

ВЪЗНИКВАНЕ НА ВИРТУАЛНИТЕ ВАЛУТИ. BITCOIN И КОНЦЕПЦИЯТА ЗАД НЕГО.

Георги Коджаниколов,

Университет по библиотекознание и информационни технологии, докторант

***Резюме:** Настоящата публикация ще направи опит да заостри вниманието на заинтересованите професионални и любителски кръгове по въпросите на нововъзникналия финансов и технологичен феномен познат като „криптовалута“. По същество темата за безналични и цифрови пари не е съвсем нова и е с давност от повече от 30г. До края на 2009г. и представянето на BitCoin¹ протокола обаче не беше позната реална алтернатива на фиатните пари, разбирани като законно платежно средство, поставено под контрола на орган на публична власт. Появата на BitCoin и множеството други криптовалути (наричани със събирателното понятие “altcoins”) след това е последващо свидетелство, че бъдещето принадлежи на безналичните, дигитални финанси². Дали те ще приемат формата на неконтролирани от правителствата криптовалути или нещо по същество различно, едва ли някой може да се наеме да прогнозира. Ясно е обаче, че реалността в сферата на финансите е коренно променена и различна от традиционно познатата ни до момента. Настоящата публикация ще разгледа в ретроспекция появата на първата криптовалута – BitCoin, както и концепцията на работата ѝ, превръщаща я във функционираща реалност.*

***Ключови думи:** BitCoin, криптовалута, цифровизация, финанси, Blockchain, децентрализация.*

EMERGENCE OF VIRTUAL CURRENCIES. BITCOIN AND THE CONCEPT BEHIND IT.

Georgi Kodzhanikolov

University of Library Studies and Information Technology, Ph.D

Abstract: This publication will make an attempt to sharpen the attention of interested professional and amateur communities on the topics of the emerging financial and technological phenomenon known as "cryptocurrency". In essence, the topic of cashless and digital money is not entirely new and is more than 30 years old. By the end of 2009 and the introduction of the

¹ Криптомат: Какво представлява криптовалутата Биткойн и как работи. (Достъпно на: <https://kriptomat.io/bg/kriptovaluti/bitcoin/kakvo-e-bitcoin/>)

² Кабаиванов, Станимир. Иконометрия за финансиста. София: Евдемония Продъкшън, 2014, 138 с.

Bitcoin protocol, however, there was no real alternative to the fiat money, perceived as legal tender placed under the control of a public authority. The emergence of Bitcoin and the multitude of other cryptocurrencies (“altcoins”) after that is further evidence that the future belongs to cashless, digital finance. Whether they will take the form of government-uncontrolled cryptocurrencies or something fundamentally different anyone can hardly guess. It is clear, however, that the reality in the field of finance has radically changed and is different from the one traditionally known to us until now. This article will take a retrospective look at the emergence of the first cryptocurrency – Bitcoin, as well as the concept of its operation, turning it into a functioning reality.

Key words: *Bitcoin*, cryptocurrency, finance, digitalisation, *Blockchain*, *decentralisation*

Въведение

В ерата на високите технологии и цифровизацията³ темата за виртуалните, безналични пари е бързо развиваща се и широковъълнуваща обществото. Изцяло цифрови дигитални валути като Bitcoin остават извън обхвата на дефинициите на регулаторите и нормотворците за законно платежно средство. Въпреки това криптовалутите – Bitcoin, като водеща и най-лесно разпознаваема, заедно с всички впоследствие появили се и събирателно наричани “altcoins”⁴, се превърнаха във функционираща реалност от естество да постави под въпрос установеното статукво на традиционните фиатни пари (fiat currencies).

Още по-въълнуваща и революционна от самите валути изглежда технологията, върху която са изградени и функционират. Блокчейнът (blockchain) е технология от нов вид, която е способна да подобрява платежните операции, като ги прави по-бързи, надеждни, прозрачни и евтини. Нещо повече, блокчейн технологията позволява изграждането и интегрирането на самостоятелна и децентрализирана система за разплащане, способна да достигне до всеки с достъп до интернет.

Появата на суверенна цифрова валута, извън контрола на публичен орган на власт има потенциала да разтърси основите на познатата ни финасова система и да

³ Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и комитета на регионите относно стратегия за цифровизация на финансовите услуги в ЕС, Брюксел, 24.9.2020 г., COM(2020) 591 final;

⁴ Dannen, Chris. *Introducing Ethereum and Solidity. Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress Publ., 2017, 206 p.

направи нейното изграждане и функциониране под нови правила неизбежно⁵. Отпадането на необходимостта хората да разчитат на регулирана от централната власт банкова институция, която да гарантира съхранението и използването на техните пари, само по себе си е революционна идея в света на финансите.

Изложение

Въпреки че криптовалутите като цяло и биткойн в частност са сравнително нови явления, нарастващата им популярност във връзка с използването им за целите на прането на пари и финансирането на тероризъм заостря необходимостта от много по-широкото им познаване и разбиране от правоохранителните органи⁶.

Имат ли криптовалутите стойност и как се измерва тя ?

Стойността на един обект се измерва със стойността, приписана му от другите участници в гражданския оборот. Принципът на търсенето и предлагането най-добре илюстрира тази зависимост. Нещо, което е рядко, но силно желано, ще има повече стойност от нещо, което е изобилно и неценено. Лошото в механизма е, че желанията на хората обикновено са непостоянни. Високо оценяването и търсено днес може да не е съответно на желаното утре. Златото е ценено, защото е рядко и с висока добавена стойност при използването му в различните стопански отрасли. Също така е много ковък метал и може да се вложи в множество и различни други продукти. Въпреки тези качества, цената на златото се колебае драматично в зависимост от това какво хората са готови да платят за него в даден момент. Неговата стойност в исторически план се е увеличавала, когато националните валути са се възприемали като по-малко надеждни. Нетолкова назад в историята във времената на „златния стандарт“ правителствата са били предпоставени да поддържат еквивалентна стойност на изсечените монети и емитирани хартиени парични банкноти в златен резерв. „Златният стандарт“ е изоставен в началото на 70-те години на XX век. От този момент до днес фиатните пари (законно емитираните парични средства – монети, банкноти, електронни пари) не представляват нищо повече от обещание за плащане без инхерентно прилежаща им стойност. В този

⁵ Доклад с препоръки към Комисията относно цифровите финанси: нововъзникващи рискове, свързани с криптоактивите – регулаторни и надзорни предизвикателства в областта на финансовите услуги, институции и пазари (2020/2034 (INL) (Достъпно на: [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034\(INL\)&l=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en), 28.11.2022)

⁶ FATF dedicated webpage on Virtual Assets: [www.fatf-gafi.org/publications/virtualassets/documents/virtualassets.html?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/virtualassets/documents/virtualassets.html?hf=10&b=0&s=desc(fatf_releasedate));

контекст не е случайно придобилото гражданственост в средите на криптоетусиастите метафорично название на BitCoin - „дигиталното злато“.

Биткойн не е свързан с никоя национална икономика и, както самият интернет, функционалната обезпеченост на системата се изгражда и поддържа от участниците в нея⁷. Максималният брой възможни единици е предварително закодиран и ограничен. Също като Интернет, той работи въз основата на протокол с отворен код⁸. Това от друга страна, означава, че на теория всеки може да създаде своя собствена криптовалута. BitCoin е замислен и конфигуриран като Peer-to-Peer (P2P) мрежа, подобна на популярния BitTorrent (използвана за споделяне на големи медийни файлове като филми и музика чрез разпространението, търсенето и изтеглянето в рамките на самостоятелната система, състояща се от всички компютри в мрежата). Не е предвиден и не съществува единен център или контролен сървър, през който да преминават ключовите процеси или където се съхраняват данните. В P2P мрежите всеки свързан компютър се счита за равноправен партньор и е на разположение за обмен и предоставяне на данни и услуги с всеки друг член на мрежата. Тази концепция е фундаментална за проектирания биткойн софтуер.

BitCoin протоколът предлага реализирани и работещи решения по отношение на парите, които правителствата не предлагат. Системата функционира изцяло децентрализирано, без участието на посредници или регулаторни органи. Друг отличителен белег на иновативното предложение е ограниченото количество на възможните за създаване и включване в оборота BitCoin единици (тук се прави аналогията с „дигиталното злато“). Революционно и непознато до този момент разрешение на фона на неограничените възможности на централните банки да емитират парични потоци в обем по тяхна преценка. Напълно суверенна и автономна система, предвидена да функционира извън света на финансовите регулации и без възможност за правителствена санкция или намеса.

BitCoin предлага алтернативна система за разплащания, която е замислена да бъде достъпна и функционална по начин, който да позволи бързото „финансово включване“ не само на хората от развития свят, но и на уязвими групи по целия свят.

⁷ Antonopoulos, Andreas. Mastering Bitcoin. Unlocking digital cryptocurrencies. O'Reilly Media, Inc., Sebastopol, 2014, 298 p.

⁸ Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Достъпно на <https://bitcoin.org/bitcoin.pdf>;

Виртуалната валута BitCoin функционира изцяло онлайн и няма физически аналог. Инфраструктурата, позволяваща нейното съществуване, по същество представлява програмен протокол с отворен код, който е достъпен за всички потребители. Кодът може да бъде свален и видян от всички. Системата от своя страна създава децентрализирана мрежа от потребители (peer-to-peer), които обезпечават функционирането ѝ. Всеки потребител в системата представлява самостоятелна единица и е свързан с останалите ползватели на BitCoin протокола. Напускането на мрежата е възможно във всеки един момент, както и присъединяването впоследствие. Не може да се каже кой е съзателят на софтуера. Проектиран и реализиран като програмен код, който да осигури функционирането на система, позволяваща на участниците в нея да взаимодействат един с друг без намесата на трета страна. Тази своеобразна автономност от централна банка или правителствена структура прави системата децентрализирана и напълно свободна от потенциалната възможност за овладяване от орган на публичната власт.

BitCoin представлява децентрализирана система, която осигурява възможността на своите ползватели самостоятелно да верифицират и обработват транзакции помежду си. Вместо трета страна извън разменящите стойност, като банка или процесор на плащания, да участва в процеса на обмен на плащания, технологията зад BitCoin използва криптографско решение (функцията SHA256⁹), кодирано в софтуера, за да гарантира легитимността и потвърждаването на обработваните транзакции. BitCoin инфраструктурата позволява обработването на плащания между участниците в нея без контрол или санкция от доверена трета страна или орган на публична власт.

Криптовалутата, използвана за размяна на стойност, също носи името BitCoin. Тя не съществува физически и извън дигиталната среда. Въпреки това се приема, че изпълва икономическата дефиниция за валута:

- 1) използва се като средство за размяна;
- 2) има стойност и може да се съхранява;
- 3) може да се разглежда като единица стойност в акаунт/портфейл;

Първият BitCoin (BTC) е създаден или „изкопан“ (mined) през 2009 г. след публикуването на протокола за технологията, описващ революционната концепция за създаването на виртуална валута.

Съзателят на първата криптовалута остава в историята със своя псевдоним – Сатоши Накамото. Неговата самоличност е неизвестна и до днес. Счита се обаче че

⁹SHA-256 Cryptographic Hash Algorithm. Достъпно на <https://www.movable-type.co.uk/scripts/sha256.html>

концептуалната идея, залегнала при създаването на виртуалната валута, неподчинена на правителство или орган на публична власт, е инспирирана у създателя ѝ от проф. Фридрих Хайек и неговата книга „Денационализация на парите“.

Според проф. Хайек да се противодейства на повтарящите се в исторически план инфлационни и дефлационни процеси би означавало държавният монопол върху парите да бъде отхвърлен. Това от своя страна би направило невъзможно за правителствата да ограничават свободното движение на хора, пари и капитали. Инфлацията, нестабилността, недисциплинираното държавно поведение, националистическите залитания в икономическата сфера са все девиации в нормалното функциониране на демократичните общества.¹⁰ Те могат да бъдат компенсирани и ако не елиминирани, то в значителна степен органичени чрез заместването на държавата в ролята ѝ на единствен субект, упражняващ монополна власт върху парите. Замяната на държавния монопол в тази насока от конкуриращи се частни субекти, би довело до изграждане и съхраняване на доверието в паричната система, би допринесло за ограничаване на количествата печатани пари, а от там и до запазване на тяхната стойност. В голяма степен в това се изразява „денационализацията на парите“.

От тази концептуална рамка се счита, че черпи вдъхновение създателят на първата криптовалута – Сатоши Накамото. Преследвайки чисто идеалистични цели по своята същност той успява да предложи революционно ново решение. Базираните на технологията дигитални пари - криптовалути са представени като чисто нов модел за преформатиране на финансовата, икономическата и културна среда.

Blockchain технологията зад bitcoin

Чрез създаването и поддържането на регистър, отчетност т.нар. „public ledger“ на направените транзакции и баланси по сметките на всички участници в системата, протколът дава напълно автономна, децентрализирана и дистрибутирана система за обмен на стойност. Вместо да разчита на трета доверена страна извън транзактиращите да поддържат тази отчетност, BitCoin протоколът децентрализира и дистрибутира тази отговорност към всички участници (nodes) в мрежата за обмен. Инфраструктурата на BitCoin записва и съхранява цялата история на транзакциите и балансите на всички участници в нея в публичен регистър или т.нар. „blockchain“ от самото начало на публикуване на проткола.

¹⁰ Велкова, Лидия, Стефан, Мичев. Социално-икономически аспекти на сигурността. – В: Национална и международна сигурност. София: Военно издателство, 2005, с. 212-232.

Блокчейнът структурира и подрежда списък от свързани данни и изгражда блокове от транзакции. Блоковете са свързани помежду си, като всеки съдържа препращаща и обвързваща го с предходно генерирания блок информация.

Блокчейн¹¹ е публично достъпен регистър на всички обработени транзакции в мрежата на Bitcoin от самото ѝ създаване до момента. Той позволява всеки, използващ софтуерния код на инфраструктурата, да има достъп до тази отчетност и съответно възможността сам да провери и да се убеди във валидността и легитимността на конкретна транзакция. Транзакциите с Bitcoin са видими и публични за всички участници в мрежата и се включват в регистрите на блокчейна само след като бъдат успешно верифицирани и потвърдени от останалите участници. Това създава гаранция, че повторното изпращане или изхарчване на конкретна единица Bitcoin няма да бъде възможно. Новите транзакции преди да бъдат верифицирани и присъединени към публичния регистър се съпоставят от софтуера в ретроспективен план с вече случилите се и записани в отчетността, за да се гарантира, че един и същи Bitcoin не може да бъде похарчен два или повече пъти.

Bitcoin протоколът предвижда ограничен брой единици – 21,000,000, които могат да бъдат създадени и пуснати в обращение. Според софтуерното разрешение това се очаква да се случи до 2040г. Процесът на създаване и генериране на нови единици Bitcoin е обозначен като копаене („mining“). Направената алюзия от създателя е с дейността по добив на злато. Вложеният символичен смисъл и корелация между ценния метал и Bitcoin е в ограниченото количество в природата на метала. Bitcoin, като дигиталният еквивалент на златото, е замислен с тази цел - да има ограничено количество. Като контрапункт на традиционната финансова система, която е практически неограничена във възможността си да печата и разпространява хартиени парични знаци.

Копачите чрез специализирания софтуер и изчислителната мощ на своите компютърни конфигурации валидират новите транзакции и ги записват в глобалния публичен регистър – блокчейн. На всеки средно около 10 минути се „изкопава“ или валидира нов блок, съдържащ в себе данни за валидирани транзакции, извършени след добавянето на последния блок от веригата. Вече добавените транзакции към блокчейна

¹¹ Making sense of bitcoin, cryptocurrency and blockchain. Bitcoin, cryptocurrency, blockchain... So what does it all mean? (Available on: <https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html>, 12.11.2022)

се считат за валидирани, което позволява на новите собственици на биткойн да се разпореждат с получените средства.

За да получат възнаграждение от мрежата, копачите участват в своеобразно състезание в решаването на сложен математически проблем въз основа на криптографски хеш алгоритъм. Решението на задачата, известно като „доказателство за работа“ (Proof of work), се включва в новия блок и служи като доказателство, че копачът е допринесъл за функционирането на системата чрез извършването на множество изчисления.

Процесът е познат като „копаене“ или добив, защото възнаграждението е проектирано да стимулира намаляваща възвръщаемост, характерна за добива на благородни метали. Максималната сума новосъздадени биткойни, следствие на процеса на копаене, е проектирано да намалява приблизително на всеки 4 г. (на всеки 210 000 нововалидирани и добавени към веригата блока).

Основната цел на добива на биткойн не е създаването на нови биткойни. Представлява механизъм, който поддържа сигурността на мрежата и я прави децентрализирана. Възнаграждението за извършена работа от системата към участниците под формата на новогенерирани единици виртуални монети и таксите за транзакциите е схема за стимулиране, която обезпечава сигурността и функционирането на мрежата.

Заклучение

Повече от десетилетие измина от появата на първата криптовалута – Bitcoin. Към момента съществуват стотици видове криптовалути, които предоставят различни функционалности. Възможностите за използването на криптовалути в съвременния свят са практически неограничени. Криптовалутите са една от проявите форми на технологичните постижения на 21-ви век. Вероятността тяхната поява да е инцидентна и да изчезнат е повече хипотетична, отколкото реална. В контекста на казаното и на фона на множеството доказани случаи на използване на криптовалути с престъпни цели, дълбинното и пълно разбиране на технологията зад тях и самата им природа се явява залог за съхраняване стабилността на финансовите системи¹². Създаването на цялостен регулаторен модел, който да позволи интегрирането им в рамките на законния

¹² Brown, David. Cryptocurrency and criminality: The Bitcoin opportunity. The Police Journal: Theory, Practice and Principles, 2016, Vol. 89 (4), p. 327–339.

граждански оборот, е едно от вероятно най-значимите и належащи предизвикателства демократичните общества.

Използвани източници:

1. Доклад с препоръки към Комисията относно цифровите финанси: нововъзникващи рискове, свързани с криптоактивите – регулаторни и надзорни предизвикателства в областта на финансовите услуги, институции и пазари (2020/2034 (INL) (Достъпно на: [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034\(INL\)&l=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en)., 28.11.2022);
2. Велкова, Лидия, Стефан, Мичев. Социално-икономически аспекти на сигурността. – В: Национална и международна сигурност. София: Военно издателство, 2005, с. 212-232;
3. Криптомат: Какво представлява криптовалутата Биткойн и как работи. (Достъпно на: <https://kriptomat.io/bg/kriptoaluti/bitcoin/kakvo-e-bitcoin/>);
4. Кабаиванов, Станимир. Иконометрия за финансиста. София: Евдемония Продъкшън, 2014, 138 с.;
5. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Стратегия за цифровизиране на финансовите услуги в ЕС. Европейска Комисия. Брюксел, 24.09.2020;
6. Antonopoulos, Andreas. Mastering Bitcoin. Unlocking digital cryptocurrencies. O'Reilly Media, Inc., Sebastopol, 2014, 298 p.;
7. Dannen, Chris. Introducing Ethereum and Solidity. Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress Publ., 2017, 206 p.;
8. Financial Action Task Force (FATF) dedicated webpage on Virtual Assets: [www.fatf-gafi.org/publications/virtualassets/documents/virtualassets.html?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/virtualassets/documents/virtualassets.html?hf=10&b=0&s=desc(fatf_releasedate)));
9. Making sense of bitcoin, cryptocurrency and blockchain. Bitcoin, cryptocurrency, blockchain... So what does it all mean? (Available on: <https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html>, 12.11.2022);

10. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Достъпно на <https://bitcoin.org/bitcoin.pdf>;
11. SHA-256 Cryptographic Hash Algorithm. Достъпно на <https://www.movable-type.co.uk/scripts/sha256.html>;