Марин Йорданов Стоянов

Биткойн от А до Я

Издава:

trade4win.info

С Ъ Д Ъ Р Ж А Н И Е

Съдържание

Увод

Човечеството се намира в изключително бързо развиваща се фаза от неговото развитие. Навлизането на компютрите все по-дълбоко и неизкоренимо в ежедневието на човека води до извода, че бъдещето му ще зависи изцяло от тях. Вече има автопилоти за коли, кораби, камиони и самолети. Нямаме нужда от географски карти, защото почти всеки вече има смартфоун в джоба си с приложенията на Google Maps (сателитни снимки и навигация). Можем с един клик да превеждаме пари от банка в банка (т.н. електронно банкиране „ebanking”:), без значение от местоположението ни. Единственото необходимо условие е да имаме достъп до компютър с интернет. Скоро е напълно възможно парите (тяхната материална форма) да изчезнат и да се превърнат в електронни кредити. Точно такъв проект е бил разработван в последните години. От известно време той е тестван в реалния свят и резултатите са изключително обнадеждаващи. Името на новата ера във финансовия свят е т.н. Bitcoin. Това е валута съществуваща само и единствено в електронен вариант (затова тя се нарича криптовалута), която превзема все повече отрасли с нейния лесен начин за използване, пращане и съхранение.

История

Първата концепция за криптовалута е описана частично още през 1998 г. в списъка за съобщения на т.н. кибер-пънк общност. Обнародвани са преложения от Веи Даи (Wei Dai) за т.н. b-money(8) и на Ник Сабо (Nick Szabo) за Bitgold. Между 1998 г. и 2005 Сабо разработва механизъм за децентрализирана дигитална валута, която нарича "Bitgold", или още наричана от някои хора "пряк предшественик на архитектурата за Bitcoin". Предполага се, че той се крие под псевдонима на изобретателя на Bitcoin, Satoshi Nakamoto. (9) (10) (11) Десетилетие след това Сатоши Накамото (Satoshi Nakamoto) намира решения на някои сложни задачи нерешени до

този момент. През 2008 г. той създава мрежовия протокол на Биткойн и първото приложение за Биткойн клиент. Под този псевдоним най-вероятно стои не само един човек, а цяла група от хора със задълбочени познания по няколко научни дисциплини като математика, криптография, компютърни мрежи и информационни технологии. Биткойн мрежата е пусната в действие през 2009 г. и от тогава придобива все по-голяма популярност.

Същност

Bitcoin е софтуерно-базирана онлайн система за плащане, описана от Satoshi Nakamoto (1) през 2008 г. (2) и е представена като софтуер с отворен код през 2009 г. (3) Плащанията се записват в публична книга(регистър), използвайки собствена разчетна единица, (4), която се нарича Bitcoin. (5) Плащанията се извършват от човек-на-човек (peer-to-peer) без централно хранилище или администратор, което кара Министерството на финансите на САЩ да определи Bitcoin като децентрализирана виртуална валута. (6) Въпреки статута й на валута да е постоянно оспорван, медиите често се отнасят до Bitcoin като крипто валута или цифрова валута. (7)

.

Биткойн (Bitcoin) е парична система и експериментална валута от нов вид, която няма подобие в досегашната история на човечеството. Няма държавен орган, централна банка, частно юридическо или физическо лице, които стоят зад Биткойн и могат пряко да въздействат. Никой не притежава изключителните права да издава, разпространява, пуска или спира от обръщение тези парични знаци. Управлението се осъществява съвместно от цялата разпределена компютърна мрежа (peer-to-peer, за краткост P2P мрежа). Няма географско местоположение за съхранение и отговорно пазене, както е при физическото злато и сребро, когато се използват за пари. Няма централен сървър, който се използва за индексиране на съдържанието, както е при торент мрежите използвани за споделяне на

електронни книги, видео или аудио файлове. Най-краткото определение за Биткойн е, че това е първата разпределена крипто-валута.

За функционирането и защитата на платежната система се използват криптографски методи, а автентичността на всички транзакции е защитена от цифрови подписи. Основен елемент от мрежата е публична счетоводна книга (public ledger) с обществено достъпен списък на всички извършени транзакции, наречен блокова верига (block chain). Това позволява на всеки потребител да провери валидността на всяка транзакция.

Платежните единици биткойн се създават като възнаграждение за извършена изчислителна работа по криптиране, при която потребителите проверяват (валидират) съществуващите блокове от блоковата верига и създават нови като използват изчислителната мощ на компютрите си. За да е легитимен, всеки блок трябва да съдържа доказателство за извършена работа, което подлежи на проверка от другите участници, когато получават нов блок за изчисление. Процесът на придобиване чрез изчисления се нарича „добиване“ или „копаене“ (mining или digging).(12)(13) Добиването е замислено така, че да са необходими значителни изчислителни ресурси, а наличното количество блокове да остава оскъдно. Наименованието е заимствано от други видове добив на оскъдни ресурси (например на злато), които изискват значително време и производствени ресурси. Колкото повече изчислителна мощ се включва в добиването, толкова повече сложността на математическата задача се увеличава, като по този начин скоростта на добиване винаги остава ограничена и предсказуема.

Потребителите могат да изпращат и получават биткойни по електронен път срещу определена такса, като използват електронно портмоне на своя персонален компютър, мобилно устройство или уеб приложение. Освен чрез „добиване“ биткойни могат да се получават срещу продукти, услуги или други валути.(14)

„Паричната маса“ на биткойни е предопределена от същността на генерирането им. Към 2014 в обръщение има над 12 милиона биткойни, като на всеки 10 минути се създават приблизително 25 биткойна. Общото им количество обаче има установена горна граница от 21 милиона(12) и на всеки четири години скоростта на добиване се намалява наполовина. Това означава, че нови биткойни ще продължат да се създават в бъдещите сто години.

До ден днешен създателя на Bitcoin остава загадка. Според една група, която следи дейността на държавните организации по целия свят, той в проект на Националната агенция за сигурност на САЩ (NSA) или от ЦРУ(CIA). Тази група се нарича project CIA и твърди, че има доказателства относно това твърдение. Тя твърди, че името Satoshi Nakamoto е знак, че Bitcoin е управлявано от някакво „Централното разузнавателно управление”. Доклада за Bitcoin е представен от Nakamoto през 2008 (15), а Nakamoto на японски грубо се превежда "Central Intelligence"- Централно разузнаване. В допулнение към това Gavin Bell (известен още като Гавин Андерсън), който е публичното лице на Bitcoin, твърди, че той е общувал с Nakamoto в продължение на много години. Въпреки това, Gavin никога не е го срещал нито е говорил с него по телефона. Също така project CIA твърдят, че програмата използвана от повечето криптовалути за създаване на т.н. secure keys е същата, която използва NSA.

“Докато всички си мислят, че Bitcoin е нова децентрализирана валута, структурното й ядро е 100% централизирано и управлявано от ЦРУ” – добавят още project CIA.(16)

The block chain

Всички сделки биват записвани в публично достъпна и разпространима книга наречена: The block chain. Приблизително на всеки 10 минути група от няколко транзакции се записва в тази книга, а от там и до всички нейни копия по света. По този начин се определя дали определен биткойн е изхарчен или си е сменил собственика и сега е притежание на някой друг. По този начин се избягва

възможността за даден биткойн да бъде охарчен 2 или повече пъти. The block chain е единственото място, където се доказва съществуването на биткойните.(25)

Начини за сдобиване с биткойн.

Директно закупуване

Възможно е директно закупуване от банкомат за биткойни или т.н. Битомати Такъв има вече и в България и се намира в Интерпред –София. Първият биткойн автомат в България беше монтиран в INTERPRED WTC Sofia. Битоматът е разположен на входа на блок Б и чрез него можете да получите биткойни срещу левове. Покупката се осъществява само с три бързи и лесни стъпки. (17)

Размяна на продукти или услуги за биткойн

Възможно е да направите размяна на продукти срещу биткойн. Много търговци правят така:

Expedia приема биткойн за хотелски резервации

Expedia, фирмата за онлайн резервации, заяви, че клиентите й вече ще могат да използват дигиталните пари.Потребителите, които изберат да платят в Bitcoin имат на разположение нова възможност за разплащане на интернет страницата. Избирането й ще ги отведе на отделен сайт, където ще оторизират трансакцията от виртуалния си портфейл с Bitcoin, пише "Уошингтън поуст". (18)

TESLA Motors приема плащания с биткойн

Виртуалната валута беше използвана за покупка на Tesla S електромобил. В шоурум на Lamborghini в Калифорния беше продаден Tesla S електромобил, като плащането беше извършено в биткойни

/bitcoin/, предава агенция Блумбърг. Колата е продадена за 103 хил. долара или около 91.4 биткойна. Трансакцията е била одобрена и извършена и купувачът, който е пожелал да остане анонимен, ще получи автомобила си в най-скоро време, съобщава Седрик Дейви, маркетинг директор на базираното в Калифорния търговско представителство на Lamborghini. (19)

Възможно е да се купи къща с биткойн

За първи път покупка на недвижима собственост беше извършена с новата виртуална валута. Анонимен купувач плати 800 биткойна за луксозна вила в Бали. Еквивалентът на сумата в реални пари е над 500 000 долара. Сделката е извършена чрез посреднически сайт, който е взел 5% комисионна. Вилата се намира на западния бряг на Бали, има красива градина и собствен плувен басейн. За новия собственик се знае само, че е от първите притежатели на биткойн.(20)

Virgin Galactic приема плащания с биткойн

Милиардерът Ричард Брандсон каза на живо по телевизия CNBC, че неговата компания за комерсиални полети в космоса ще приема биткойн като платежно средство.(21)

Университета в Кипър приема Биткойн като разплащателно средство за студентите, които искат да си платят семестриалната такса. (22)

И много други приемат биткойн като ресторанти и кафенета (http://pizzaforcoins.com/), компютри(www.dell.com)(23) и периферия (www.pcmag.bg), групово пазаруване (www.grabo.bg) и много други.

За улеснение на потребители има специализиран сайт в, в който можете да намерите местата в цял свят, където се приема виртуалната валута като разплащателно средство. Този сайт е: www.spendbitcoins.com

Копаене на биткойн

Чрез т.н. минно дело или още наричано „копане” на биткойн. – То представлява предоставянето на индивидуалната изчислителна мощ за обработка на данни и поддържане на т.н. block chain. Всеки, който го направи бива възнаграден с новосъздадени биткойни. „Миньорите: могат да бъдат разположени навсякъде по света стига да разполагат с изчислителна мощ и надежден интернет. Техните машини обработват плащания, като проверяват дали всяка сделка е валидна и я добавя към block chain-а.(24). Информацията за обработка се разделя на отделни блокове и за 2014 обработката на дин блок се възнаграждава с 25 биткойна. На всеки 4 години наградата се намаля наполовина и така докато бъде достигнат последния биткойн (те са строго ограничени до 21 милиона) през 2140г. От 2013 г насам минното дело се превърна в много конкурентно дело. Внедрява се специализирана технология издяла съсредоточена в копането на биткойни. Най-добрата технология за целта е т.н. application-specific integrated circuits (накратко ASIC процесорите), която става единствено и само за тази цел и за нищо друго.(26) В началото на тази т.н криптовалутна революция е било възможно и с настолен компютър да се „копае”, но в днешни времена ако не се използват тези строго специализирани машини, индивида няма да може да си покрие разходите за ток и няма да изкопае нищо(27)

Шансовете да изкопаете биткойн самостоятелно са много малки, затова хората се групират в т.н. „миньорски басейни”. По този начин група хора обединяват изчислителната си мощ и копаят заедно като после изкопаното се разделя пропорционално на това, кой с колко мощност е участвал(28). Дори и участвайки в тези басейни, консумираната електрическа енергия си остава огромно перо от разходната част.(27)

Механика на биткойн копането.

В по-долните редове ще обясня термини като: значението на “proof of work”, „трудността на веригата”, хеширане, копане и изкопаване. Все важни термини от същността на биткойн феномена.

Криптографски хеш-функции

Те са съществена част от Биткойн протокола. Казано накратко – хеш-функцията е математически алгоритъм, който преобразува входен масив от данни в изходен низ (или поредица от символи). Да предположим например, че имаме алгоритъм, който събира всички цифри на дадено число. Ако числото е 1234, алгоритмът ще ни върне изходен низ 10.

1234 ==> 10

Изглежда просто, но има определени характеристики на **добрите хеш-функции**, които ги правят подходящи за използване в криптографията. Имайте ги предвид, защото те са **жизненоважни за функционирането на Биткойн протокола**.

Изчисляването на хеша за каквито и да са входящи данни трябва да е **лесна задача,** но също така да е невъзможно (предвид съвременното ниво на компютрите) да изчислите входящите данни, ако имате хеша им, дори и да знаете математическия алгоритъм, използван за хеширане. В този смисъл, погледнете горния пример – можем да сметнем, че хешът е 10 при входен масив 1234, но обратната сметка не е толкова лесна. В нашия случай съществуват много възможни стойности, които да върнат същия изходен резултат, например 55, 136, 7111 и други. Предвид простотата на функцията ни обаче, всеки може лесно да налучка началния масив. Хеш-функциите, ползвани в индустрията обаче, са толкова сложни, че не могат да бъдат разбити дори и от квантови компютри (не и в разумен срок и срещу приемливи разходи).

За разлика от примера ни, всеки хеш трябва да отговаря на точно един входящ масив от данни. Ако два различни начални масива дават един и същ хеш като резултат, имаме хеш колизия (от англ. hash collision). Добрите криптографски хеш-алгоритми нямат този проблем.

Хеш-функцията трябва да може да работи с входни масиви с различен размер и съответно да връща изходен низ с фиксиран размер. Например:

———————————————————-

hello ==>
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824go
odbye ==>
82e35a63ceba37e9646434c5dd412ea577147f1e4a41ccde1614253187e3dbf9

———————————————————-

Полученият хеш трябва да има една и съща дължина, независимо дали началната стойност е с размер 10 или 10 000 знака.

Малка промяна във входящия масив трябва да даде напълно различен хеш, който по никакъв начин не е свързан с хеша от първоначалния вариант на входящия масив. Например вижте как съвсем леки промени в изписването на еднаквото по значение „Hello World“ се отразява на хеша на този израз:

———————————————————-

hello world ==> 98c615784ccb5fe5936fbc0cbe9dfdb408d92f0f
Hello World ==> a830d7beb04eb7549ce990fb7dc962e499a27230
Hello World! ==> 8476ee4631b9b30ac2754b0ee0c47e161d3f724c
Hello, World ==> 6782893f9a818abc3da35d745a803d72a660c9f5

———————————————————-

Биткойн използва криптографската хеш-функция SHA256 (от англ. Secure Hash Algorithm 256-bit). Тези алгоритми са разработка на Агенцията за национална сигурност (NSA) на САЩ. Предполагам, че си задавате въпроса, дали можем да се доверим на нещо създадено точно от тях? Да, това наистина е повод да сме подозрителни, но истината е, че алгоритмите

са публични и са анализирани от стотици специалисти по криптография от цял свят, които са постигнали консенсус относно надеждността им.

Merkle trees

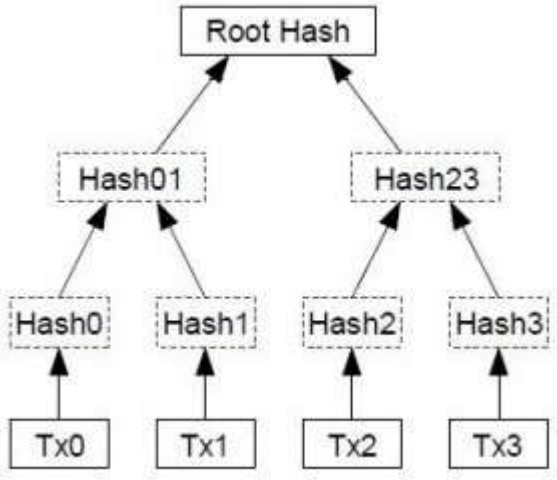
След като изяснихме основата, нека се фокусираме върху самия протокол. В първата част отбелязахме, че всички биткойн транзакции се предават до всеки от пиърите в мрежата (всеки, който си е включил клиент на биткойн или „копачка“). Копачите събират тези транзакции и извършват множество проверки, за да установят, че са валидни. Транзакциите, преминали проверките за достоверност, се добавят към масива от данни, с който копачът се стреми да изчисли новия блок във веригата и така да получи наградата от 25 биткойна. С това всъщност започва процесът по създаването на един блок. Първата стъпка е да се приложи хеш-функция (от тук нататък ще го наричаме хеширане) на всяка транзакция в басейна от данни посредством SHA256 алгоритъм. Суровият вид на данните от транзакциите изглежда така:

01000000017a06ea98cd40ba2e3288262b28638ce
c5337c1456aaf5eedc8e9e5a20f062bdf000000008a
473044022030e2d23be71a907a3ad7de846b3bbe8
886c4a839e1aa2cf0d314b1d327f12d2a022039718
fc3886a171e4ec2b138e6547b03dd326ef7f12295d
06e351e7c02010068014104e0ba531dc5d2ad13e2
178196ade1a23989088cfbeddc7886528412087f4b
ff2ebc19ce739f25a63056b6026a269987fcf538313
1440501b583bab70a7254b09effffffff01b02e052a0
10000001976a9142dbde30815faee5bf221d6688e
bad7e12f7b2b1a88ac00000000

След хеширането те приемат следния вид:

2d94683fa2f8aaae4a6f377d93b875f680adf96b9c3e9577554b742f412fa9ad

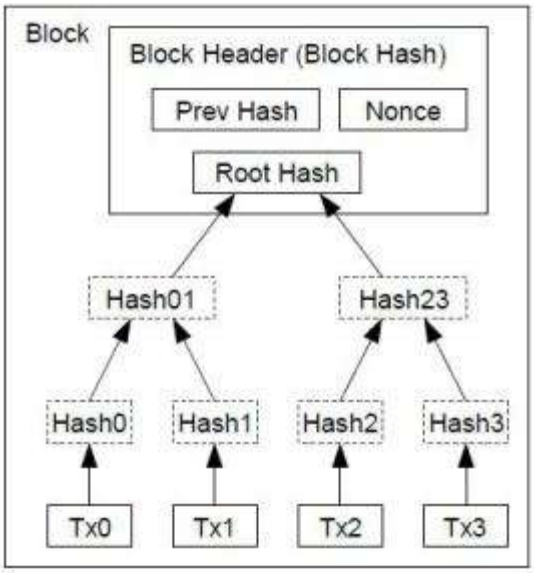
Всички хешове на транзакциите са организирани в така нареченото Merkle Tree или хеш дърво. Това дърво е подобно на турнирната схема на Шампионската лига след групите. Хешовете са организирани в групи по двойки, които се съединяват и отново се хешират. Същото се прави за всеки нов набор от двойки, докато се оформи структура подобна на дърво.



фиг.1.

Горният пример се състои само от четири транзакции (Tx0,Tx1,Tx2,Tx3), но един реален блок носи информацията за стотици транзакции, затова и дървото ще бъде доста по-голямо. Хешът на върха на дървото се нарича Merkle Root или Root Hash. Не се притеснявайте, ако до тук не разбирате защо транзакциите са организирани в подобна структура. Скоро всичко ще ви се изясни.

Root Hash-а от всички транзакции се поставя в главната част на блока заедно с хеша от предишния блок (това ще бъде разяснено по-късно) заедно с едно случайно число, нареченоNonce (също ще бъде обяснено по-късно). Главната част на блока трябва да изглежда така:



фуг.2.

Към главната част на блока се прилага хеш-функция с SHA256 алгоритъм, в следствие на което полученият хеш служи като идентификатор на блока.

Доказателство за работа (Proof of work)

Биткойн протоколът определя параметри за вида на хеша на хедъра на всеки блок. Неговият хеш трябва да бъде по-малък от предварително зададено число. Казано по друг начин, въпросният хеш трябва да започва с определен брой нули. Примерно един валиден хеш може да изглежда така:

000000000000002e9067f1cf7252333f7aeb619c89d220985a70ac0e015248e0

Всеки блок, чийто хеш в хедъра не започва с указания брой нули, ще бъде отхвърлен от мрежата. Броят на нулите се променя динамично от протокола на всеки две седмици в опит да поддържа средно време за откриване на блок от 10 минути. От тук идва и терминът „трудност на мрежата“: колкото повече нули се изискват, толкова по-висока е трудността за копаене.

Така, да преговорим как създаваме валиден блок като копачи: проверили сме за достоверност всички получени от нас транзакции,

подредили сме ги в Merkle Tree, открили сте Root Hash-а на това дърво, добавили сме го в хедъра на блока, заедно с хеша на предишния блок и Nonce число.

Тук идва ролята на въпросното число – Nonce. В случая то е просто случайно число, добавено в главната част на блока, с цел да увеличаваме неговата стойност в опит да открием валиден хеш, започващ с определения брой нули. Ако първият опит за създаване на валиден хеш се провали, просто добавяме единица към него и създаваме нов хеш, като отново проверяваме дали той е валиден. Да предположим например, че искаме да намерим хеш-а на “Hello, world!” така, че той да съдържа най-малко три нули в началото. Ако получим хеш, който не отговаря на условието, добавяме единица към стойността на Nonce и хешираме отново.

„Hello, world!0″ =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
„Hello, world!1″ =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
„Hello, world!2″ =>
ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
…
„Hello, world!4248″ =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
„Hello, world!4249″ =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
„Hello, world!4250″ =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Този пример ни отне 4251 опита в търсенето на такава стойност на Nonce, която присъединена към “Hello, world!” да върне изходящ низ, започващ най-малко с три нули. Обърнете внимание, че целият блок с транзакциите не се пресмята отново с всеки опит. Това е съществено за Биткойн копаенето – хешираме само хедъра на блока, отново и отново,

докато някой миньор в мрежата успее да създаде валиден хеш, започващ с толкова нули, колкото изисква трудността на мрежата към този момент.

Копачите просто предават блока на всеки от останалите пиъри в мрежата. Всички останали миньори проверяват работата му, за да се уверят, че тя е валидна. Ако нямат забележки, те добавят новия блок в локалното си копие на публичната книга (блок-веригата) и започват да приемат транзакции за съставянето на следващия блок и да се състезават с надеждата, този път те да имат късмета да намерят заветния хеш първи.

В зората на Биткойн миньорите са извършвали изчисленията на базата на SHA256-алгоритъма посредством процесорите на техните компютри. Колкото повече хешове в секунда можете да изчислите, толкова по-голям е шансът да "изкопаете" блок и да спечелите съответната награда. Копаенето с процесори бързо отстъпи място на това с видеокарти, които се оказаха доста по-ефективни в изчисленията. Съвременните миньори използват специализиран хардуер – ASICs (application specific integrated circuits), за да копаят биткойни. Тези устройства представляват създадени специално за целта компютърни чипове, които са проектирани да изпълняват SHA256 изчисления и нищо друго. Не е рядкост да видите миньор, който притежава изчислителна мощ от над един трилион хеша в секунда (един терахеш – 1 TH/s). Към момента (02.2014) общата изчислителна мощ на мрежата е 2.61 петахеша в секунда (2.61 PH/s).

Значението на Coinbase транзакцията

Първата транзакция във всеки блок се нарича "coinbase" транзакция. Това е транзакция, при която миньорът изпраща на себе си 25 биткойна, създадени "от нищото". Тъй като всеки миньор прави това към собствения си адрес, първата транзакция във всеки блок ще се различава за всеки миньор. Припомнете си характеристиките на криптографската хеш-функция: най-малката промяна във входящия масив води до напълно различен хеш. Тъй като хешът на "coinbase" транзакцията в основата на Merkle trees е

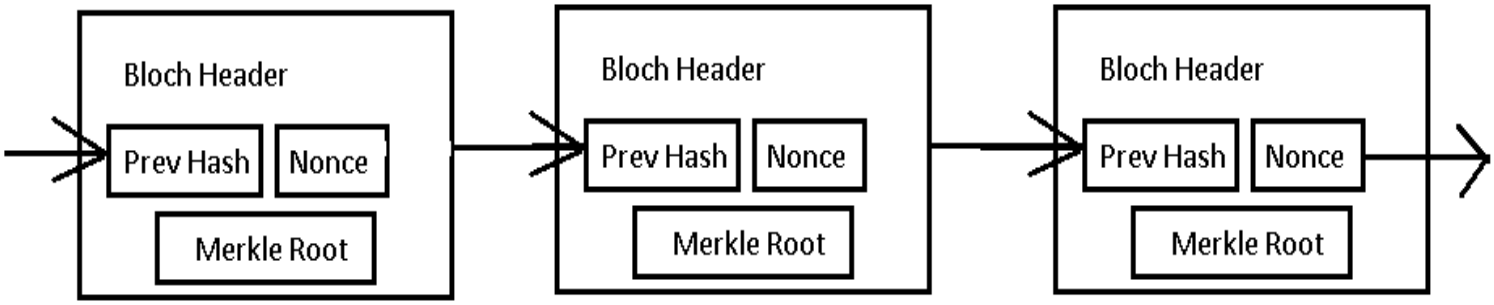
различен за всеки миньор, следователно и цялото Merkle tree, включително и Root Hash-а ще бъде различен за всеки миньор. Това значи, че стойността на Nonce, необходима за пресмятането на валиден блок, също ще бъде различна за всеки миньор. Така всеки спокойно може да почне с nonce=1 и да го увеличава, като знае, че математически не губи нищо спрямо другите. Ако даден компютър прави два пъти повече операции в секунда от друг, то вероятността той да намери първи хеш на блока с определения брой нули, е два пъти по-голяма.

Смисълът на Merkle Tree

Каква е идеята зад Merkle Tree? Хедъра на дървото случи като уникален подпис на всички съдържащи се транзакции в него. Би било възможност да се търси хеш на всички транзакции плюс nonce плюс хеша от предния блок, но това би било огромно количество данни за изчисляване на всеки хеш. Тъй като хедъра на Меркле дървото играе ролята на уникален идентификатор на транзакциите в него, се използва само хедъра за входящ параметър, който да представя всички транзакции. Разбира се, когато някой изкопае блок и го предостави на другите в мрежата, всеки един проверява, дали новото дърво е конструирано правилно според принципите на Merkle.

Хеш верига

Хешът на един блок е включен в главната част на всеки следващ. Схематично това изглежда така:



фиг.3.

Ако злонамерен потребител иска да подправи или премахне транзакция, която вече е в блок-веригата, промяната ще доведе до това, че хешът на транзакцията ще създаде промени по целия път нагоре до Merkle Root-а. Практически е невъзможно ново-полученият хедър да създаде валиден хеш (доказателство за работа). От тук следва, че нападателят ще има нужда да пресъздаде (изчисли хешовете) на целия главен блок и да изгуби огромно количество време, за да открие точната стойност на Nonce. Но нека предположим, че това се случи. Може ли той обаче да излъчи подправения блок в мрежата и да се надява, че миньорите ще заместят стария такъв с новия, или че новите потребители ще изтеглят подправения блок? Отговорът е не. Причината за това е, че хешът на всеки блок е включен в главната част на следващия. Ако нападателят промени блок номер 100, това ще доведе до промяна в главната част на блок 101, което от своя страна ще доведе до промяна на главната част на блок 102 и т.н., по целия път на блок-веригата. Всеки опит за промяна на съществуваща транзакция в блок-веригата изисква не просто промяна на блока, съдържащ транзакцията, но и промяна на всички следващи блокове. В зависимост от това, колко назад във веригата е една сделка, това може да отнеме на атакуващия седмици, месеци или дори години, за да промени цялата останала част от блок-веригата. Както споменах и в първата част, докато нападателят не контролира по-голямата част от изчислителната мощ на мрежата, останалата част от нея ще добавя нови блокове в основната верига по-бързо, отколкото той ще може да добавя в подправената верига. Това гарантира, че легитимната верига остава най-дълга, а веригата на нападателя се игнорира.

Шест потвърждения

Единственото изключение от това правило е случая, в който злонамереният нападател има късмет. Както знаем, трудността на мрежата се регулира така, че да отнема средно 10 минути, за да се намери валиден

блок. Следователно, на един нападател, който държи 10% от мрежата, са нужни средно 100 минути, за да намери валиден блок (или 200 минути при 5% и т.н.), но това са средни стойности. Теоретично е възможно нападателят да има късмет и да уцели блок в рамките на минута, дори когато са му нужни средно 100. Ако този блок съдържа двоен харч, тогава е възможно фалшивата транзакция да се включи в блок-веригата, а легитимната такава да бъде отхвърлена (мрежата ще приеме, че легитимната сделка е двоен харч). Колкото по-назад в блок-веригата е една транзакция, толкова повече пъти атакуващият системата трябва да има късмет и да изкопае блок преди останалата част от мрежата, за да разшири веригата си повече от основната. От гледна точка на вероятностите, шансовете за такава атака намаляват експоненциално с всеки следващ блок. Това е равносилно на печалба от лотарията няколко пъти подред. В представянето на идеята си Сатоши Накамото изчислява вероятностите нападателят да успее да направи двоен харч. В следващата таблица Q е процента от цялата мрежа, която контролира потребителя, а P е вероятността той да замени Z брой блокове.

q=0.1
z=0 P=1.0000000
z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173
z=9 P=0.0000046
z=10 P=0.0000012

q=0.3

z=0 P=1.0000000

z=5 P=0.1773523

z=10 P=0.0416605

z=15 P=0.0101008

z=20 P=0.0024804

z=25 P=0.0006132

z=30 P=0.0001522

z=35 P=0.0000379

z=40 P=0.0000095

z=45 P=0.0000024

z=50 P=0.0000006

Solving for P less than 0.1%…P < 0.001

q=0.10 z=5

q=0.15 z=8

q=0.20 z=11

q=0.25 z=15

q=0.30 z=24

q=0.35 z=41

q=0.40 z=89

q=0.45 z=340

Може да се види, че атаки с дял 10% от мощността на мрежата ще имат шанс за успех 0.024% и затова е препоръчително, ако продавате нещо скъпо да изчакате транзакцията да е отразена шест блока назад във веригата или казано накратко – да имате шест потвърждения преди да предадете стоката.(39)

Биткойн портфейл.

За да можете да станете собственик на биткойни трябва да имате т.н. биткойн портфейл. Това е мястото, където се съхраняват (складират) вашите електронни пари.(29). Чрез този портфейл можете да пращате или да получавате биткойни. Архитектурата на биткойна използва т.н. криптографски ключове: един публичен, чрез който се идентифицира вашия портфейл (нещо като адрес, на който може да се пращат средства) и един личен, чрез който вие можете да пращате и който удостоверява, че вие сте собственика на въпросния портфейл. (30)

Предимства на биткойна

Лесен трансфер на средства

Изключително лесно и евтино се прехвърлят средства до всяка точка на света. Достатъчно е да имате компютър и интернет за да можете да превеждате биткойни. За разлика от банките тук няма комисионни за банката понеже прехвърлянето става от човек на човек без посредник.

Не може да бъде конфискуван

За да бъде отнет от собственика трябва да бъдат придобити двата ключа и без тяхната наличност не може да се оперира с електронния портфейл.(31)

Анонимност

Могат да се извършват покупки на продукти с пъна анонимност Електронния портфейл е напълно анонимен и трансфера на средства от и към него не изисква: име, подпис или други лични данни. Нужно е само и единствено идентификационния ключ, който показва адреса където да

бъдат пратени средствата. Точно поради това му качество, биткойна се смята за средство, чрез което могат да се извършват криминални дейности.(32). През октомври 2013 ФБР затваря сайта: www.silkroad.com, чрез който са се продавали оръжия, наркотици и други забранени стоки само и единствено чрез биткойн като разменно средство. Тогава ФБР замразяват 144 000 биткойна на стойност по тогавашната му цена 28,5 милиона долара (33)

Недостатъци на биткойна

Скъпоструваща техника

Закупуването на специализирана техника за копане на биткойни е изключително скъпо начинание, като цената на днешните машини е около 10000 долара.

Разход на електроенергия

Използването на такава машина води до огромни разходи за ток и в много от случаите е възможно тя да работи на загуба. Печалбата се изчислява по следната формула: брой изкопани биткойни умножени по моментната цена и от резултата се изваждат разходите за закупуване на специализирания хардуер и разходите за електричество.(27)

Биткойните са апетитни за хакери

Биткойните са апетитни за хакери и могат да бъдат откраднати заедно с ключовете и да бъдат продадени без дори да се усетите.

Висока ликвидност

Високата им ликвидност може да изиграе лоша шега на инвестиралите в това средство, тъй като цената се мени изключително бързо и в двете посоки. При това положение е възможно инвеститора да е закупил биткойн на дадена цена и след ден два цената да се срути и да загуби голям процент от себестойността му.

Възможности, които предоставя биткойна

Начин за избягване на инфлацията

Чрез него може да се избегна инфлацията. - Те са ограничен брой (21 милиона) и не може да се генерират нови за разлика от парите, които просто биват напечатани ниви.

Средство за безконтактни плащания.

В днешно време технологията се е развила до такива нива, че може да си инсталирате електронен портфейл на смартфона и по този начин биткойните Ви са на ваше разположение навсякъде по света където ги приемат, а тези места с всеки изминал ден стават все повече и повече.

Край на финансовата система

Възможно е биткойна да сложи край на финансовата система, такава каквато я познаваме днес. - Всеки сам ще си е банка и ще

разполага със средствата си и ще може да праща където си поиска без комисионни и други подобни разходи. С една дума биткойна може да донесе свобода каквато не ни е понятна до този етап от развитието на човечеството.

Мнения на обществото за биткойна.

Обществото се дели на 2 отбора. Едните защитават това явление и са напълно положително настроени спрямо него, а другите са точно обратното.

Положителни възгледи.

- Бившия вече председател на федералния резерв на Америка Бен Бернанке се изказва положително по въпроса за съществуването на биткойна със следните думи: „Биткойна притежава положителни черти и е възможно да има добро бъдеще в дългосрочен план, стига тази иновация да представи по-бърза и по-сигурна и по-ефективна система за разплащания”(34)
- Joe Weisenthal от Business Insider: „ Биткойните са по-портативни(преносими), отколкото куфарче пълно със $100 банкноти или диаманти. Значи има някаква полза. И въпреки че мисля, че инфлационната параноя е тъпа, със сигурност е истински феномен. И всичко, което може да направи златото, Биткойна може да го направи по-добре. Всъщност комбинираме контрабандната полезност на парче хартия със снимка на Бен Франклин, със свойствата на златото да хеджира инфлацията. Това е добро постижение. Но няма да подпали светът. „(35)

Отрицателни възгледи.

- Ако хората започнат масово да използват биткойн, дигиталната валута ще остане в историята като разрушител на долара. Това заяви бившият американски конгресмен Рон Пол, цитиран от CNN.

„Някои институции ще загубят бизнеса си, ако хората спрат да използват техните системи за разплащане. Централните банки, като Федералния резерв на САЩ, ще загубят способността си да забавят и ускоряват икономическата активност. Правителствата искат абсолютен монопол върху парите и кредитирането. Те няма да се откажат лесно"(36)

- Цената на нашумялата напоследък виртуална валута биткойн е неустойчиво висока. Това заяви в интервю пред Bloomberg Алън Грийнспан, председател на Федералния резерв на САЩ в периода 1987-2006 г.

"Не мога да разбера откъде идва подкрепата за биткойните. Това е един балон. Валутата трябва да има истинска стойност. Трябва наистина да разгърнете въображението си, за да достигнете до извод каква е истинската стойност на биткойните. Аз не съм в състояние да го направя, може би някой друг може", отбеляза 87-годишният бивш ръководител на щатската централна банка. (37)

Фундаментален анализ на цената на биткойна.

Както знаем, цената на всеки (свободен) пазар се определя от търсенето и предлагането. Ето четири основни фактора, които влияят на двете страни на уравнението.

Търговците въвеждат биткойн много по-бързо от потребителите

Броят на търговците, приемащи плащания с биткойн, се е увеличил с пет до десет пъти през последните шест месеца – нещо, което едва ли може да се каже за броя на „потребителите“. Това е важно за кръговрата в екосистемата на биткойн…

Вие сте си купили 1 биткойн от борсата. По този начин вие сте увеличили глобалното търсене макар и с пренебрежимо малко. После ги ползвате за покупка на нещо от някой търговец. Този търговец обаче ползва услугите на bitpay.com или coinbase.com, които са нещо като Visa и MasterCard на биткойна. Вие пращате вашия биткойн на тях, те веднага го продават на борсата (или на друг желаещ да си купи биткойн в случая с coinbase.com), за да могат да изплатят доларите на търговеца. Защото търговецът не е инвеститор в биткойн, той го ползва, за да си **увеличи продажбите** в долари, с които купува стоката си, плаща наема и заплатата на работниците си. Така че, макар да увеличавате **мрежовия ефект за биткойн** когато харчите биткойн (нещо много полезно в дългосрочен план), вие де факто допринасяте за увеличено предлагане на биткойн по борсите, което води до по-ниски цени, както при всеки пазар. Така че, в крайна сметка, нетното повишено търсене на биткойни се равнява на количеството койни, които са купени с инвестиционна цел.

Загубата на инерция в цената

Когато цената тръгна нагоре в края на 2013 множество спекуланти влезнаха на пазара с цел „инвестиция“ или по-скоро бърза и лесна печалба. Негативните новини (най-вече от Китай) обаче пукнаха балона и „оптимистичните“ инвеститори стават все по-голямо малцинство спрямо тълпата сочеща ги с думите „Казвахме ли ви?“.

Макар и лошо за цената в краткосрочен аспект, това е добро развитие за биткойн фундаментално, тъй като ще държи спекулантите и слабо-информираните за същността му потребители настрана. А те не са ни нужни,

защото ще продадат при първите признаци на „паника“. Това ще позволи на биткойн да намери своето равновесие преди да тръгне плавно нагоре отново.

Третата основна сила в определянето на баланса между търсене и предлагане е тази на:

Засилваща се конкуренция при копачите

До преди година копаенето на биткойни е било easy money: **Трудността на копаене** била лесна, всеки нов блок носил 50 биткойна, а не 25 като сега, нямало нужда от инвестиции в research and development за нови, по-бързи чипове. В онези времена копачите (или майнърите, както някои предпочитат да ги наричат) покривали инвестициите си като продавали по-малко от 50% от изкопаните биткойни. В днешно време, този процент е по-скоро 90%. Това означава, че 22 биткойна отиват за продажба на пазара всеки десет минути. Това прави над 3,000 нови биткойна за продажба всеки ден – по днешни цени, този наплив се нуждае от **ново търсене за $1,200,000 всеки ден,** за да се укроти цената.
И последният, но съвсем не маловажен, фактор за намаляващата цена е

Крахът на биткойн борсите

Този крах е всъщност положителен за развитието не само на **биткойн, но и за финансовата култура в света като цяло.**

Тук обаче имаме нещо друго предвид. Хората вече не вярват на борсите – повечето от тях, които искат да си купят биткойни, предпочитат да минат по сигурния път – този на приятелите или **услугите на localbitcoins в страната им**. Но не и копачите – те нямат време да търсят купувачи там, защото едва ли могат да намерят толкова. От тук търсенето на борсите не представлява реалното търсене по света, но – забележете! – борсовата

цена е тази, според която се образуват цените в localbitcoins и при търговията между приятели. Това е много тънък, но много основен момент…

В заключение може да се каже, че цената на биткойн ще пада докато тези сили намерят своя противовес (ако се замислите, всяка от горните точки си има такъв). Къде ще е тя, никой не може да каже, само може да се надяваме да е $400. Ако има нещо, което може да направим (освен да купуваме, разбира се), е да предоставим услуги с биткойн, които са невъзможни с фиатните пари. Това сякаш изглежда не толкова лесно предвид окастрената функционалност на биткойн да изпълнява функции на чиста валута за сега, но скоро дори и в тази сфера ще се появят услуги, пред които VISA и MasterCard бледнеят. Другата надежда е, най-сетне в пазара да навлязат институционалните инвеститори – нещо, за което бе дадена **зелена светлина в САЩ наскоро**. (38)

Технически анализ на цената на биткойна.

На фиг.4. е представен техническия анализ на цената на биткойна към16.10.2014г. Този анализ не представлява препоръка за вземане на инвестиционно решение относно покупка или продажба на биткойни. Анализът е от прогнозен характер и представлява моето лично мнение и виждане за бъдещето на цената на биткойна.

Фиг. 4

На фигура 4 е изобразена графика в месечен времеви интервал и се забелязва техническата формация: възходящ триъгълник(41). Според теорията за тази формация след достигане на зоната означена в розово (400$ - 450$) би трябвало да се породи импулсивно (бъдещата вълна 5) движение нагоре. Пресичането й е агресивен сигнал за покупка, а консервативния такъв би било пресичането на цената на зелената зона (650$ - 700$) (42). Нека да погледнем последното низходящо движение. То е породено от огромна поръчка за продажба на 26000 броя биткойни(40) и на фигура 4 е изобразено с червена елипса. Това е класически момент за образува не дъно, тъй като отпада един огромен продавач и по този начин

се отключва бъдещето движение в посока на горе, поради факта, че няма да има съпротивление на това движение.

Видове криптовалути

В днешно време биткойна си остава най-популярната криптовалута, но освен нея има изключително много други. В таблицата по-долу можете да добиете представа за разнообразието от криптовалути по света.

Криптовалута	Алгоритъм	Блокове	Трудност	Награда	Цена в биткойни	борса	%печалба спрямо биткойн
Alphacoin	Scrypt	655258	1,5211	50	0.00000035	Cryptsy	1 097,32%
AmericanCoin	Scrypt	109194	2,29518	100	0.00000078	Cryptsy	3 226,54%
Anoncoin	Scrypt	85689	43,087	5	0.00064001	Cryptsy	7 083,73%
Argentum	Scrypt	424320	0,595	3	0.00000685	Cryptsy	3 291,77%
BBQCoin	Scrypt	851239	3,18723	42	0.00000214	Cryptsy	2 689,68%
BitBar	Scrypt	57967	19,827	0.15196	0.00406847	Cryptsy	2 974,10%
Bitcoin	SHA-256	316762	23 844 670 038,80300	25	1.		100,00%
Bottlecaps	Scrypt	478537	6,42085	10	0.0000128	Cryptsy	1 901,38%
Bytecoin	SHA-256	41321	1 083 454,82700	50	0.00000651	Cryptsy	28,63%
CryptogenicBullion	Scrypt	354793	0,412	0.03906	0.00015617	Cryptsy	1 412,26%
CHNCoin	Scrypt	365774	1,16422	88	0.00000087	Cryptsy	6 241,29%

Cosmoscoin	Scrypt	469399	0,48784	3.май	0.00000505	Cryptsy	3 455,65%
Craftcoin	Scrypt	133291	0,43	2	0.00000715	Cryptsy	3 169,68%
Devcoin	SHA-256	150682	14 378 873 014,30000	5000	0.00000009	Cryptsy	0,00%
Diamond	Scrypt	386228	0,939	1	0.00015671	Cryptsy	15 917,27%
DigitalCoin	Scrypt	816303	3,764	15	0.00001231	Cryptsy	4 677,35%
Elacoin	Scrypt	113803	3,56697	1.89226	0.00003425	Cryptsy	1 733,15%
Elephantcoin	Scrypt	1023712	0,21294	50	0.00000005	Coins-E	1 218,96%
Extremecoin	Scrypt	32945	13,833	1	0.000029	Bter.com	199,96%
EZCoin	Scrypt	399199	1,41995	50	0.00000045	Cryptsy	1 501,46%
Fastcoin	Scrypt	2541927	0,68127	32	0.00000059	Cryptsy	2 643,24%
Feathercoin	Scrypt	205848	107,32378	200	0.00005001	Cryptsy	8 887,89%
Franko	Scrypt	635149	0,586	0.25	0.00007276	Cryptsy	2 960,54%
Freicoin	SHA-256	65555	1 316 735,06922	189.83965	0.00000356	Cryptsy	48,89%
GoldCoin	Scrypt	173351	7,78798	45	0.00001652	Cryptsy	9 101,85%
Grandcoin	Scrypt	390357	3,50423	1000	0.00000009	Cryptsy	2 313,54%
HoboNickels	Scrypt	850881	8,687	5	0.00005178	Cryptsy	2 842,40%
Infinitecoin	Scrypt	1207226	0,076	64	0.00000001	Cryptsy	803,19%
IXCoin	SHA-256	205959	5 793 008 186,04100	96	0.00005749	Cryptsy	0,09%
Joulecoin	SHA-256	486283	29 825,29243	16	0.0000011	Cryptsy	56,13%
Junkcoin	Scrypt	161742	8,672	50	0.0000005	Cryptsy	275,85%
Litecoin	Scrypt	575917	8 549,63732	50	0.01141	BTC-e	6 364,43%
Luckycoin	Scrypt	303200	2,831	44	0.0000016	Cryptsy	2 364,42%
Megacoin	Scrypt	211506	34,73814	25	0.00006502	Cryptsy	4 462,71%

Mincoin	Scrypt	352222	5,70774	2	0.00002826	Cryptsy	944,47%
Neocoin	Scrypt	288002	2,08013	29	0.00000202	Cryptsy	2 686,02%
Nybble	Scrypt	43411	7,19572	50	0.00000055	Cryptsy	366,22%
Noirbits	Scrypt	112650	21,13769	20	0.00000522	Cryptsy	471,08%
Novacoin	Scrypt	98309	349,42536	сент.42	0.00195	BTC-e	5 013,98%
RoyalCoin	Scrypt	49265	1,69175	100	0.0000008	Cryptsy	4 510,30%
OpenSourcecoin	SHA-256	370266	57 874,19331	4	0.00000195	Cryptsy	12,86%
Orbitcoin	Scrypt	677778	0,381	1	0.00004638	Cryptsy	11 610,81%
PPCoin	SHA-256	113465	162 651 434,84600	88.54053	0.00184	BTC-e	95,53%
Phoenixcoin	Scrypt	331928	0,91	50	0.00000082	Cryptsy	4 284,80%
Philosopherstone	Scrypt	193527	21,70977	32	0.00001506	Cryptsy	2 116,54%
Redcoin	Scrypt	406707	6,10665	50	0.00000061	Coins-E	473,44%
Sexcoin	Scrypt	672148	1,83546	100	0.00000126	Cryptsy	6 521,55%
Spots	Scrypt	95776	10,84119	49	0.00000066	Cryptsy	285,14%
Stablecoin	Scrypt	493013	0,557	25	0.00000114	Cryptsy	4 869,54%
Starcoin	Scrypt	129451	0,68769	100	0.00000008	Cryptsy	1 109,55%
Terracoin	SHA-256	305537	1 340 065,43300	20	0.00005045	Cryptsy	71,82%
Tigercoin	SHA-256	275257	294 438,56651	128	0.00000061	Cryptsy	25,18%
Unobtanium	SHA-256	396724	457 401,81300	0.5	0.00318991	Cryptsy	332,58%
Zetacoin	SHA-256	1186421	38 313,47077	3.90625	0.00001655	Cryptsy	160,98%
Betacoin	SHA-256	124994	223 094,67600	128	0.0000012	Cryptsy	65,50%
Dogecoin	Scrypt	344960	856,61	125000	0.00000025	Cryptsy	3 479,51%

eMark	SHA-256	166439	362 517,83766	50	0.00000286	Cryptsy	37,58%
Earthcoin	Scrypt	287515	14,532	10000	0.00000003	Cryptsy	1 969,01%
GlobalCoin	Scrypt	300011	0,768	100	0.00000065	Cryptsy	8 072,41%

Таблица 3

Заключение

- В днешно време с развитието на технологиите, криптовалутите стават все по-популярни и използваеми.
- Цената на биткойна зависи от търсенето
- Той ще продължи да съществува до тогава, докато има разменна стойност (докато за него могат да се закупуват стоки и услуги)
- С оглед на това, че все повече хора и организации приемат биткойна като разплащателно средство се стига до извода, че и цената му евентуално би нараснала в близко бъдеще.
- Единствено глобална забрана на биткойна би довела до неговото заличаване и спиране от обръщение.
- Поради факта, че той се води децентрализирана валута се стига до извода, че няма кой да го забрани в глобален мащаб.
- Докато има хора, които да го ползват той ще съществува.

Л И Т Е Р А Т У Р А

1. Ron Dorit; Adi Shamir (2012). "Quantitative Analysis of the Full Bitcoin Transaction Graph". Cryptology ePrint Archive.
2. "Bitcoin: A Peer-to-Peer Electronic Cash System". bitcoin.org. October 2008.
3. Davis, Joshua. "The Crypto-Currency: Bitcoin and its mysterious inventor.". The New Yorker
4. "Regulation of Bitcoin in Selected Jurisdictions". The Law Library of Congress, Global Legal Research Center. January 2014.
5. Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency". Daily Tech. 12 June 2011.
6. "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy". fincen.gov. Financial Crimes Enforcement Network. 19 November 2013..
7. Joyner, April (25 April 2014). "How bitcoin is moving money in Africa". usatoday.com. USA Today.
8. Wei Dai b-money Published at http://www.eskimo.com/weidai/bmoney.txt Nov. 1998
9. http://techcrunch.com/2013/12/05/who-is-the-real-satoshi-nakamoto-one-researcher-may-have-found-the-answer/
10. http://www.ibtimes.co.uk/articles/527078/20131203/satoshi-nakamoto-nick-szabo-bitcoin-creator-revealed.htm
11. http://blogs.wsj.com/moneybeat/2014/04/16/bitcoin-creator-satoshi-nakamoto-unmasked-again/
12. Jerry Brito and Andrea Castillo. Bitcoin: A Primer for Policymakers. // Mercatus Center. George Mason University, 2013. с. 5..
13. Накратко за това как се “добива” Bitcoin. // CFO.
14. Ho do I get Bitcoins?(For Beginners).//The bitcoin Bulletin 11. March 2011
15. Satoshi Nakamoto www. http://nakamotoinstitute.org/ 2008

16. Jerin Mathew; International Business Times; August 9 2014
17. http://www.wtcsofia.bg/novini/article/v-interpred-stc-sofija-beshe-montiran-prvijat-bitomat-v/
18. Veline Nascimento; http://dnes.dir.bg/news/rezervatzii-Bitcoin-expedia-16868757?nt=13 13.06.2014
19. http://www.economy.bg/business/view/11103/Tesla-Motors-prie-pyrvoto-si-plashtane-v-bitcoin 09.12.2014
20. http://profit.bg/news/800-bitkojna-za-luksozna-vila-v-Bali/nid-120879.html 25.03.2014
21. Matthew J. Belverde CNBC http://www.cnbc.com/id/101220710#. 22.11.2013
22. Matt Clinch CNBC http://www.cnbc.com/id/101217586 21.11.2013
23. http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing
24. Ashlee Vance (14 November 2013). "2014 Outlook: Bitcoin Mining Chips, a High-Tech Arms Race". Businessweek.
25. Ramzan, Zulfikar. "Bitcoin: What is it?". The Khan Academy.
26. Rockman, Simon (2014-01-17). "Manic miners: Ten Bitcoin generating machines". The Register.
27. Bays, Jason (9 April 2014). "Bitcoin offers speedy currency, poses high risks". Purdue Exponent. The Exponent Online.
28. Mills, Kelly (3 April 2014). "Bitcoins lose viability". The Arbiter. Boise State Student Media.
29. Villasenor, John (2014-04-26). "Secure Bitcoin Storage: A Q&A With Three Bitcoin Company CEOs". forbes.com. Forbes.
30. Bitcoin: Bitcoin under pressure". The Economist. 30 November 2013.
31. Благовест Белев в ефира на Bulgaria On Air, управител на „Tavex”
32. Tracy, Ryan (5 November 2013). "Bitcoin Comes Under Senate Scrutiny". The Wall Street Journal.
33. Andy Greenberg (23 October 2013). "FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road" (blog). Forbes.com.
34. Steven Perlberg, BERNANKE:Bitcoin May Hold Long-Term Promise, Business Insider 18 november 2013

35. Tymothy B. Lee, The Washington, 3 Post December 2013
36. Jose Pagliery, Ron Paul:Bitcoin could ‘destroy the dollar’, CNN Money, 4 December 2013
37. Jason Farrell, Alan Greenspan: Bitcoin is a bubble, Daily Reckoning, 5 December 2013
38. David Mondrus, Searching for the True Value of a Bitcoin, Bitcoin Magazine, 8 april 2014
39. Spas Vutov, Механика на биткойн копането, www.hash.bg , 21.08.2014
40. Daniel Harrison, www.coindesk.com, 06.10.2014
41. Venzen Khaosan, www.cryptocoinnews.com, 05.10.2014
42. Glenn Neely, Mastering Elliott Waves. Presenting the Neely Method: The first Scientific, Objective Approach to market Forecasting with the Elliott Wave Theory, Published by Windsor Books for the Elliot Wave Institute, 1990