№ 1 (1), 2019
ISSN 2682 - 9517

ОСОБЕНОСТИ НА BLOCKCHAIN ТЕХНОЛОГИЯТА

Красимир Крумов, Атанас Атанасов

FEATURES OF BLOCKCHAIN TECHNOLOGY

Krasimir Krumov, Atanas Atanasov

Химикотехнологичен и металургичен университет, бул. Св. Климент Охридски 8, 1756 София, Тел (+3592)8163484, E-mails: kr.krumov@gmail.com, naso@uctm.edu

Abstract: This report aims to provide the basics of decentralized databases in the newest Blockchain structure. Principles of construction and the way of working are provided. The known strengths and weaknesses are considered. A short comparative analysis between blockchain and the old database structures was made. We have also paid attention to future opportunities for exploitation, as well as the assessment of the development over time.

Key Words: blockchain, decentralization, future DB, dAPP in Blockchain, Proof of Work algorithm, Proof of Stake algorith

ВЪВЕДЕНИЕ

Съвременният свят е изпълнен със събития и обекти, постоянно запъващи нашето време, движение, реалност.

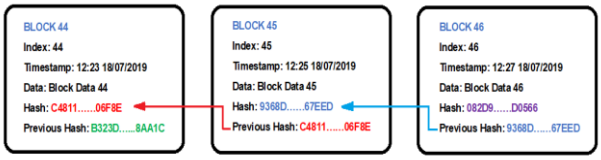
Все повече и повече навлизаме в ерата на постоянното документиране. Разбира се възниква и въпросът за съхраняването и обработването на информацията, достъпност и сигурност. В 21-ви век всеки определено изисква данни за всякакви обекти в ежедневието си. Това определя необходимостта от възможности за записване, съхранение, както и от възможности за бърза експлоатация на всякакви бази данни, натрупани във времето. Дали съществуващите и създадени в близкото минало бази данни са подходящи? Дали има какво още да се сътвори? Дали всичко ново и съвременно ще е достатъчно революционно? Всички тези въпроси си задаваме и изучавайки и анализирайки, търсим най-подходящата за всяко начинание.

ИЗЛОЖЕНИЕ

В настоящата статия е направен кратък обзор на блокчейн технологията [1, 3], на нейните принципи, особености и приложения. Това е последния създаден DataBase продукт, развиващ се стремглаво в съвременния свят и смело уповаващ се на всички създадени в миналото бази данни. Ще направим сравнителен анализ на характеристиките, приложимостта и възможностите за експлоатация чрез специализирани dAPP.

1. ОСНОВА НА BLOCKCHAIN СТРУКТУРАТА

Буквалният превод от английски на термина Blockchain е блокова верига. Това представлява свързана структура от блокове, сами по себе си изграждащи разпределена и децентрализирана база от данни. Блоковете са свързани помежду си в постоянно растяща верига. Блоковете съдържат записи с трансакции, които са кодирани криптографски. Освен трансакции, всеки блок съдържа информация за предходния блок (Фиг. 1.) и е удостоверен с времеви маркер (Timestamp). Това осигурява хронологична цялост на информацията във веригата и дава възможност за проследимост назад до първия блок.



Фиг. 1. Блокова верига (Blockchain)

Така технологията осигурява сигурност чрез самия дизайн. Типично е блоковата верига да се съхранява в мрежата в разпределен вид – с копия на структурата в компютъра на всеки участник в мрежата. Няма точно определено едно главно копие. Тази равнопоставеност на съхранението използва връзка от типа всеки към всеки (Peer to Peer)[11] и спазва протокол за валидиране на новите блокове. Веднъж валидиран и записан никой блок не може да бъде променян без одобрение (консенсус) на останалите участници в блокчейн веригата.

Технологията Blockchain се развива в последните няколко години, тъй като тя е в основата на криптовалутите и трансакциите с тях.

Първоначалните изследвания по криптографска защита на верига от блокове са свързани с разработки на S. Haber и W. Stornetta от 1991/92 г. [4, 5, 8]. Разработките им са свързани със система, която да гарантира, че времевият отпечатък (timestamp) на даден

документ не може да се променя. През 2008 за първи път започва да се употребява терминът блокчейн, като това се свързва с Satoshi Nakamoto, който разработва нова концепция за добавяне на нови блокове във веригата, както и с добавяне на нов метод за Hashcash криптиране на информацията. От 2016 г. много организации и концерни, сред които са IBM, World Economic Forum и др. откриват компютърни центрове с основна цел – развитие и приложение на блокчейн технологията.

2. ХАРАКТЕРИСТИКИ НА БЛОКОВАТА ВЕРИГА

Някои от основните характеристики на създадената блокова структура са:

- **Децентрализираност** - няма нужда от поддържане на сървър, защото всеки компютър, който участва в блоковата верига играе ролята и на клиент и на сървър.
- **Сигурност** (копие от информацията е налична при всеки участник).
- **Достъпност** - използва се *peer to peer* връзка чрез интернет протокола.
- **Устойчивост** или невъзможност за промяна (свързано е с протокола).

Всички изброени предимства са в основата на идеята и разработката на този иновативен метод за разпространение на информацията. Съществуват и отрицателни страни, като:

- невъзможност за съхранение на големи обеми от данни. Това е свързано с ограниченото количество информация, която може да се публикува във всеки блок. В противен случай ще се получи набъбване, безгранично нарастване на веригата, а от там и невъзможност за съхранение.
- кодиране, хеширане на информацията – принцип, който определя надежността на съхранение, но в същото време изисква мощност за декриптирането при опит за достъп и необходимост за използване на данните.

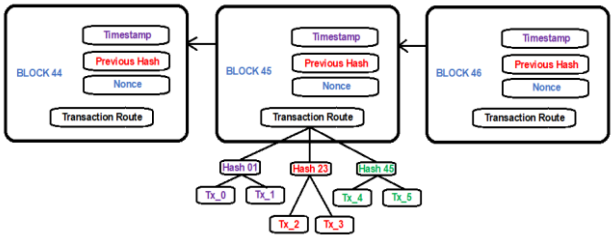
3. СТРУКТУРА НА БЛОК ОТ ВЕРИГАТА

Блокът (Фиг. 2.) се състои от заглавна част (*Header*) и тяло (*body*). Тялото включва трансакциите. Например при биткойн веригата средната големина на блока е около 1MB, а той може да съдържа повече от 500 трансакции.

Заглавната част на блока съдържа:

- хеш стойността на заглавната част на предходния блок (родителя).
- *хеш* корена на дървото на *Markle*, който се изгражда чрез рекурсивно хеширане на двойки трансакции и така обхваща хеш стойностите на трансакциите в блока.

Всеки блок използва [2, 6] хеша на предходния блок, за да формира своя собствен хеш, а това се превръща в негов уникален идентификатор във веригата. Това означава, че при подмяна или добавяне на една единствена трансакция в даден блок, то трябва да се промени неговата хеш стойност и да се реконструира цялата верига след него. Като се има предвид, че копие от блокчейна се съхранява на много компютри в мрежата и е необходим консенсус за всяка промяна, то ако няма такъв консенсус, тази задача става невъзможна.



Фиг. 2. Структура на блок от веригата [8]

Ключова роля при изграждането и поддържането на веригата от блокове е *хешированието*. Чрез криптографска *хеш* функция, базирана на математически алгоритъм, входните данни се преобразуват в изходен низ с фиксирана дължина, наричан *хеш*, *хеш стойност* или *цифров подпис*. Криптографската хеш функция има следните характеристики:

- ✓ хеш стойността се генерира лесно;
- ✓ декриптирането (т.е. възстановяването на оригиналните входни данни на база на хеша) е невъзможно;
- ✓ не е възможно, за различни входни данни да се получи еднаква хеш стойност – т.е. липсва колизия.

Има различни криптографски хеш функции. Например в блокчейна на биткойн се използва SHA- 256 (*Secure Hesh Algoritm 256 – bit*), който генерира 256 – битова (32 байта) хеш стойност. Обикновено тя се представя като шестнадесетично число, състоящо се от 64 цифри.

4. ПРОМЯНА НА ДАННИТЕ ИЛИ ДОБАВЯНЕ НА НОВ БЛОК

В процедурата по промяна или добавяне на данните в съществуващ или добавяне на нов блок се използват различни методи на одобрение. Начинът на одобрение се нарича консенсус между участниците в мрежата. Това е процес на одобрение, потвърждаване на данните от всички или от мнозинството от участниците. Този процес на съгласуване се извършва автоматично чрез протокола за консенсус. В биткойн мрежата например се използва протоколът „Доказателство за работа" (Proof of Work – PoW).

Фиг.3. Постигане на консенсус за промяна на данните в блока.

Участниците в мрежата (възли, *Node*) осъществяват комуникация помежду си, за да приемат (решат) кой нов блок да бъде включен в структурата (Фиг. 3.). Когато бъде постигнат консенсус, то се обновява цялата структура. В процеса на осъществяване на консенсус алгоритъма – всеки участник (*Node*) извършва работа по калкулацията – математически операции за намиране на хеша на новия блок. Затова този процес е свързан с необходима сериозна изчислителна мощност. Използваните устройства са мощни компютри, използващи много виртуални процесорни ядра. Процесът се разделя на подзадачи и така на основата на паралелни алгоритми се получават по-бързи изчисления. Основен минус в описания консенсус алгоритъм PoW остава енергоемкостта. За всеки участник в мрежата са необходими изчислителна мощност, свързаност (гарантирана интернет връзка), енергиен капацитет (сериозна енергийна възможност). Всички тези особености се окачествяват като негативни и затова в блокчейн технологиите се разработват и други методи за консенсус алгоритъм. Те имат за цел отстраняване на негативите и постигане на по-висока скорост на работа. Един такъв алгоритъм е PoS (Proof of Steak)[10]. При този алгоритъм не се налага използването на мощни машини, а от там и намаляване на консумацията на енергия. Този алгоритъм все още е в процес на изграждане и разработка и предстои въвеждането му в мрежата на криптовалутата Ethereum.

5. ПРИЛОЖЕНИЕ НА BLOCKCHAIN ТЕХНОЛОГИЯТА

Основното приложение в миналото и основа на създаването на Blockchain технологията е свързано със създаването на виртуални криптовалути. Създадени са много такива, от които най-известни и експлоатирани: Bitcoin [4], Etereum, Ripple, LiteCoin и др. Всяка валута има своите особености и идеи при създаването си, а най-сериозния репер в системата на размяна остава основоположника Bitcoin.

Използването на виртуални валути в близко бъдеще може да изтласка експлоатацията на реални пари в нормалния свят. За момента тези валути са твърде ненадеждни (с оглед стабилен курс на обмяна), не са достатъчно добре приети сред търговци и доставчици. И макар, че всичко това прави виртуалните валути несъвършенни и със сравнително неясно бъдеще, то са видни и убедителните ползи от тях. А те са: почти никакви такси и комисионни в разплащането и превалутирането; избягването на излишни институции-посредници, като банки и други кредитни организации. От тази гледна точка икономически ползата от виртуалните пари е силно определена. Естествено, съществуват и негативи, защото определени виртуални валути са създадени с идеята за непроследимост. Това спомага експлоатирането им за негативни цели. Така възниква въпросът за смисъла от създаването на новите валути и технологии, както и етичният характер на прогресивните нови технологии. Независимо от всичко изброено абсолютен факт е че множество банки и финансови институции още от 2017 правят инвестиции в блокчейн технологиите и мрежите. Те са свързани с кредитиране, операции с акции, сигурност на трансакции.

Едно от новите приложения на блокчейна се очертава да бъде в логистика при транспортирането на стоки. В този процес участват поне три страни, като доставчици/изпращачи, превозвачи и получатели. Обработката на всяка една пратка/доставка е свързана с редица трансакции и документи като товарителници, фактури, доказателство за доставка и др. Чрез изграждане на блокчейн мрежа членовете й ще могат да валидират всички документи и трансакции, свързани с процеса на логистика и верига на доставки.

Понеже блокчейн технологията използва така наречената разпределена книга, която е криптографски подсигурена, то тя може да управлява интелигентните договори. Интелигентен договор (smart contract) е компютърен протокол, предназначен да улесни, провери или наложи договарянето или изпълнението на договор и разплащането между страните на основата на определена валута или криптовалута. Интелигентните договори позволяват извършването на надеждни сделки без трети страни. Още повече тези договори позволяват проследимост на клаузи при неизпълнение, на които съответната страна се известява за наложените санкции. Страните участващи в такъв договор са неизвестни, но всички участници в блокчейна получават информация за сделката и може да следят коректността й.

Приложението на тези договори, например, може да бъде между енергиен доставчик и физически клиент или фирма потребител. Подобна блокчейн система е внедрена в Австралия от 2017г. На практика приложението на този вид договори в различни области и дейности е неограничено, а това обуславя възможността за силно развитие и приложимост на блокчейн мрежите в някои важни държавни и частни структури:

- Удостоверителни услуги и нотариални записи;
- Гласуване на избори [7] за регистриране на гласоподавателите, за проверка на самоличността им и за електронно отчитане на гласовете;
- Образованието при издаването на дипломи, сертификати и академични справки,

- Здравеопазването – здравно досие с проследимост на осигуровки, прегледи, клинични пътеки и предписани медикаменти,
- Индустриални производства, използващи записване на процеси и времеви промени в изделия и др.
- Застраховане – здравни, имуществени, автомобилни и др. застраховки и контрол върху клаузите им.

ЗАКЛЮЧЕНИЕ

Разгледани са основните характеристики, принципът на действие на блокчейн технологиите, техните предимства и недостатъци и бъдеща употреба.

Блокчейн технологията е сравнително нов инструмент, но е с потенциални приложения в много области и организациите, в които се използват сигурни трансакции без посредници.

Бъдещето на блокчейн мрежите е все още неясно и трудно за прогнозиране. Очаква се те да претърпят редица преобразувания и промени.

Множество изследвания [9] за развитие на тези технологии сочат, че в близко бъдеще до 2030г.:

- много правителства ще въведат собствени криптовалути, което ще доведе до нова ера в разплащанията, както и до регулация на непризнатите от много страни криптовалути.
- в развитите страни да се въведе в употреба блокчейн идентичност, която да замени документи за самоличност, като лична карта и паспорт, както и документите за собственост, като нотариални актове, автомобилни талони др.
- блокчейн мрежите ще доведат до промени в световната търговия, при която много регламенти и договори за внос/износ между отделните страни ще бъдат оторизирани чрез тези мрежи.

ЛИТЕРАТУРА

1. Singhal B., Dhameja G., Panda P, Beginning Blockchain A Beginner's Guide to Building Blockchain Solutions , 2018, Apress Publishing
2. What Is Blockchain Technology?, www.cbinsights.com/research/what-is-blockchain-technology/
3. Yaga D., Mell P., Roby N., Scarfone K., Blockchain Technology Overview, National Institute of Standards and Technology, 2008, doi.org/10.6028/NIST.IR.8202
4. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven, Bitcoin and cryptocurrency technologies: a comprehensive introduction, Princeton University Press,2016.
5. Haber, Stuart; Stornetta, W. Scott, How to time-stamp a digital document, Journal of Cryptology, 1991 issue **3**(2) pp. 99–111,doi:10.1007/bf00196791
6. Damien Cosset, Blockchain: what is in a block?, 2017,https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo
7. 19 индустрии, които технологията блокчейн ще промени,//knowhow.company/blockchain/tehnologiata-blockchain-promenia-19-industrii/
8. https://en.wikipedia.org/wiki/Blockchain
9. Kate Mitselmakher, The Future of Blockchain Technology: Top Five Predictions for 2030, 11, October, 2018, https://www.blockchain-expo.com/2018/10/blockchain/future-of-blockchain-technology
10. Тасев В., PoW vs PoS, (r)evolution of blockchain, 2018-
11. Ковачев А., Blockchain: Build your own P2P network from scratch with Automaton, 2018
12. Тасев В., PoW vs PoS, (r)evolution of blockchain, 2018, https://dev.bg/събитие/pow-vs-pos-revolution-of-blockchain
13. www.coinmarketcap.com