MILITARY APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Luboslav M. Bochev

Faculty of Artillery, Air Defense and Communication and Information Technology, Vasil Levski National Military University, Shumen, Bulgaria, luboslavbochev@abv.bg

Abstract: This report addresses the use of blockchain technology and the benefits in the military forces.

Keywords: military information systems, blockchain

ВОЕННИ ПРИЛОЖЕНИЯ НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА

Любослав М. Бочев

Увод

Иновациите в областта на отбраната имат за цел усъвършенстване на отбранителните способности, чрез внедряване на модерни технологии и тяхното приложение. Технологиите се развиват динамично и с много широк обхват, нуждата от тяхното разбиране и използване е от изключителна полза за отбраната. Този доклад се фокусира върху технологията блокчейн и нейното въздействие и възможности за постигане на информационно превъзходство.

1. Какво е технологията Блокчейн

Блокчейн технологията е създадена през 1991г. от Стюарт Хабер и Скот Сторнета. Тяхната идея е да се създаде система база от данни различна от традиционната клиен-сървър, използвана в World Wide Web. В релационните бази от данни информацията се съхранява централизирано, като достъп до тази информация имат лицата наречени „админи", които се грижат за информацията. Защитата и способността да се подправя информация съхраняваща се в централизираните бази от данни, дава стимул за създаване на нова система която предлага децентрализирана мрежа запазваща суверенитета на данните. За децентрализация се използва p2p мрежата, която позволява на група устройства да изпращат и получават данни без посредник между тях. Това става като устройствата от този тип мрежи използват разпределени изчислителни ресурси, като „процесорна мощ", „дисково пространство" и др. Участниците от този тип мрежа са напълно равноправни и могат да бъдат, както хостове така и сървъри наричат се с общо название пиъри. За да може да се усъществи възможността компютъра да може да работи като клиент и сървър е нужен подходящ софтуер и протокол за специфичната цел.

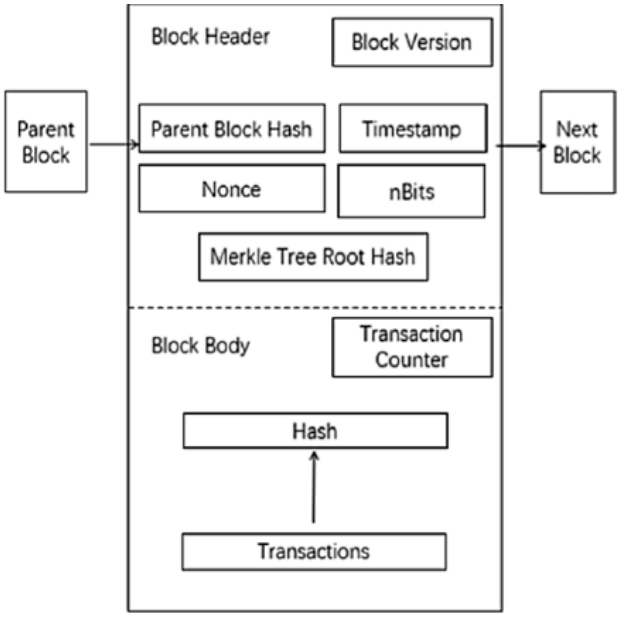
Технологията Блокчейн е усъвършенствана база от данни, като информацията в нея се съхранява от всички пиъри в мрежата, като разстящ лист от блокове които са свързани използвайки асиметрична криптография. Всеки един участник получава копие от тази информация. Цялата информация в блокчейна е публично видима от всички участници в „разпространена счетоводна книга" (distributed ledger). В тази разпространена книга ако се промени информацията ще промени уникалния код на блока(хеш кода) и ще образува домино ефект, при който се развалят всички връзки след тази. Затова тази книга е неизменяща се (immutable). При всяка една промяна или добавена нова информация, кода който работи отдолу изпраща копие (broadcast) до всеки един компютър (node) в системата, така мрежата се синхронизира между устройствата.

2. Как работи Блокчейн системата?

Блокчейн технологията работи върху разпространена p2p мрежа, в която свързва блокове с информация по специфичен начин използвайки хеширане за връзка между предишния и следващия блок. Всеки един блок се валидира от така наречените миньори (това са нодове в системата които валидират данните), тези миньори се състезават кой пръв ще валидира блока като решават криптографски задачи. За да бъде достоверен отговора се използва протокол за спорозомение. Това е техника, при която всички други миньори определят дали отговора от първия миньор е верен и ако е правилен, се споделя (broadcast) на всички нодове. След което, този нов блок от данни се прикрепя към предишния блок и това създава блокчейна. Валидирането на данните се определя от протокола на проекта който използва такъв тип база от данни.

2.1 Блокове

Това са градивните елементи на блокчейна, тяхната структура е разделена на:



(header): В тази част на блока се съхранява хеш стойността на предишния блок, (time stamp), nBits, (nonce) и (merkle root).

- Хеширане:

Хеширането е процес, при който при подаване на входни данни, данните минават през алгоритъм за криптиране, при който на изхода изкарва низ от букви и цифри и представлява уникален код за тези данни, при дори малка промяна, кода се променя. Обикновено се използва SHA-256.

- Time stamp:

Това е времето на създаване на блока.

- Nbits:

Представлява трудността която е зададена от протокола за валидиране на определен блок.

- Merkle root:

Това е структура от данни която е изградена от трансакции намиращи се в body частта. Всяка една трансакция се хешира една с друга докато остане само една, тази една се нарича корен (root).

- Nonce:

Това е число което се използва само веднъж. Това число представлява работата която се извършва от миньорите. Всички миньори инкрементират това число и по този начин променят хеш стойността на блока. Блока се счита за валиден, тогава и само тогава, когато достигне до число, което дава хеш стойност и отговаря на предварително зададени условия от протокола. Колкото повече участници се опитват да отгатнат това число толкова повече трудността за неговото намиране е по-голяма.

(body): В тялото на блока се намират всички събрани трансакции, които образуват така наречения “merkle root”.

- Merkle root : Тип структура от данни която като резултат на изхода се формира хеш стойност който се съхранява в заглавната част (header).

Свързването на блоковете става по подобен начин на имплементация като единичен свързан списък (single-linked list). Този списък е структура от данни свързана по линеен път помежду си чрез указатели (pointers).

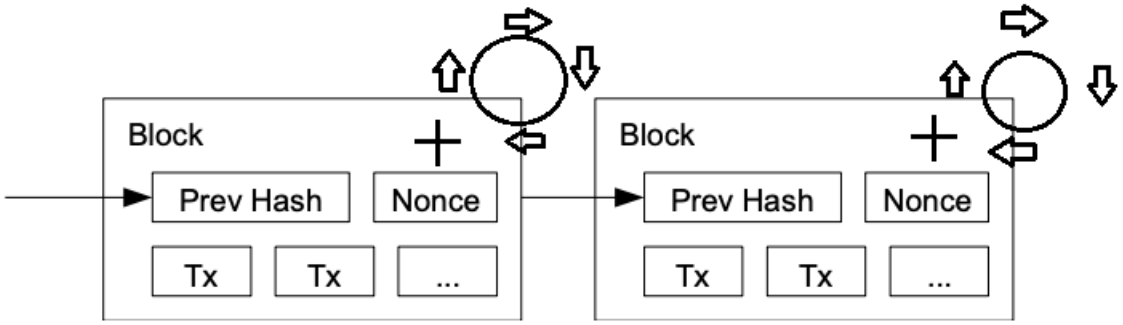
2.2 Процес копаене (Mining)

Това е процес при който всички нодове участващи в системата се опитват да отгатнат целевия хеш (target hash), който се задава от самия протокол на блокчейна. Понеже използвания алгоритъм в повечето случай е SHA-256 възможните комбинации да се отгатне този хеш са много. Заради този проблем в създадените проекти се създава хеш стойност с различна трудност. Трудността се вдига, или намалява зависимост от това, колко изчислителна сила е вложена.

Във всеки един блок съществува число (nonce), което миньорите непрекъснато променят и по този начин променят крайния хеш на всеки блок. За да бъде валиден хеш стойността, тя трябва да бъде равна или по-малко от зададената предварително.

След като стойноста бъде намерена, преди блока да бъде свързан към останалите, този резултат се тества от всички и чак тогава се свързва към блокчейна.

Заради създадената синхронизация, при опит за лъжа другите нодове разбират това и този блок се анулира



2.3 Consensus Protocol (Протокол за спорозомение)

Протоколите за спорозомения са условия при които участниците се съгласяват за достоверност на всеки блок.

Консенсус протоколите имат две основни предизвикателства:

- Защита на мрежата от хакери

- Протоколите защитават блокчейна по такъв начин, че ако хакер се опита да промени някой от блоковете, той трябва да промени всички други след него. Това прави този опит безмислен, защото е необходимо огромно количество изчислителна сила за да може да го направи.

- Конкуриращи се блокове

Възможна е ситуация в която два блока да се валидират по едно и също време, или поради забавяне в мрежата някой нодове да не успеят да се синхронизират навреме. В този случай няма нищо зловредно, а вероятно събитие.

Поради такъв вид ситуации е нужно да съществува удостоверен механизъм, по който да се вземе решение и да няма грешки.

Видове консенсус механизми:

- Proof of Work
- Proof of Stake
- Proof of Capacity
- Proof of Activity
- Proof of History
- Proof of Importance

Всички тези консенсус механизми правят множество проверки за удостоверяване, валидация и много други за предотвратяване на грешки и атаки срещу системата.

3. Проекти на базата на блокчейн

Блокчейн проектите не спират само до криптовалути. Технологията се развива от това не само да замени финансовата система, а и много други сектори.

Технологията може да замени :

- Защитено споделяне на медицински документи;
- NFT пазари (това са пазари за търгуване с дигитално колекционерство);
- Плащания навсякъде по света;
- Защита на лична информация;
- Система за предотравяване прането на пари;
- Система за гласуване;
- Система за недвижимо имущество;

3.1. Биткойн

Сатоши Накамото група от хора или самостоятелна личност под този никнейм създава биткойн, проект използвайки блокчейн технологията през 2009 година. Биткойна е първия децентрализиран проект, който използва блокчейн и икономически консенсус механизъм PoW (Proof of Work). Биткойна представлява публична дистрибутивна система за съхраняване на информация, като целта му е да се използва за паричен обмен. Парите, или единиците, които се разменят в системата са т.нар. дигитални биткойни които имат лимитирана стойност до 21 милиона. Системата е публична защото блокчейна може да се види от всеки. Дистрибутивна е защото всеки с добър хардуер може да съхранява и участва в блокчейн мрежата. Това също е и първия дефлаци-

онен актив. С времето предлагането на биткойна спада и това предразполага за дефлационни сили.

3.2. Етериум

Това е технология, която използва блокчейн, но е много повече от това да работи като разплащателна система. Етериум предлага програмен език, на който могат да се създават приложения (smart contracts) работещи върху блокчейна. Това прави етериум, платформа за изграждане на децентрализирани приложения работещи изцяло върху блокчейна. Проекти изградени върху платформата:

- Децентрализирани финанси(DeFi);
- Децентрализирани игри (Axie Infinity, Dark Forest);
- Система за търгуване с изкуство, колекционерство(NFT), дигитална собственост;
- Създаване на децентрализирани сайтове, даване под наем на изчислителна сила;

Стотици други проекти могат да бъдат измислени, всичко което го има централизирано в интернет, като сайтове с услуги, може да бъде направено върху тази платформа.

Много други наследници на Етериум платформата съществуват, но тя дава основата за изцяло един нов, децентрализиран свят освободен от рестрикциите които се налагат.

4. Военни приложения на блокчейн технологията

Технологиите все повече се развиват и необходимостта на въоръжените сили да бъдат в крак с технологичното развитие на света все повече увеличава интереса на министерството на отбраната за тяхното изучаване. Следващото поколение възникващи технологии, като изкуствения интелект, умни дронове, роботи и други, се нуждаят от защитена, надеждна и точна информация. Защитата и съхраняването на информацията е от изключителна важност в киберсвета на отбраната. Всеки физически или дигитален актив на военните може да бъде проследен използвайки блокчейн технологията, която предпазва информацията непроменена, децентрализирана, което я прави трудно унищожима. Дигитализираните счетоводни книги (digitized ledgers) предоставят възможността да се следи преноса на информация и нейното съхранение. Блокчейн има потенциала да създаде напредък във възможностите, координацията и сигурността на министерството на отбраната за основните военни технологии, които позволяват стратегическо, оперативно и тактическо превъзходство на въоражените сили.

4.1.Видове военни приложения

- Подобраване на киберсигурността

Информационните системи винаги са били уязвими на кибератаки и данните съхранявани в тях могат да бъдат компроментирани. Такива уязвимости могат да бъдат много опасни причиняващи заличаване на данни, управление на кон фиденциална апаратура, преводи на средства, управление на дистанционни оръжейни системи.

Използвайки дистрибутивност, криптография, способността само да се въвежда данни без да се изтрива и използването на консенсус механизъм за взимане на решения между участниците в мрежата, подобрява досегашните слабости в мрежите.

- Намалява правенето на грешки при взимане на решения

(Single point of failure) са вид грешки, които ако се допуснат има вероятност да спре цялата система. Блокчейна предоставя възможност за справяне с подобен тип грешки и ефективно спряване в извънредни ситуации и намаляване на загуби. Използването на криптография за доказателство за идентичност отстранява тези тип грешки докато централизираните информационни архитектури остават с такъв тип слабости. Причината е че колкото повече нодове се добавят в системата, толкова повече вероятността за компроментиране на данни намалява. Природата на

блокчейна да бъде дистрибутивна предотвратява компроментирането на мрежата за разлика от клиент-сървър модела.

- Зашита на данните

Всички данни добавени в блокчейн базата от данни не могат да бъдат променени без да разберат останалите нодове в системата. Криптирането на данните предоставят високо ниво на защита, както и това че не се намират на централизирано място.

Данните споделяни в мрежата могат да бъдат публични, частни и споделими. Конфиденциалността в екосистемата на министерството на отбраната и на големи предприятия се нуждаят от механизми на рестрикции на определени групи, които да имат достъп до тази информация. Например генерала трябва да има най-висок достъп до информация докато подчинените му офицери ограничен до определени области. Придържайки се към децентрализирания принцип осигурява ефективно управление на данни, доставки и автоматични системи използвайки приложения написани върху блокчейна(smart contracts).

- Подобраване на ефективността на логистиката и веригата за доставки

Технологията на блокчейн действа като средство за доверие в екосистемите за обществени поръчки, като позволява по-голяма видимост и сътрудничество между местонахождението и местоназначението. По целия свят компании зависими от доставки се обръщат към блокчейн технологиите. Производители, търговци на дребно, трансокеанските корабни компании внедряват базиран на блокчейн „трак" и проследяване "системи, които осигуряват видимост и доверие на компонентите на храните и продуктите от тяхния произход до крайния потребител. Тези системи предоставят случаи на използване за потенциална верига на доставки на министерството на отбраната използвайки блокчейн.

Преодоляването на разликата между физическия и дигиталния свят се нуждае от мост за разработване на логистична екосистема, която се подхранва от сътрудничество и доверие.

Сложните вериги за доставки на отбраната, които транспортират оборудване и персонал в трудни терени по целия свят. Липсата на видимост и киберустойчивост на всички нива в тези вериги на доставки се признават за една от най -големите заплахи, пред които е изправен този сектор. По време на този процес има редица критични точки, където процесът може да се провали и където има възможности за манипулиране.

Блокчейнът не само може да реши тези проблеми, той предлага по-сигурен запис за управление на веригата за доставки

5. Изводи

В заключение, блокчейн технологията може да бъде разглеждана като дистрибутивна счетоводна книга, която позволява да се подобрят много слабости в досегашните използвани варианти на работа. Подобно на интернет, развитието на блокчейн значително ще ускори процесите във всички области.

References

1. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World by Alex Tapscotta and Don Tapscotta

2. The Truth Machine: The Blockchain and the Future of Everything by Paul Vigna

3. The Age of Blockchain, достъпно на адрес:
https://books.google.bg/books?hl=bg&lr=&id=6_NRDwAAQBAJ&oi=fnd&pg=PA21&dq=military+applications+of+blockchain+technology&ots=ZF6zRDJZrl&sig=7ixpSPBd3idzSVwi6YeVus7T3rI&redir_esc=y#v=onepage&q=military%20applications%20of%20blockchain%20technology&f=false