместими. Силно препоръчително е поддържаните рамки за задачи да са с отворен код и да могат да бъдат валидирани от всеки, който участва.

Интерфейсите за задачи описват техническите параметри, зададени от доставчиците на награди,

както и формата, в която се получават решенията. Периодът, за който се предлага наградата за намиране на решение, е ключов параметър за такава задача. Друг параметър е видът на състезанието. В някои случаи първото валидирано решение може веднага да получи наградата. В други случаи проблемът може да има много решения и първото представено решение може по-късно да бъде подобрено от други предложения. В този случай наградите се дават на най-доброто решение, представено в конфигурирания период, ако има такова.
Структурата на наградите е набор от данни, който следи предлаганите награди за решения на специфични изчислителни проблеми и допълнителни конфигурационни данни. Единична награда може да бъде просто съотношение едно към едно между сумата токени, предложена за решение на проблема. Те могат да имат и сложна структура, при която една сума токени може да бъде присвоена за пробив в различни проблеми. Също така, за всеки проблем различни участници могат да присвоят различно конфигурирани награди. Оригинално ограничение е, че периодът за активни вторични награди (зададени от участниците в задачите, които не са оригиналният доставчик на задачите) не трябва да удължава периода на оригиналната награда за задачата.
Видът награда е ключов параметър за системата, който трябва да се вземе предвид.

- Всеки голям публичен блокчейн предлага токени като криптовалута по подразбиране. Естествено е наградите да се предлагат и събират в собствената валута на блокчейна.

- Гъвкавостта на съвременните публични блокчейни позволява на всяко dApp да предлага и управлява собствен токен. Решение със собствена валута може да се използва в допълнение към финансирането на изграждането и експлоатацията на такава система.

- Друг подход е да се зададе награда в конкретна стейбълкойн, която е от другата страна на скалата. Неговите награди са независими от колебанията на блокчейн валутата.

- Най-сложният подход е да не се фиксира един единствен токен за награда, а да се позволи няколко токена да бъдат валидни награди.

Целта за награда може да бъде дефинирана толкова гъвкаво, колкото позволява системата. Всяка сума на наградата може да бъде зададена за решаване на която и да е от предварително дефиниран набор от задачи.
Компонентът **Планировчик** (Scheduler) гарантира, че наградите могат да бъдат получени след предварително определен период. Неговата отговорност е да изчислява и сравнява подадените задачи в края на конфигурирания период. В конкретния случай, когато няма подадени валидни решения, наградите трябва да бъдат върнати на *доставчика на задачите* и на *сътрудниците на задачите*.

Глава 3. DLT-базирана система за управление на SDM процеси

Глава 1 описва как блокчейн, със своите характеристики като сигурност, прозрачност и надеждност, може да трансформира традиционния бизнес и да предложи качествено нова архитектура и опростени процеси за крайния потребител. И докато много разработчици в момента са фокусирани върху трансформирането на настоящия си бизнес, има една ИТ област, която също би могла да се възползва от блокчейн, а именно управлението на жизнения цикъл на разработката на софтуер. В SDLC повечето предизвикателства възникват във фазата на внедряване, конфигуриране, актуализиране и поддръжка на софтуера при крайния клиент (System Deployment and Maintenance - SDM). Именно в тази фаза използването на блокчейн би решило типичните проблеми, съпътстващи първоначалната инсталация и конфигуриране на софтуера в продуктивна среда.

3.1 Типични сценарии на SDM

Този раздел разглежда ИТ сценарий, близък до реална бизнес система. Той се състои от различни софтуерни продукти, работещи на локални сървъри, в облачна среда и интегрирани IoT устройства. Типичните участници, отговорни за внедряването на такава сложна система, са:

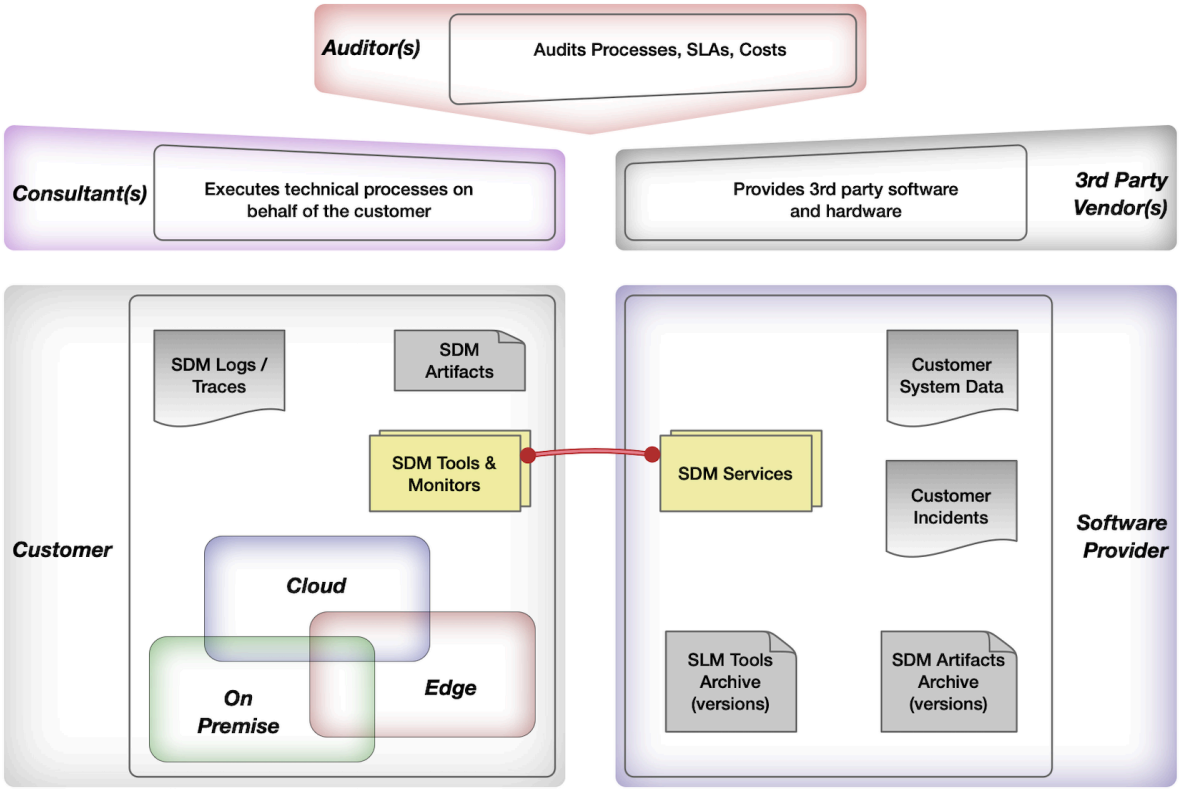

Figure 19 SDM environment and participants

3.4 Архитектура на SDM системата, базирана на DLT

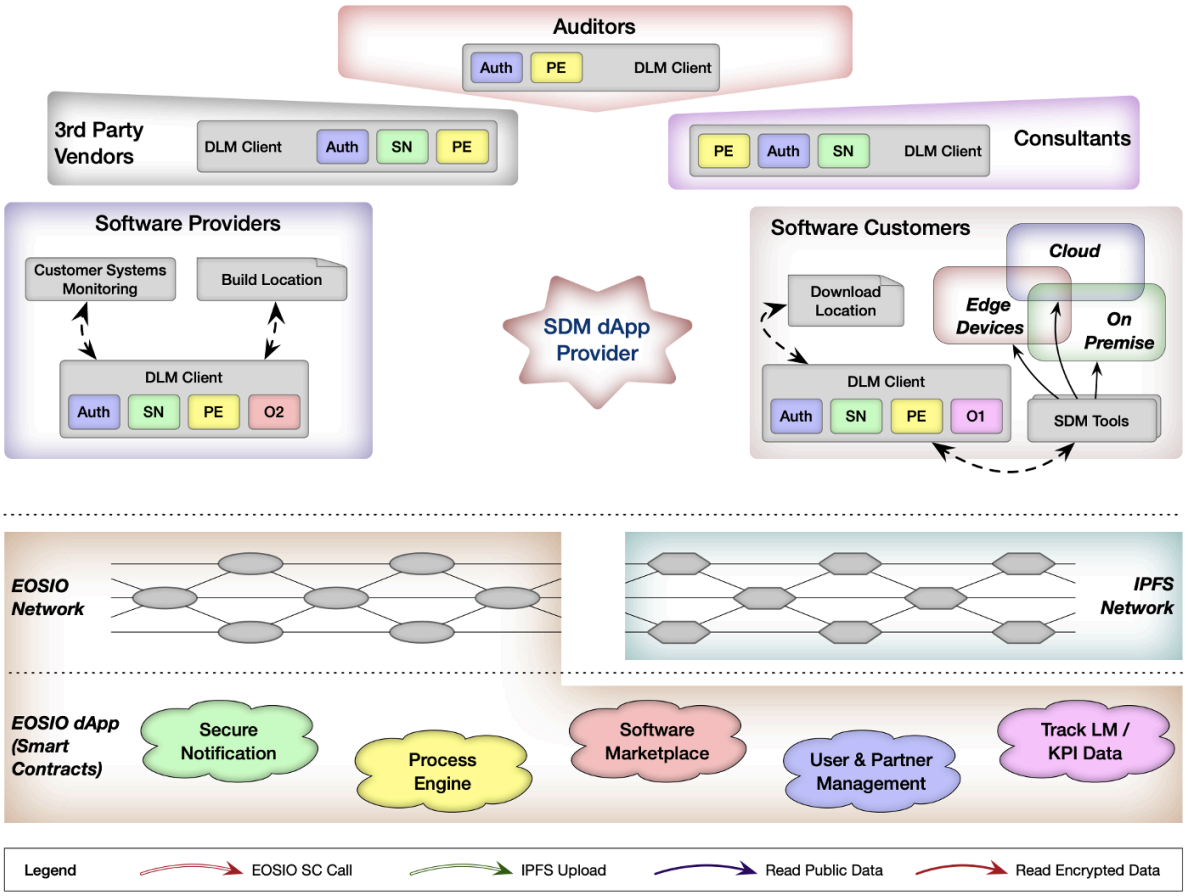

Figure 25 SDM system architecture

Основните елементи на системата са публична EOSIO блокчейн мрежа, разпределена система за съхранение на файлове IPFS, едно dApp, публикувано в EOSIO и използващо указатели към файлове, съхранявани в IPFS. Всеки участник в разпределения SDM процес използва един или повече локално инсталирани клиенти/агенти за Distributed Lifecycle Management (DLM), за да комуникира с блокчейна/dApp, и тази комуникация в повечето случаи ще достигне и до другите участници в SDM процеса и/или базата данни (IPFS).

Архитектурата е базирана на пет интелигентни договора [56,57], които могат да бъдат дефинирани като модули: модул за управление на потребители (User and Partner Management), модул за управление на процеси (Process Engine), модул, осигуряващ сигурна комуникация (Secure Notification), модул за софтуерен пазар (Software Marketplace) и модул, съдържащ данни от клиента за проследяване на LM/KPI данни (Track LM/KPI Data). Тези модули са част от dApp.

Ролята на локалните разпределени агенти (DLM) е да предоставят възможност на клиентите да удостоверяват и използват интелигентните договори на SDM dApp, да

прикачват ресурси под формата на файлове към IPFS. Данните, които DLM записва в EOSIO или IPFS, не са криптирани, но ако е необходимо, за да се запази сигурността на данните, те ще бъдат криптирани с помощта на публичните ключове на страните в процеса, които имат право да четат данните.

Чрез петте интелигентни договора и благодарение на ключовите характеристики на EOSIO, всички стъпки на SDM се реализират по сигурен и надежден начин. Начин, който осигурява качествена услуга с ясни отговорности, предвидимост на поведението, описание и автоматизация на добрите практики и надеждно съхранение на (историческа) информация. Следващата глава демонстрира на практика как модулите взаимодействат и как се реализира един от ключовите SDM сценарии.

Глава 4. Публично проверим генератор на случайни числа – използване и прототип

Многобройни съвременни ИТ системи зависят от правилното създаване на сигурни случайни и псевдослучайни числа. Критично предизвикателство в този процес е гарантирането, че външни субекти могат независимо да проверят целостта на тези стойности, предпазвайки се от потенциална манипулация от която и да е участваща страна. Платформите за интелигентни договори, задвижвани от блокчейн, които са получили широко разпространение в различни индустрии, предлагат обещаващо решение, като позволяват генерирането на случайни числа с пълна публична проверимост. Един ключов аспект за подобряване на надеждността и сигурността на генерираните числа е чрез добавяне на ентропия, допринесена от потребителя.

4.1. Генериране на случайни и псевдослучайни числа

Генерирането на сигурни случайни и псевдослучайни числа играе фундаментална роля в съвременните информационни системи и формира критична основа на съвременната инфраструктура за сигурност. Отвъд дигиталната област, множество приложения, несвързани с ИТ, в различни сектори също зависят силно от висококачествена случайност, за да поддържат справедливи, безпристрастни и статистически валидни процеси. Някои примери включват:

- **Избор на съдии и/или съдебни заседатели**: Правните системи използват генериране на случайни числа, за да избират безпристрастно съдебни заседатели от набор от допустими кандидати, като по този начин гарантират обективност в съдебния процес.
- **Лотарии и хазарт**: Случайността е от съществено значение в хазартните и лотарийните системи, за да се гарантира справедливост, непредсказуемост и устойчивост на манипулации.

- **Статистическо вземане на проби**: В дисциплини като социални науки, икономика и маркетинг, случайното вземане на проби гарантира, че данните, събрани от популациите, са представителни и безпристрастни, което повишава валидността на статистическите заключения.
- **Рандомизирани клинични изпитвания**: В биомедицинските изследвания, случайното разпределение на участниците в групи за лечение и контрол е жизненоважно за елиминиране на пристрастията при подбора и гарантиране на надеждността на резултатите от изпитванията.
- **Случайни инспекции**: Протоколите за осигуряване на качеството в производството често използват методи за случайно вземане на проби за избор на продукти за инспекция, като по този начин осигуряват справедлива оценка и намаляват систематичните пристрастия.
- **Рандомизиран ред на представяне**: В академична и професионална среда, рандомизацията на реда на представяне помага за смекчаване на възприеманото фаворизиране и запазва процедурния неутралитет.
- **Случайно тестване за наркотици**: За да насърчат справедливостта и възпиращото действие, организациите прилагат случаен подбор при провеждането на тестове за наркотици, предотвратявайки целенасоченото им насочване и осигурявайки равна вероятност за подбор.

Във всички тези приложения, качеството на процеса е силно зависимо от качеството на използваните случайни числа. Високата ентропия, безпристрастната случайност минимизира системните пристрастия и повишава надеждността, като гарантира, че резултатите не са обект на прогнозиране или външно влияние. Следователно, надеждното генериране на случайни числа е в основата на обективността и справедливостта както в цифровите, така и в реалните системи.

4.2. Сигурно използване на Blockhash като част от RNG seed-а

Използването на блокчейн технологията за генериране на публично проверими случайни числа предлага прозрачен, защитен от неправомерно използване механизъм, който насърчава доверието и целостта в системи, изискващи безпристрастна случайност.

Предложеният метод включва използването на EOSIO блок-хешове, които са криптографски хешове, получени от заглавката на блок. Заглавката на всеки блок съдържа хеша на предходния блок, създавайки сигурна верига от блок-хешове, която гарантира непроменимостта на блокчейна, предотвратявайки ретроактивни промени.

RNG процедурата се състои от три отделни фази:

1. Подготовка (по избор, онлайн или офлайн): Тази фаза може да се извърши офлайн, онлайн или

чрез комбинация от двете. Например, списък с потенциални съдии за дадено дело може да бъде цифрово подписан и подготвен офлайн. Този файл може да бъде качен в публично достъпно хранилище за прозрачност. Независимо от неговата наличност, цифровият подпис трябва да бъде включен във фазата на инициализация, за да се гарантира автентичността на процеса на подбор. Ако ангажиментите за хеширане са част от процедурата на случай на случай, всички ангажирани хешове трябва да бъдат качени или посочени в блокчейна преди фазата на инициализация, за да се гарантира, че са отчетени.

2. Инициализация (онлайн): Тази стъпка отбелязва началото на процеса на подбор или случай на случай и изисква взаимодействие с блокчейна EOSIO. Трябва да включва следните компоненти:

- Авторизация на инициращата страна

- Препратки към всички ангажименти за хеширане, използвани при изчисляването на началните числа на случайния генератор (RNG)
- Препратки към всички съответни офлайн данни, които идентифицират избраните обекти, без да се компрометира чувствителна или лична информация (напр. чрез използване на разпределени файлови системи като IPFS)
- Подписи на документи, свързани с процеса на подбор (съхранявани офлайн или на централизирана/разпределена файлова система)
- Информация за вида, количеството и предназначението на случайните данни
- Подробности за използвания алгоритъм на случайния генератор, включително всички ограничения

3. Последваща обработка (по избор, офлайн или онлайн): Последващата обработка не е задължителна, ако не е включен ангажимент за хеширане. Полезността на онлайн последващата обработка зависи от използвания метод за подбор. Методите, базирани единствено на блокови хешове като начални числа, обикновено не изискват последваща обработка. Обобщаването на резултатите от RNG в тази фаза обаче повишава прозрачността и улеснява проверката. Ако са включени ангажименти за хеширане, последващата обработка включва своевременно разкриване на предварително генерирани случайни числа (съвпадащи с извършените хешове), за да се финализира изчислението на случайните числа.

4.4 Методи за избор на семената (seed), използващи блокчейнови хешове

Предложеният метод включва използването на EOSIO блокови хешове, които са криптографски хешове, получени от заглавката на блок. Заглавката на всеки блок съдържа хеша на предходния блок; съществуват няколко метода за избор на начално число (seed) за случайни числа (RNG) въз основа на EOSIO блокови хешове: Използване на текущ/следващ блокхеш, използване на блокхеш с

фиксирано закъснение, използване на блокхеш със случайно закъснение, използване на блокхеш за събиране на случайност по време на закъснение, използване на блокхеш и хеш-ангажимент.

Сравнително обобщение на сложността, скоростта и сигурността на всички методи, обсъдени в тази глава, е представено в Таблица 3.

Seed Choosing Method	Complexity	Speed	Security: Mid Stakes	Security: High Stakes
Blockhash: Next Block	Low	Instant	High	Low
Blockhash: Fixed Delay	Low	Fast	High	Low
Blockhash: Random Delay	Low	Fast	High	Medium
Blockhash: Collect Entropy	Medium	Fast	High	Medium
Blockhash + User Entropy	High	Slow	High	High

Table 3 Comparison of seed selection methods

4.5 RNG прототип на EOSIO/Antelope

За целите на тази работа, прототипът за доказуемо генериране на случайни числа е внедрен във Vaulta, но техническите основи произлизат директно от споделената линия EOSIO/ Antelope.

4.6 Гранични условия за прототипа

Съществуват различни аспекти за практическото използване на дистрибуторско приложение, базирано на DLT. Някои от най-важните параметри са цената (TCO), скоростта, надеждността и прозрачността.

1. **Цена** за използване на предложеното доказуемо решение за случайни числа (RNG). Всички разпределени приложения изразходват ресурси за съхранение на данни и за използване на DLT като платформа за интелигентни договори. Четенето на данни от DLT обикновено е безплатна операция. За да бъде устойчиво, всяко решение ще се опита да минимизира разходите за съхранение и операции с DLT, като същевременно постига целите си. Един от начините за поддържане на ниски разходи е да се преместят колкото се може повече от операциите му офлайн. Прототипът е проектиран да покрива само абсолютния минимум от операциите, необходими за генериране на доказуеми случайни числа. Стъпките за подготовка и последваща обработка, както е описано в раздел 4.3, са напълно офлайн, така че не се добавят към онлайн разходите за използване на DLT. Единствената стъпка, която трябва да бъде онлайн – инициализацията на RNG, е реализирана в метод „rngstart“, който може да се използва за всеки от първите 4 метода, описани в раздел 4.4.

2. **Скоростта** обикновено не е определящ фактор за качеството на случайния генератор (RNG), но не би трябвало да отнема твърде много време за обработка. Четирите метода, които прототипът поддържа, генерират случайни данни почти мигновено - по-малко от секунда за първия метод до няколко минути за последния и най-сигурен метод.

3. **Надеждността** е важно качество на случайния генератор, използван в случаи с висок залог. Тук предимството на блокчейн/DLT е голямо предимство, тъй като тяхното свойство „разпределен“ гарантира, че няма единични точки на отказ.

4. **Прозрачността** е друга силна страна на повечето приложения, базирани на блокчейн/DLT. Използваните данни за RNG са видими за всеки. Пълните данни, използвани по време на процеса на RNG, могат да бъдат валидирани анонимно и безплатно. Този аспект позволява на множество страни да ги валидират независимо и да гарантират тяхната коректност.

4.7 Описание и работа на прототипа

Прототипът е реализиран за блокчейна Vaulta, използвайки Vaulta Web IDE. Името на интелигентния договор е get_random, а основната му входна точка е действието rngstart.

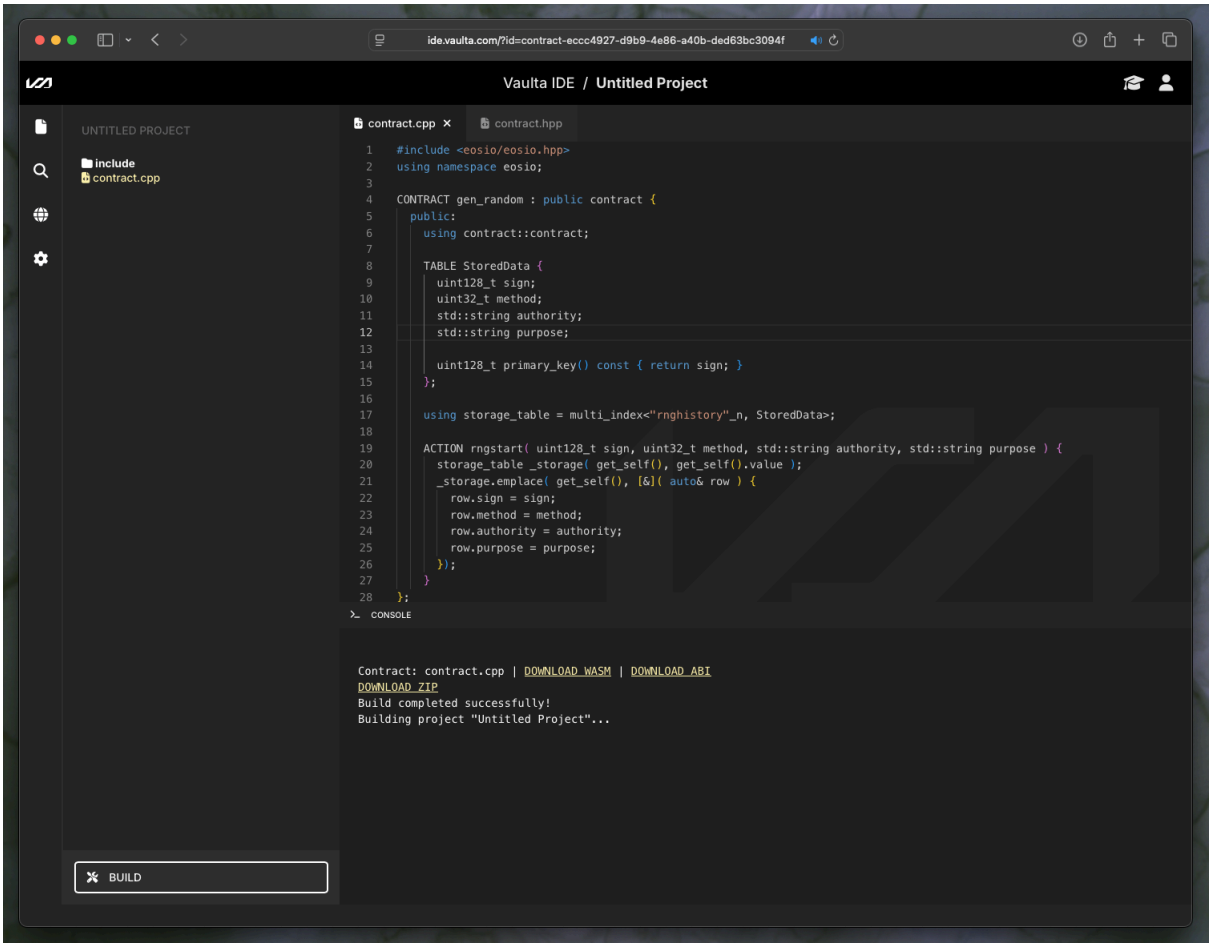

Figure 40 Initial state of the prototype

Действието rngstart има няколко параметъра в имплементирания прототип (Фиг. 40):

- **sign** (uint128_t) – Това е единственият задължителен параметър и служи като основен

идентификатор за всеки екземпляр на генериране на случайност. Криптографският дайджест/подпис на документа извън веригата определя целта на избора и входните данни. Той може да съдържа и друга релевантна информация за процеса на избор. Тъй като този документ може да съдържа лични данни, предмет на разпоредби (напр. GDPR), не се записват лични данни във веригата, а се съхранява само подписът на документа. Следователно, за генериране на случайност знакът се използва като идентификатор, който (i) делегира всички описателни детайли на посочения документ и (ii) предоставя гаранция за автентичност/цялостност за страните, които имат достъп до този документ.

- **method** (uint32_t) – Този параметър описва метода, използван за избор на блокчейн или блокчейнове, които се използват като начално число за генериране на случайно число. Ако методът не трябва да се споделя, той може да бъде описан в документа, който е идентифициран със знак.
- **authority** (std::string) – описание на организацията, която изпълнява процеса на генериране на случайни числа. Това е незадължително свойство, което може да се използва за филтриране на процесите, но не е задължително, когато организацията не е необходимо да оставя следи в публичното пространство.
- **purpose** (std::string) – подобно на параметъра authority, purpose е незадължителен параметър, който може допълнително да опише процеса в рамките на структурата на авторитетите, използваща резултата от генерирането на случайни числа.

Използване на прототипа.

Първата стъпка след внедряването на прототипа е тестването му. На Фигура 41 виждаме във Vaulta Wen IDE опцията за внедряване на договора върху реална тестова блокчейн мрежа. В нашия случай избираме „Jungle Testnet“ като една от оригиналните и най-популярни тестови блокчейни на EOS/Vaulta. За внедряването на прототипа използваме акаунт в Jungle Testnet - „dkhsyqa1lmvn“. Както можем да видим от лявата страна на Фигура 41, след като успешно изградим и внедрим интелигентния договор в Jungle Testnet, имаме създадена таблица rnghistory, за да съхраняваме резултатите от всички изпълнения на генерирането на случайни числа.

В резултат на тестването на прототипа можем да заключим, че той работи и правилно генерира доказуемо случайни числа, използвайки блокчейна като начален код за генератора на случайни числа.

По този начин потвърждаваме, че използването на прототипа показва, че блокчейн технологията EOSIO е подходяща за създаване на разпределени приложения, които използват предимствата, предоставени от използването на блокчейна като платформа за интелигентни договори. Такова приложение може да бъде много малко и ефективно, като същевременно използва предимствата, предоставени от технологията EOSIO/Antelope по дизайн.

Глава 5. Апробации и доклади на научни форуми

5.1. Апробация в научни форуми

Резултатите от дисертацията са публикувани в следните статии:

1. Jeliazkov J., Kostadinov H., Using EOSIO Technology for Publicly Verifiable Randomness, Studies in Computational Intelligence, Vol. 641, pp. 87 – 96, 2025, Springer, Scopus, SJR: 0.190
2. Jeliazkov J., Kostadinov H., Decentralized Research Incentivization System, Studies in Computational Intelligence, Vol. 641, pp. 97 – 103, 2025, Springer, Scopus, SJR: 0.190

5.2. Доклади на научни форуми

1. Jeliazkov J., Kostadinov H., Incentivizing Research Using DLT-based Smart Contract Platforms, Annual Meeting of the Bulgarian Section of SIAM, 17 - 19.12.2019г.
2. Jeliazkov J., Kostadinov H., Generation of secure public-verifiable random numbers, Annual Meeting of the Bulgarian Section of SIAM, 20 - 22.12.2022г.

Глава 6. Заключение

6.1. Научен принос на дисертацията

1. Извършен е анализ на съществуващи решения за платформи за интелигентни договори, базирани на блокчейн технология и технологии за разпределен регистър (DLT).

2. Разгледани са най-популярните съвременни технологии за разпределено съхранение, заедно с техните предимства и слабости, когато се разглеждат като основа за платформа за интелигентни договори. EOSIO е избрана като платформа за последващите приложения.

3. Описана е разпределена система за стимулиране на научноизследователската и развойна дейност, в която се определят награди за намиране на уникалното или най-доброто решение на даден проблем.

4. Описана и анализирана е разпределена система за управление на жизнения цикъл на корпоративен софтуер, използваща технологията EOSIO като платформа за интелигентни договори.

5. Описана е разпределена система, използваща набор от алгоритми за генериране на проверими случайни числа, изградена върху платформа за интелигентни договори, базирана на EOSIO като базов блокчейн.

6. Представен е прототип, работещ с технологията Vaulta/EOSIO за генериране на доказуеми случайни числа, базиран на иновативната архитектура, и е описана подробно средата, в която работи: интерфейси, интелигентни договори, модели на данни и комуникационни протоколи.

7. Обобщени са резултатите от разработването на новите системи, базирани на платформи за интелигентни договори, и са проведени анализи за различните сценарии, успешно решени от иновативната архитектура. Демонстрирани са предимствата, особено в областите на проследимостта, сигурността и дефинирането на отговорностите.

Разпределената система за стимулиране на научните изследвания и разработки, базирана на технологията EOSIO, е описана в Глава 2. Дефинирана е подробна блокчейн архитектура, която решава проблемите на дефинирането и стимулирането на намирането на конкретни научни резултати. Резултатите от това изследване са публикувани в: Jeliazkov J., Kostadinov H., Decentralized Research Incentivization System, Studies in Computational Intelligence.

Архитектурата за генериране на доказуемо случайни числа, описана с нейните модули, комуникационни протоколи и връзки между различните разпределени модули, е проверена и тествана с прототипа, описан в Глава 4. Описана е и връзката между блокчейн и IPFS като хранилище за документа, използван за дефиниране на алгоритми и граници за генериране на доказуемо случайни числа. Сериозно внимание е обърнато и на средата за разработка и начина, по който децентрализираните приложения (DAPP) са написани в EOSIO. Резултатите от архитектурния дизайн и анализ са публикувани в Jeliazkov J., Kostadinov H., Using EOSIO Technology for Publicly Verifiable Randomness, Studies in Computational Intelligence.

6.2. Обобщение

Историята показва, че при внедряването на иновации, научните институции винаги са играли водеща роля, чиято функция е да изследват, анализират и съдействат за изясняване на приложимостта на новата тема в реалния живот. Както и че всяко изследване, независимо от обема и обхвата му, е стъпка напред в посока на приложимост, за да се

улесни използването на по-добри и по-ефективни процеси и услуги от страна на хората и бизнеса.

Ето защо бих искал да благодаря на Института по информационни и комуникационни технологии към Българската академия на науките за възможността да бъда част от техния талантлив екип и да направя скромния си принос за утвърждаването на блокчейн като нов висококачествен стандарт в революционизирането на класическите бизнес процеси.

Специални благодарности и на моя колега Бисер Цветков за ползотворното време, прекарано заедно в дискусии и генериране на идеи. Очаквам с нетърпение да продължат работата си по темата и скоро да представят актуализирани разработки.

Накрая бих искал да благодаря на моя научен ръководител Христо Костадинов за неуморната му подкрепа по време на следването ми, за безценните му насоки относно етапите на осъществяване на научна дейност, за помощта му при определянето на цели и демонстрирането на резултати, както и за начина на публикуване на доклади и статии.

Библиография

1. Imran Bashir (2018), “Mastering blockchain: distributed ledgers, decentralization and smart contracts explained”, Packt Publishing; 2nd Revised edition

2. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

3. Paul A. Tatro (2018) “Blockchain Unchained: The Illustrated Guide to Understanding Blockchain”, Book Counselor LLC

4. Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., Vines, J. “Making sense of blockchain applications: a typology for HCI.” In: CHI 2018. ACM (2018)

5. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, ‘‘Blockchain challenges and opportunities: A survey,’’ Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018

6. Basit Shahzad, Jon Crowcroft, “Trustworthy Electronic Voting Using Adjusted Blockchain Technology.”, IEEE Access 7: 24477-24488

7. Bhardwaj, S., Kaushik, M. “Blockchain—technology to drive the future.” In: Satapathy, S.C., Bhateja, V., Das, S. (eds.) Smart Computing and Informatics. SIST, vol. 78, pp. 263–271. Springer, Singapore (2018).

8. Suhaliana bt Abd Halim, N., Rahman, M.A., Azad, S., Kabir, M.N.” Blockchain security hole: issues and solutions.” In: Saeed, F., Gazem, N., Patnaik, S., Saed Balaid, A.S., Mohammed, F. (eds.) IRICT 2017. LNDECT, vol. 5, pp. 739–746. Springer, Cham (2018).

9. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture consensus and future trends", Proc. IEEE Int. Congr. Big Data (BigData Congr.), pp. 557-564, Jun. 2017.

10. Daniel Drescher (2017) “Blockchain Basics A Non-Technical Introduction in 25 Steps”, ISBN: 978-1-4842-2604-9

11. UNITED STATES NUCLEAR REGULATORY COMMISSION (2002), “System Development and LifeCycle Management (SDLCM) Methodology”, Handbook, Version 2.3

12. R. Turpin, “A progressive software development lifecycle”, Proceedings of ICECCS '96: 2nd IEEE International Conference on Engineering of Complex Computer Systems

13 Gagan Gurung, Rahul Shah, Dhiraj Prasad Jaiswal, “Software Development Life Cycle Models-A Comparative Study”, International Journal of Scientific Research in Computer Science Engineering and Information Technology

14. Shylesh S. (2017), “A Study of Software Development Life Cycle Process Models.” SSRN Electronic Journal

15. Andreas M. Antonopoulos “Mastering Bitcoin”, 2nd Edition, Publisher(s): O'Reilly Media, Inc.

16. Sudhan, A., & Nene, M. J. (2018). “Peer Selection Techniques for Enhanced Transaction Propagation in Bitcoin Peer-to-Peer Network”, 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)

17. Matthew Underhill, “The Bitcoin Book: A Beginner's Guide to the Future of Finance”, Independently published (September 21, 2020)

18. Zhu, F., Chen, W., Wang, Y., Lin, P., Li, T., Cao, X., & Yuan, L. (2017). “Trust your wallet: A new online wallet architecture for Bitcoin”, 2017 International Conference on Progress in Informatics and Computing (PIC).

19. D. Larimer, EOS.IO Technical White Paper

20. EOSIO resource, https://eos.io

21. Zheng, W., Zheng, Z., Dai, H.-N., Chen, X., & Zheng, P. (2021). “XBlock-EOS: Extracting and exploring blockchain data from EOSIO”, Information Processing & Management, 58(3), 102477.

22. IPFS resource, https://ipsf.io

23. Jianjun, S., Ming, L., & Jingang, M. (2020), “Research and application of data sharing platform integrating Ethereum and IPFs Technology”, 2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES).

24. Guidi, B., Michienzi, A., & Ricci, L. (2021), “Data Persistence in Decentralized Social Applications: The IPFS approach”, 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC).

25. Buterin V.: A Next-Generation Smart Contract and Decentralized Application Platform (2013). https://github.com/ethereum/wiki/wiki/White-Paper

26. Canessane, R. A., Srinivasan, N., Beuria, A., Singh, A., & Kumar, B. M. (2019), “Decentralised Applications Using Ethereum Blockchain”, 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)

27. C. Dannen, “Introducing Ethereum and Solidity”, Berkeley, CA:Apress, 2017.

28. David Lee Chaum, “Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups”, University of California, Berkeley, 1982

29. David Lee Chaum, Blind Signatures for Untraceable Payments

30. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, 1991.

31. Ralph C. Merkle, "A Digital Signature Based on a Conventional Encryption Function." 1998

32. Cynthia Dwork and Noni Naor (1993). “Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology”.

33. Adam Back, "Hashcash - A Denial of Service Counter-Measure", technical report, August 2002

34. Jakobsson, M., Juels, A.: Proofs of work and bread pudding protocols. In: Secure information networks, Springer (1999)

35. Kathleen E. Wegrzyn, Eugenia Wang, “Types of Blockchain: Public, Private, or Something in Between”, Published To: Manufacturing Industry Advisor Innovative Technology Insights Dashboard Insights

36. Parma Bains, “Blockchain Consensus Mechanisms: A Primer for Supervisors”, January 2022

37. Lashkari, B., & Musilek, P. (2021), “A Comprehensive Review of Blockchain Consensus Mechanisms”, IEEE Access, 9, 43620–43652.

38. Yusoff, J., Mohamad, Z. and Anuar, M. (2022), “A Review: Consensus Algorithms on Blockchain”, Journal of Computer and Communications, 10, 37-50

39. Casino, F., Dasaklis, T.K., Patsakis, C. “A systematic literature review of blockchain-based applications: Current status, classification and open issues.” Telematics and Informatics 2019

40. lnes, S., Jansen, A., “Blockchain technology as s support infrastructure in e-government”, In: Janssen, M., Axelsson, K., Glassey, O., Klievink, B., Krimmer, R., Lindgren, I., Parycek, P., Scholl, Hans J., Trutnev, D. (eds.) EGOV 2017. LNCS, vol. 10428, pp. 215–227. Springer, Cham (2017)

41. García-Bañuelos, L., Ponomarev, A., Dumas, M., Weber, I., “Optimized execution of business processes on blockchain” In: Carmona, J., Engels, G., Kumar, A. (eds.) BPM 2017. LNCS, vol. 10445, pp. 130–146. Springer, Cham (2017).

42. Bocek, T., Rodrigues, B., Strasser, T., Stiller, B., “Blockchains everywhere - a use-case of blockchains in the pharma supply-chain” In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (2017)

43. Shae, Z., Tsai, J., “On the design of a blockchain platform for clinical trial and precision medicine” In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (2017)

44. Toyoda, K., Mathiopoulos, P., Sasase, I., Ohtsuki, T., “A novel blockchain-based Product Ownership Management System (POMS) for anti-counterfeits in the post supply chain”, IEEE Access 5, 17465–17477 (2017)

45. Munsing, E., Mather, J., Moura, S., “Blockchains for decentralized optimization of energy resources in microgrid networks”, In: 2017 IEEE Conference on Control Technology and Applications (CCTA) (2017)

46. Kshetri, N.,” Blockchain’s roles in strengthening cybersecurity and protecting privacy. Telecommun”, Policy 41, 1027–1038 (2017)

47. Aitzhan, N.Z., Svetinovic, D., “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams”, IEEE Trans. Dependable Secure Comput. 1 (2016)

48. Grumbach, S., Riemann, R., “Distributed random process for a large-scale peer-to-peer lottery”, In: Chen, L.Y., Reiser, H.P. (eds.) DAIS 2017. LNCS, vol. 10320, pp. 34–48. Springer, Cham (2017)

49. Wijaya, D.A., Liu, J.K., Suwarsono, D.A., Zhang, P., “A new blockchain-based value-added tax system”, In: Okamoto, T., Yu, Y., Au, M.H., Li, Y. (eds.) ProvSec 2017. LNCS, vol. 10592, pp. 471–486. Springer, Cham (2017)

50. Zishan Zhao, “Comparison of Hyperledger Fabric and Ethereum Blockchain”, 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)

51. IBM Hyperledger Fabric. Retrieved from https://www.ibm.com/blockchain/hyperledger

52. Androulaki, E., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Laventman, G. (2018), “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”, Proceedings of the Thirteenth EuroSys Conference on - EuroSys ’18.

53. Debajani Mohanty, “R3 Corda for Architects and Developers: With Case Studies in Finance, Insurance, Healthcare, Travel, Telecom, and Agriculture”, Apress; 1st ed. edition (June 29, 2019)

54. Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C. (2017), “A Distributed-Ledger Consortium Model for Collaborative Innovation”, Computer, 29–37.

55. M. Hearn, “Corda: A Distributed Ledger white paper R3”, Nov. 2016, Available: docs.corda.net/_static/corda-technical-whitepaper.pdf

56. Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S., & Ylianttila, M. (2021), “Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research”, IEEE Access, 9, 87643–87662.