BLOCKCHAINS AND SMART CONTRACTS FOR THE INTERNET OF THINGS

Shtiliyana R. Stoyanova

National military university „Vasil Levski" , Veliko Tyrnovo

Abstract: *Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner. We also point out certain issues that should be considered before the deployment of a blockchain network in an IoT: from transactional privacy to the expected value of the digitized assets traded on the network.*

Keywords*: Blockchain, distributed systems, internet of things.*

БЛОК-ВЕРИГИ ТЕХНОЛОГИЯ И УМНИ ДОГОВОРИ, ПОДПОМАГАЩИ „ИНТЕРНЕТ НА НЕЩАТА"

Щилияна Р. Стоянова

Национален военен университет "Васил Левски", ф-т „Общовойскови", гр. Велико Търново

1. Въведение

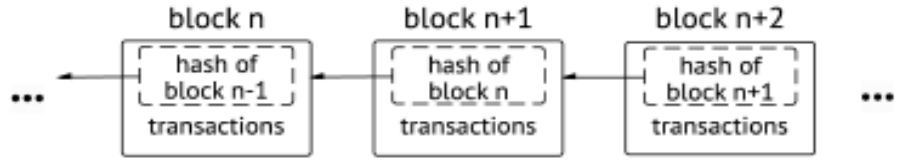
Блок-вериги технологията все по-често привлича интереса на търговските дружества в различни сфери: от финансова [1] и здравни грижи [2, 3], комуникационни услуги [4], недвижими имоти [5, 6] и държавния сектор [7]. Причината за огромният интерес е чрез използването на блокови вериги , приложенията, които преди това са се изпълнявали само чрез доверен посредник, работят по децентрализиран начин, без да е необходима външна намеса за постигане на същата функционалност със същата степен на сигурност. Това просто не е било възможно преди.

Интелигентни договори - самостоятелно изпълняващи се скриптове, намиращи се в блоковите вериги, като тези концепции позволяват точна, безотказна и автоматизирана работа. Това трябва да направи блоковите вериги примамливи за работещите изследователи и разработчици в сферата "Интернет на нещата" (IoT).

Цел на този доклад е да се даде подробно описание за това как блоковете и интелигентни договори работят, за да се идентифицират плюсовете и минусите, които въвеждането им носи в система. Докладът е структуриран в няколко раздела, обхващаши следната тематика: какво е блок-верига, как действа мрежата на блоковата верига, как интелигентните договори позволяват да се ограничи взаимодействието между операторите на дадена мрежа, и как могат да бъдат създадени и автоматизирани, разглежда как IoT и блоковите вериги могат да се използват заедно, да се подчертаят съществуващите приложения на IoT-on-the-blockchain и да се разгледат някои проблеми, които могат да възникнат по време разработването на блоковите вериги, представят се някои решения за преодоляване на проблемите, които могат да възникнат.

Описание на блок-вериги технологията

Блок-веригата, която е разпределена база от данни се използва и споделя между членовете на мрежата. Тя е въведена с Bitcoin [8] за избягване на проблема с двойното плащане на такси [9].



Фигура 1. Блок схема на блог верига технологията

Всеки блок във веригата (виж фиг. 1) съдържа списък на транзакциите и хеш към предишния блок. Изключението от това е първият блок на верига (не е изобразен), наречен генезис, който е общ за всички клиенти в блокова верига и няма родител. Блоковете от веригата могат да стоят сами за себе си и не е необходима криптомерност [11]. Блок-веригата се представлява като дневник, чиито записи са включени в блокове с времеви марки. Всеки блок се идентифицира чрез криптографския си хеш. Всеки блок препраща към хеш блока, който е пред него. Това създава връзка между блоковете, като по този начин създава верига от блокове или блок-верига - виж фигура 1. Всеки възел с достъп до този преди него, обратно свързан списък с блокове, може да го прочете и да разбере каква е състоянието на данните [10], които се разменят в мрежата.

По-лесно може да се разбере как функционира блок-верига, когато се изследват как функционира блоково верижната мрежа. Това е набор от възли (клиенти), които работят на една и съща блок-верига чрез копието, което всеки един държи. Един възел може по принцип да действа като входна точка за няколко различни потребители на блок-верига в мрежата, но за простота се предполага, че всеки потребител осъществява транзакции в мрежата чрез свой собствен възел. Тези възли образуват мрежа от тип peer-to-peer, където:

1) Потребителите взаимодействат с блоковата верига чрез двойка частни/публични ключове [9]. Те използват своя частен ключ, за да подписват собствените си транзакции и са адресируеми в мрежата чрез своя публичен ключ. Използването на асиметрична криптография води до установяване на автентичността, целостта и репутацията в мрежата. Всяка подписана транзакция се излъчва от потребителския възел на хонорарите си с едно хоп;

2) Съседните блокове гарантират, че тази входяща транзакция е валидна, преди да я предаде по-нататък; невалидните транзакции се изхвърлят. В крайна сметка тази транзакция се разпространява в цялата мрежа;

3) Транзакциите, които са събрани и валидирани от мрежата чрез горепосочения процес по време на договорен времеви интервал, се подреждат и записват в блок за кандидатстване с временна стойност. Това е процес се нарича mining (миниране). Минният възел излъчва този блок обратно в мрежата. Изборът на минния възел и съдържанието на блока зависят от консенсусния механизъм, който мрежата използва;

4) Възлите потвърждават, че предложеният блок (а) съдържа валидни транзакции и (б) препратките чрез хеша на правилния предходен блок в тяхната верига. Ако случаят е такъв, те добавят блока към тяхната верига и прилагат транзакциите, които съдържа, за да актуализират своя световен изглед. Ако това не е така, предложеният блок се изхвърля. Това означава край на кръга.

Това е повтарящ се процес. Когато се говори за потвърждаване на транзакцията в стъпка 2, естественият въпрос е: какво представлява валидна транзакция?

В една блок-верижна мрежа това, което има по същество, е набор от недоверчиви клиенти, които споделят база данни без доверен посредник [11]. Тайната за предаване на конфиденциални съобщения е от огромно значение[13]. За да се предотврати избухването на хаос в тази разпределена среда и за да се подпомогне мрежата да достигне общ глобален поглед към света (т.е. постигане на консенсус), всяка блокова верига трябва да установи определени правила, които всяка транзакция на базата данни трябва да спазва. Тези правила, които зависят от приложението, се програмират във всеки клиент на блок-веригата, който след това ги използва, за да реши дали дадена входяща транзакция е валидна и съответно дали тя трябва да бъде препредавана в мрежата или не. В опростения модел на "споделена база данни", която се представя тук, нека се приеме, че всеки ред от базата данни е присвоен на публичен ключ (или адрес), който контролира кой може да го редактира. След това валидна транзакция е тази, която се опитва да промени реда, за който има съответният подпис.

Когато всеки възел в мрежата следва стъпките, изброени по-горе, споделената върху която работи, се превръща в автентичен и запечатан във времето запис за дейността на мрежата [10]. Трябва да се обърне внимание, че възлите не трябва да се доверяват на други, което създава термина "доверие"; вместо това доверието се постига като възникваща собственост от взаимодействията на различните участници в системата.

Установяване на консенсус по мрежата

Възлите трябва да се договорят за транзакциите и за реда, по който са изброени в номинирания блок. В противен случай отделните копия на блоковата верига ще се различават; възлите ще имат различен изглед на състоянието на света и мрежата повече няма да може да поддържа уникалната хронология (т.е. блок-верига), освен ако този възел не бъде решен.

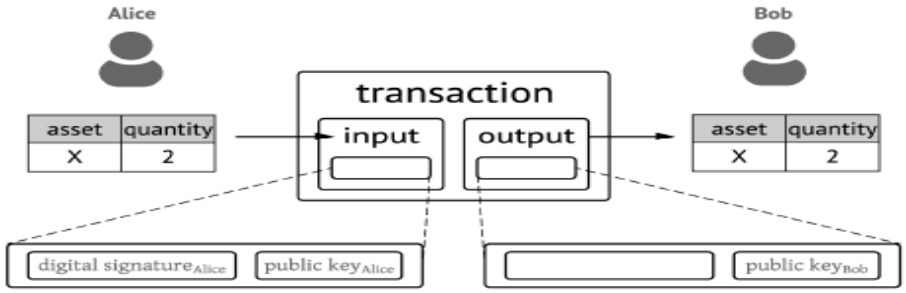
За целта е необходим разпределен, съгласуван механизъм във всяка блокова верига, за да се постигне това. Видът на използван механизъм за консенсус зависи от типа блоково верижна мрежа и вектора на атаката, която мрежовият оператор приема.

Доказателство за участие (Proof-of-stake-PoS) е алтернатива на доказателството за работа, което изисква много по-малко изчисления на процесора за добива. В PoS шансовете за извличане на следващия блок възли са пропорционални на равновесието на този възел. Схемите на PoS имат свои собствени силни и слаби страни , а действителните реализации се доказват да бъдат доста по сложни .

Практическата византийна толерантност (Practical Byzantine Fault Tolerance-PBFT) е такъв алгоритъм. Той предлага решение на проблема с византийските генерали , който работи в асинхронни среди като интернет. (Bitcoin чрез механизма, описан по-горе, също така предлага практическо решение на същия проблем.). Той включва трифазен протокол и понятието "първичен" (лидер) възел, който действа като блок миньор; лидерът може да бъде променен от останалата част от мрежата чрез т.нар. "механизъм за гласуване", ако се срине или ако има произволно поведение (византийски грешки). PBFT работи при предположението, че по-малко от една трета от възлите са дефектни (f), поради което казват, че тя изисква най-малко $3f + 1$ възли.

Трансфер на цифрови активи по блокова верига

За да покажете как работи прехвърлянето на активи, най-добре е да се разгледа опростен пример от банковия свят. Пример е централната база данни на банката, която следи общите баланси на всеки клиент. По същество се разглеждат таблица с три колони: "тип актив", "собственик" ("контрагент") и "количество" ("сума"). Например, ред в тази таблица с "USD", "Alice", "10" идентифицира Алис с десет депозирани в тази банка. Боб има сметка в същата банка с $ 0 в него. Когато Алис прехвърля $ 2 на акаунта на Боб, "количество" на долара / Alice (типа на актива / собственика) се актуализира до $ 8, а този на USD / Bob сега прочита $ 2. Актив ($ 2 USD) или по-скоро цифровото представяне на този актив е прехвърлен между две предприятия чрез преобразуване на съответните редове в базата данни. Това прехвърляне на цифрови токенизирани активи може да бъде постигнато лесно и по криптографски сигурен начин, като се използва блоково верижната мрежа, която използва транзакционния модел Bitcoin. Ако се помисли отново за модела на база данни, споделяна от недоверчиви клиенти в безпристрастна среда, както в раздел II-A. Всеки ред носи същите имена, както в банковия пример по-горе, с изключение на това, че собственикът вече държи публичния ключ на потребителя, на когото е разрешено да редактира реда. Да се приеме, че базата данни показва, че Алис притежава 10 единици от актив X. (Ще се види как е установена тази истина, т.е. как тези активи са били генерирани скоро). Това е ред в тази база данни, който носи публичния ключ на Алис в " колоната "собственик" и стойностите "X" и "10" съответно в колоните "тип актив" и "количество". Да се предположи, че Алис знае публичния ключ на Боб. Как Алис прехвърля 2 единици от X на Боб? Тя подписва транзакция, която променя реда й, намалява стойността на X по 2 и създава нов ред, чийто "собственик" е настроен на публичния ключ на Bob и чиито "тип актив" и "стойност" "elds" са настроени съответно на "X" и "2".



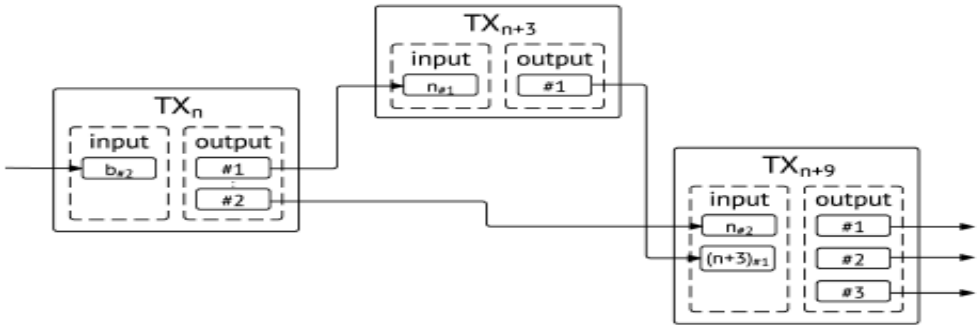
Фигура 2. Транзакция, която прехвърля взетия актив (X) от Алис на Боб. Алис влиза в системата и създава забрана срещу публичния ключ на Боб, така че само Боб може да го похарчи.

Алис прехвърли 2 единици от X на Боб, като създаде нов ред с тази информация и му го даде; Фигура 2. (В действителност, транзакцията на Алис също е изтрила собствения си ред, е създала нов ред, определен за един от нейните публични ключове, и е преместен с останалите 8 единици на X, които тя държи там. Това се прави, за да се контролира конкуренцията. За предотвратяване на конфликти между операциите за едновременно записване в системата; редове не се променят, вместо това те се изтриват и се създават нови редове с актуализираните стойности [11].) Новият баланс на актива "X" на Боб може да бъде изчислен чрез обединяване на всички редове в базата данни, съответстващи на неговите публични ключове и чийто "тип актив" е зададен на "X". Същото важи и за Алис.

Трябва да се бърне внимание, че една транзакция може да адресира до няколко съществуващи редове вместо само една, т.е. прехвърляне на активи, разпръснати в базата данни, стига да е правилно подписана за достъп до тях. Тези съществуващи, все още изтрити редове се наричат неизразходвани транзакции (UTXO) в Bitcoin; те са създадени от по-ранни транзакции в системата. UTXO, които транзакцията консумира, се наричат транзакционни входове; UTXO, които транзакцията създава, се наричат транзакционни изходи.

Транзакцията след това основно изтрива набор от редове (UTXO) и създава набор от нови редове (UTXO) в базата данни (виж фигура 3 за пример). Един очевиден въпрос от горното описание е: как да се генерират активи и да се въвеждат във веригата.

Преди да се стигне до състоянието на Алис с 10 единици от X, тези 10 единици на X трябва да дойдат от някъде.



Фигура 3. Транзакция на n изразходва втората UTXO

Транзакцията представена на фиг. 3. е транзакцията b (b # 2) и генерира два нови изхода (n # 1 и n # 2), изразходвани от транзакции n+3 и n+9 съответно. Подобен процес се отнася за всяка транзакция в мрежата. Транзакциите са следователно свързани помежду си и дават възможност за лесно проследяване на пробите. Отговорът е, че зависи от мрежата и нейната цел. Обикновено упълномощеният възел използва специален тип транзакция за въвеждане на актив (или нови дялове на актива) в мрежата.

Ако се приеме, например, частна блок-верижна мрежа между Алис, Боб и Карол. Карол определя това чрез използване на MultiChain , платформа за блокиране, която възлага разрешения (може да се свърже с мрежата, да осъществи транзакция в мрежата, може да издаде в мрежата) на публични ключове. Карол конфигурира мрежата така, че нейният публичен ключ да може да из-

дава активи в мрежата. Тя кани Алис и Боб да се присъединят; и двамата са наясно с способността на Карол да издава активи на веригата. Всичките имат двойка частни и публични ключове. Карол подава подписана транзакция, която генерира 10 единици от X. Възлите в мрежата считат тази сделка за валидна, тъй като нейният публичен ключ е разрешен по подходящ начин. След това Керол прехвърля тези новосъздадени единици от X на Алис, което ни води до Алис с 10 единици от X.

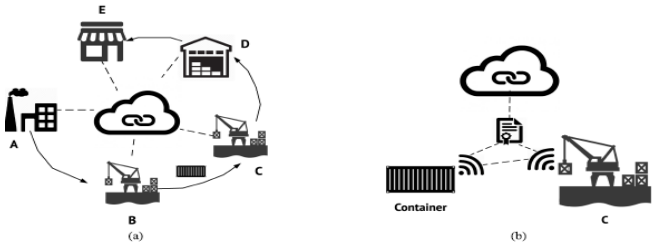
В случая на Bitcoin в мрежата се въвеждат нови битови монети с всеки изваден блок: Минният възел включва така наречената транзакция в блока от транзакции, които излъчва в мрежата. Това прехвърляне на монети няма входни данни и не възнаграждава добива на възел с предварително определено (от мрежата) количество bitcoins.

Блокови вериги и IoT

Създателите правят възможно преминаването от децентрализирана архитектура към все по-разширяващата се система на „Интернет на нещата“ да бъде устойчива. От страна на производителя, настоящият централизиран модел има високи разходи за поддръжка, заради разпространението на софтуерните актуализации до милиони устройства в продължение на години, след като са били прекъснати дълго. От страна на потребителя има оправдано липса на доверие в устройствата, които "стоят" във фонов режим и необходимостта от подходът "сигурност чрез прозрачност". Тези проблеми могат да бъдат разрешени с широко обхватен модел "peer-to-peer", който може да работи по прозрачен начин и да разпространява сигурно данните; авторите правилно посочват, че този модел е елегантно решение на този проблем.

Полезността на блоковете в настройка на IoT не спира там. Ако се обмисли типичния пример за веригата за доставки, който се използва, за да се подчертае стойността на блок-верига: контейнер, който напуска производствения обект (точка А), се транспортира по железопътния транспорт до съседния порт (точка Б) (точка В), се транспортира отново до съоръженията на дистрибутора (точка Г), докато окончателно достигне мястото на търговеца на дребно (точка Е). Този процес включва няколко заинтересовани страни и проверки по пътя, всички от които са показани на фигура 4а. Всеки участник обикновено поддържа собствена база данни, за да следи актива, който те актуализират въз основа на входящите данни от другите страни по веригата.

Мрежата, която използват блоковите вериги, която е създадена за проследяване на този актив, би означавала, че сега има една обща база данни, в която да се следи, къде се получават актуализации с криптографска проверка, да се разпространява автоматично по мрежата и да се създаде опровержима следа от информация. Например (Фигура 4b), когато превозвачът стигне до крайния порт, той изпраща подписано съобщение към предварително определен и договорен интелигентен договор, за да позволи на всеки от веригата да знае, че контейнерът е в точка В. Тъй като транзакцията е подписана, той действа криптографски надежден прием на корабната компания че контейнерът е достигнал до пристанището на местоназначението. Приемникът в пристанището изпраща до същия интелигентен договор, за да потвърди, че той е в притежание на контейнера.



Фигура 4. Пример за проследяване на активите, използващи интелигентни договори и интернет.

На фигура 4а контейнерът напуска производственото предприятие (A), достига до съседния порт (B) по железопътния транспорт, транспортира до целевия порт (C) и след това до съоръженията на дистрибутора (D) мястото на търговеца на дребно (E). На фигура 4b се съсредоточаваме върху етапа B-C. Носителят на контейнер изпълнява ръкостискане с дока на целевия порт (C), за да потвърди, че контейнерът е доставен до очакваното място. След като завърши ръкостискането, той подава към интелигентен договор, за да подпише доставката. Портът за местоназначение

следва заедно, за да потвърди получаването. Ако възелът в С не публикува в договора в приемлив срок, превозвачът ще знае и може да започне разследване на място.

Някои проблеми и техните решения.

Могат да се идентифицират няколко трудности, които може да възникнат при експериментирането на разработчиците на системи IoT с блокови вериги или при внедряване на техни устройства в IoT, които да участват в блок-верижна мрежа. В сравнение с правилно конфигурирана централизирана база данни, блоковите вериги като цяло ще доведат до слабо представяне при по-ниска производителност на обработка на транзакциите и по-големи закаснения. Този проблем е особено изразен в обществените мрежи, където се извършват proof-of-work механизми (доказателствени механизми), въпреки че нови предложения, като Bitcoin-NG, показват обещаващи резултати. Като цяло, тази технология е цената, която трябва да се плати за безпристрастна децентрализация и устойчивост.

Поддържането на поверителността на блоковата верига е сложен проблем. Всяко участващо устройство е идентифицирано от техния публичен ключ (или неговия хеш). Участникът не е необходимо да знае ключовете на всички останали; той просто се нуждае от ключа на неговата транзакция. Въпреки това всички сделки в блоковите вериги се случват публично. Чрез анализирането на тези данни, заинтересованата страна може да идентифицира модели и да създава връзки между адресите и в крайна сметка да разкрие действителните идентичности.

Няколко начина да се смекчи, но не напълно да се реши този въпрос, ако поверителността е важна за разглежданото приложение са:

1) Нека даденото устройство да използва нов ключ за всяка транзакция или да използва различен ключ за всеки контрагент, за да се направи разпознаването на шаблона различно.

2) В случай на частни блокчета, препоръчително е да не се използва една и съща блок-верига за всички транзакции, ако друг участник може да получи конкурентно предимство чрез проследяване на активността на устройството ви.

Правната приложимост на интелигентните договори е ограничена. Работата се върши, за да бъдат техническите правила за интелигентните договори правно приложими и задължителни за всички страни. Начин за увеличаване на шансовете за юридическа приложимост е да се включи позоваване на действителния договор в реалния свят в интелигентния договор и обратно. Допирателна към това е въпросът за очакваната стойност на активи, които са осуетени. Блоковете се използват за търговия с тези символи, защото са свързани с някаква стойност. В блок-верига, която не поддържа интелигентни договори, двойната интеграция не е опция.

Една блокова верига може да се нуждае и от следните механизми за допълване на нейната функционалности трябва да бъдат децентрализирани, за да не се нарушава характерът на мрежата:

- DNS услуга, която съдържа насоки към ресурси. Blockstack , например предоставя такава услуга в мрежата Bitcoin. Потребител изпраща подходящо кодирана транзакция в блока за Bitcoin, за да създаде блокове на Blockchain, които филтрират блок-веригата за последователности от данни, съответстващи на валидни блокиращи транзакции, и ги използват, за да променят съответно базата данни с имена.
- Сигурна комуникация и обмяна на информация. Както се отбеляза по-горе, съобщенията в блок-веригата се четат от всеки участник в мрежата. Всеки път, когато е необходим частен комуникационен канал, вместо това трябва да се използва протокол като телешоу или Whisper. Потребностите на мрежата за споделяне на файлове могат да бъдат адресирани чрез конфигурирана P2P система като IPFS .

V. ЗАКЛЮЧЕНИЯ

Комбинацията от блокови вериги и „интернет на нещата“ може да бъде доста мощна. Блоковите вериги осигуряват гъвкави, наистина разпределени системи от типът "peer-to-peer" и безопасна комуникация между трети лица дори и без наличие на доверие. Интелигентните договори позволяват да се автоматизират сложни многоетапни процеси. Устройствата от „интернет на нещата“ са точките на контакт с физическия свят. Когато всички те са комбинирани се автоматизира отнемащите много време дейности по нови и уникални начини, постигане на криптографска защита, както и спестяването на значителни разходи и време в процеса. Смята се, че по-нататъшното интегриране на блоковите вериги в областта на „интернет на нещата“ ще доведе до

значими трансформации в различни индустрии, с което да се въведат нови бизнес модели и като с това да се преразгледат как се прилагат съществуващите системи и процеси.

References:

[1] А. Мизрахи. (2015). Записване на собственост на базата на блокови вериги: http://chromaway.com/papers/A-blockchainbased-property-registry.pdf

[2] Г. Грийнспан. (2015). Прекратяване на дебатите срещу Bitcoin или Blockchain.

[3] http://www.multichain.com/blog/2015/07/bitcoin-vsblockchain-debate/

[4] Д. Кели и А. Уилямс. (2016 г.). Система за търгуване с облигации на четиридесет големи банки. HTTP: http://www.nytimes.com/reuters/2016/03/02/business/02reuters-bankingblockchain-bonds.html

[5] Д. Опара. (2016 г.). 3 начина, по които блоковите вериги ще променят пазарът за недвижими имоти. http://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/

[6] Двойно харчене - Bitcoin WiKi, https://bg.bitcoin.it/wiki/double-spending.

[7] Документация на Eris Industries – Blockchains. https://docs.erisindustries.com/explainers/blockchains/

[8] И. Кар. (2016 г.). Естонските граждани скоро ще имат най-защитената база от данни в света и доказателство за това са здравни записи. http://qz.com/628889/this-eastern-european-country-is-moving-its-health-recordsto-the-blockchain/

[9] М. Уолпорт, Технология на разпределените книги: отвъд блоковата верига ",UK С. Лейси. (2016 г.). Енергийната блокада: Как Bitcoin може да бъде катализатор за разпределената мрежа. http: //www.greentechmedia. com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-forthe-distributed-gr

[10] С. Накамото. (2008 г.). Bitcoin: Система за електронна парична система от тип "Peer-to-Peer". https://bitcoin.org/bitcoin.pdf

[11] W. Suberg. (2015). Най-новото партньорство на Factom поема здравеопазването на САЩ.

[12] Стоянова В., Възможности за изпращане на тайни съобщения през Интернет, CIO бр. 7, 2015