Техническо описание на работата на Биткойн

Въведение

Биткойн е първата децентрализирана криптовалута, създадена през 2009г. от анонимния разработчик или група от разработчици под псевдонима Сатоши Накамото. Основната иновация на Биткойн е неговата възможност да предлага цифрови транзакции между потребители без необходимостта от посредник като банка или друга финансова институция. Тази възможност е осъществена чрез използването на блокчейн технология, механизъм за децентрализиран консенсус, известен като Proof of Work (PoW), и криптографски алгоритми. Всеки участник в мрежата може да валидира транзакции, да изпраща и получава биткойни, което прави системата устойчива на цензура и същевременно сигурна.

Криптография и децентрализация

Основното за децентрализацията на Биткойн е използването на публична и частна криптография, която осигурява сигурността на транзакциите и защитава участниците в мрежата. Публичните ключове действат като адреси за получаване на средства, докато частните ключове служат за подписване на транзакции, доказвайки собствеността на средствата, без да разкриват идентичността на собственика. Комбинацията от криптография и Proof of Work гарантира, че участниците в мрежата могат да валидират транзакциите, като същевременно поддържат сигурност и консенсус без нуждата от централен орган.

1. Нодове (Възли)

В Биткойн мрежата нодове, или възли, са машини (компютри) или устройства, които изпълняват софтуера на Биткойн и играят критична роля за поддържане на мрежата да бъде децентрализирана. Всеки нод може да бъде независим участник, който съхранява,

валидира и разпространява транзакции и блокове. Има два основни типа нодове:

Пълни Нодове (Full Nodes)

Пълните нодове са гръбнакът на Биткойн мрежата. Те съхраняват пълното копие на блокчейна – всеки блок и всяка транзакция от началото на мрежата. Техните основни функции включват:

- **Валидиране на транзакции и блокове**: Пълните нодове проверяват дали транзакциите са валидни, т.е., дали изпращачът разполага с необходимите средства (чрез UTXO модела) и дали подписите съответстват на частните ключове.
- **Поддържане на консенсус**: Всеки пълен нод проверява всички нови блокове спрямо правилата на мрежата (например: дали блокът спазва трудността, дали не съществува двойно харчене).
- **Разпространение на информация**: Когато един нод валидира блок, той го предава на останалите нодове, създавайки децентрализиран механизъм за синхронизация.

Ролята на пълните нодове в сигурността

Тъй като пълните нодове съхраняват пълната история на блокчейна, те предотвратяват атаки като двойно харчене (double spending). При опит за извършване на двойно харчене, пълните нодове ще отхвърлят втората транзакция, защото тя ще се базира на UTXO, което вече е използвано. Когато нова транзакция бъде направена от някой потребител, тя отива в mempool - списъка със непотвърдени (чакащи) транзакции, от който миньорите взимат и опитват да ги валидират.

Леките Нодове (SPV - Simplified Payment Verification)

Леките нодове не изискват пълно копие на блокчейна, а съхраняват само заглавията на блоковете и използват пълни нодове за валидиране на транзакциите. Те проверяват дали дадена транзакция е включена в блок чрез меркел доказателства (Merkle Proofs), без да съхраняват всички транзакции.

- **Спестяване на ресурси**: SPV нодовете не се нуждаят от съхранение на цялата блокчейн база данни, което ги прави подходящи за мобилни устройства и приложения, които се стремят да минимизират трафика и съхранението.

- **Зависимост от пълни нодове**: Тези нодове разчитат на пълните нодове за предоставяне на валидирани данни, но въпреки че теоретично са по-уязвими на атаки, те остават достатъчно сигурни за повечето потребители.

2. Миньори и Процесът на Копаене (Mining)

Миньорите са основните участници, които осигуряват сигурността на Биткойн мрежата, като създават нови блокове и добавят нови транзакции към блокчейна. Те използват специализирано оборудване (ASIC) за решаване на сложни криптографски задачи чрез Proof of Work (PoW).

Алгоритъмът Proof of Work

Миньорите трябва да намерят специфична стойност, наречена "nonce", която, когато се комбинира с информацията от блока (включително хеша на предходния блок), генерира нов хеш чрез алгоритъма SHA-256, който отговаря на текущата трудност на мрежата. Тази задача изисква значителна изчислителна мощност и случайно търсене на правилния nonce чрез многократни хеширания. Хешът на блока трябва да отговаря на зададената цел на трудността, която се настройва на всеки 2016 блока.

ASIC и Еволюция на Оборудването

Първоначално миньорите използваха обикновени процесори (CPU) за копаене на Биткойн, но с времето алгоритъмът се усложни и потребителите преминаха към използването на графични процесори (GPU), които са по-подходящи за паралелни изчисления. Днес ASIC (Application-Specific Integrated Circuits) устройства са стандартът в индустрията, тъй като те са специално проектирани да извършват SHA-256 хеширания много по-бързо и ефективно от универсалните процесори.

Мрежови трудности и консенсус

Миньорите играят важна роля в процеса на консенсус. Всеки нов блок трябва да бъде валидиран и добавен към блокчейна чрез консенсус на всички пълни нодове. Миньорите също така формират

защитен слой, тъй като процесът на копаене изисква огромни ресурси, което прави атаките срещу мрежата (като "51% атака") много трудни и скъпи.

3. Механизъм на Трудността

Механизмът на трудността е съществен компонент на Биткойн, който автоматично регулира сложността на задачата за копаене, за да поддържа средно време за създаване на блокове от 10 минути. Трудността се настройва на всеки 2016 блока (приблизително на всеки две седмици).

Регулиране на трудността

Трудността се определя от времето, необходимо за генериране на предишните 2016 блока. Ако блоковете са били създадени по-бързо от очакваното (по-кратко от 10 минути на блок), мрежата автоматично увеличава трудността. Ако са били генерирани по-бавно, трудността намалява. Формулата за регулиране на трудността е следната:

$$\text{Трудност} = \text{Предишна трудност} \times \frac{\text{Време за 2016 блока}}{\text{Целево време (20160 минути)}}$$

Този адаптивен механизъм е може би най-новаторската част в протокола и е от съществено значение за запазването на консенсуса в мрежата и предотвратяването на прекомерно увеличаване на новосъздадените биткойни.

Връзка между хеширащата мощност и трудността

Важен аспект на трудността е динамичната ѝ връзка с наличната хешираща мощност (hashrate) в мрежата. Хеширащата мощност представлява сумарната изчислителна мощност, която всички миньори използват, за да генерират нови блокове. При увеличение на хеширащата мощност (например при добавянето на нови миньори в мрежата), броят на хеширащите опити се увеличава, което води до по-бързо намиране на нови блокове. За да се възстанови равновесието и да се поддържа време от около 10 минути за създаване на блок, трудността на мрежата се увеличава. Ако

хеширащата мощност намалее, трудността също ще намалее, за да гарантира, че мрежата ще продължи да функционира при зададените условия.

Това динамично регулиране гарантира устойчивостта на Биткойн мрежата, като предпазва от неравномерни скорости на добив на нови блокове, които биха могли да доведат до инфлационен ефект върху общата емисия на Биткойн.

Значението на консенсусния алгоритъм

Механизмът на трудността в комбинация с Proof of Work прави Биткойн мрежата устойчива срещу атаки като "51% атака", при която даден участник би опитал да контролира мнозинството от хеширащата мощност. За да извърши успешна такава атака, участникът би трябвало да контролира над 50% от изчислителната мощност на мрежата, което би било изключително трудно и скъпо поради нарастващата трудност (вече непосилно дори за държави като САЩ и Китай). Дори ако такъв опит бъде направен, миньорите, които работят в съответствие с правилата на мрежата, биха могли да отхвърлят този потребител от нея и да запазят консенсуса.

4. Блокове и Блокчейн

Структура на блока

Всеки блок в Биткойн съдържа няколко основни компонента:

- **Заглавие на блока (Block Header)**: Заглавието съдържа основна информация за блока, включително хеш на предходния блок, времеви печат (timestamp), nonce и корен на Меркъл дървото (Merkle Root).
- **Меркъл Дърво (Merkle Tree)**: Структурата на Меркъл дървото позволява на Биткойн да проверява дали дадена транзакция е включена в блок без необходимостта от цялата транзакционна информация. Всяка транзакция се хешира, след което се комбинира с друг хеш в двойка, докато не се получи единичен корен хеш – Merkle Root.
- **Транзакции**: Това е основната част от блока, съдържаща всички транзакции, които са били потвърдени от миньорите и включени в този блок.

Хеш на блока и верига от блокове

Всеки блок верифицира предходния блок чрез неговия хеш. Този хеш се генерира на базата на информацията от заглавието на предишния блок, което създава непрекъсната верига от блокове, която може да бъде проследена чак до първия блок, известен като "генезисния блок". Тази верига от хеширани блокове е това, което гарантира неизменността на Биткойн блокчейна – всяка промяна в информацията на даден блок би променила неговия хеш и следователно би нарушила цялата последователност от блокове, което прави опитите за подправяне на данни практически невъзможни.

Потвърждения на блоковете

Когато дадена транзакция се включи в блок, тя се счита за потвърдена веднъж, но сигурността на тази транзакция нараства с всеки следващ блок, който е добавен към веригата. Обикновено се смята, че транзакция е "сигурна" след шест потвърждения, тъй като вероятността някой да модифицира блок с всяко следващо потвърждение спада експоненциално.

5. UTXO Модел (Unspent Transaction Output - непохарчен транзакционен изход)

Биткойн използва UTXO модела за управление на транзакциите и баланса на потребителите. Всеки изход от транзакция (т.е когато един адрес е получил биткойни), който не е използван в нова транзакция, се счита за "непохарчен" (unspent). Тези непохарчени изходи могат да бъдат използвани като входове в бъдещи транзакции. UTXO моделът е различен от моделите, използвани от традиционните банкови системи, при които се съхранява баланс по сметка.

Как работи UTXO?

Когато потребител извърши транзакция в Биткойн, той не изпраща конкретна сума биткойн от баланса си, а вместо това посочва кои UTXO иска да използва. Всеки UTXO има специфична стойност, а

общата сума на UTXO, използвани в транзакцията, трябва да покрива сумата, която потребителят иска да изпрати. Ако стойността на използваните UTXO е по-голяма от сумата за изпращане, излишъкът се връща на потребителя под формата на нов UTXO.

Пример за UTXO:

Представете си, че Георги има три UTXO в своя портфейл: 1 BTC, 0.5 BTC и 0.2 BTC. Ако той иска да изпрати 0.6 BTC на Петър, той може да използва UTXO-то от 1 BTC. В този случай 0.6 BTC ще отидат при Георги, а останалите 0.4 BTC ще се върнат при Петър като нов UTXO.

Предимства на UTXO модела

- **Гъвкавост**: UTXO моделът позволява на участниците в мрежата да комбинират и разделят изходи свободно, което прави транзакциите по-гъвкави и лесни за верифициране.
- **Подобрена сигурност**: UTXO моделът осигурява по-добро разделение между баланса и идентичността на потребителите, тъй като балансът се определя от сумата на UTXO, а не от централизирана сметка.

6. Емисия на Биткойн и лимитът на 21 милиона

Една от ключовите характеристики на Биткойн е неговият ограничен лимит на общата емисия, който е фиксиран на 21 милиона биткойна. Това ограничение е зададено в оригиналния код на Биткойн от Сатоши Накамото и не може да бъде променено без консенсус от цялата мрежа (нодовете).

Как се създават нови биткойни?

Всеки нов блок, който се добавя към блокчейна, съдържа т.нар. блокова награда, която се изплаща на миньора, който е успял да намери валидния nonce за този блок. Тази награда е съставена от два компонента:

- **Награда за блок**: Първоначално, когато Биткойн стартира, тази награда беше 50 биткойна на блок. На всеки 210 000 блока

(около на всеки четири години) наградата за блок се намалява наполовина. Този процес се нарича халвинг (halving).
- **Такси за транзакции**: Освен блоковата награда, миньорите събират таксите за всички транзакции, включени в блока. С намаляването на наградата за блок с времето, таксите за транзакции ще играят все по-важна роля в стимулирането на миньорите.

7. Криптографски Подписи в Биткойн

Криптографските подписи са съществена част от сигурността на Биткойн и гарантират, че само притежателят на даден частен ключ може да изразходва съответните биткойни. В основата на Биткойн са ECDSA (Elliptic Curve Digital Signature Algorithm) и новите внедрения като Schnorr подписите, които предлагат подобрения по отношение на мащабируемост и сигурност.

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA е криптографски алгоритъм, използван в Биткойн за създаване и проверка на дигитални подписи. Биткойн използва кривата secp256k1 – специален вид елиптична крива, избрана заради своите ефективни изчисления и силни криптографски свойства. Елиптичната крива осигурява достатъчна сложност, за да направи практически невъзможно извличането на частен ключ от публичен ключ.

Как работи ECDSA?

ECDSA се базира на два основни компонента:

- **Частен ключ**: Секретен номер, който служи като средство за създаване на дигитални подписи. Той трябва да бъде строго пазен, тъй като всеки, който има достъп до частния ключ, може да подписва транзакции отговарящи към съответния публичен ключ.
- **Публичен ключ**: Генериран от частния ключ с помощта на математически операции върху елиптичната крива. Публичният ключ се използва за верифициране на подписите, без да се разкрива частният ключ.

Подписването на транзакция с ECDSA гарантира, че транзакцията не може да бъде променена след подписването, а публичният ключ позволява на всички участници в мрежата да проверят валидността на подписа.

Недостатъци на ECDSA:

- **Многоподписни сценарии (Multisig)**: ECDSA не е особено ефективен при създаване на сложни многостепенни договори, изискващи множество подписи.
- **Размер на подписите**: Размерът на подписите при ECDSA не е малък, което води до по-голямо пространство, заето в блокчейна.

Schnorr Подписи

Schnorr подписите са алтернативен алгоритъм за дигитални подписи, който беше добавен към Биткойн чрез ъпгрейда Taproot. Schnorr подписите предлагат няколко предимства пред ECDSA, включително по-компактни подписи и възможността за „подписова агрегация" (signature aggregation).

Предимства на Schnorr Подписите:

- **Агрегиране на подписи**: Едно от основните предимства на Schnorr подписите е възможността за комбиниране на множество подписи в един, когато се използват в многоподписни (multisig) сценарии. Това не само намалява размера на транзакциите, но и прави такива транзакции неразличими от стандартните едноподписни транзакции, като подобрява сигурността и поверителността.
- **По-компактни подписи**: Schnorr подписите са по-малки по размер в сравнение с ECDSA, което позволява по-ефективно използване на блокчейн пространството.
- **Линеен по дизайн**: Линейността на Schnorr подписите позволява по-лесна и по-бърза верификация на подписите, особено в сложни транзакционни сценарии.

Приложение на Schnorr в Taproot

Taproot ъпгрейдът комбинира Schnorr подписите с концепцията на "scriptless scripts", което позволява създаването на сложни логически договори (като мултиподписни сценарии и блокирани във времето транзакции) без нуждата тези договори да бъдат видими в

блокчейна. Това добавя както функционалност, така и поверителност.

8. Адреси в Биткойн

Биткойн адресите са резултат от хеширане на публичния ключ и служат като идентификатори, на които могат да бъдат изпращани биткойни. Има няколко различни вида Биткойн адреси, които са въведени с цел подобряване на сигурността, мащабируемостта и потребителския опит.

Legacy Адреси (P2PKH)

Това са оригиналните Биткойн адреси, започващи с цифрата „1". P2PKH (Pay to Public Key Hash) адресите се базират на хеширане на публичния ключ с помощта на SHA-256 и RIPEMD-160 алгоритми.

- **Формат**: Адресите започват с „1", пример: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
- **Недостатъци**: Тези адреси заемат повече място в блокчейна и не поддържат SegWit, което ги прави по-скъпи за употреба при транзакции.

SegWit Адреси (P2SH-P2WPKH)

Segregated Witness (SegWit) е надстройка на Биткойн, която промени начина, по който данните за подписите се съхраняват в блоковете. Този формат адреси, започващ с „3", позволява по-ефективно използване на блокчейн пространството чрез премахване на данните за подписите от основната част на блока.

- **Формат**: Адресите започват с „3", пример: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
- **Предимства**: Намалени такси за транзакции и подобрена мащабируемост.

Native SegWit Адреси (Bech32)

Bech32 адресите са по-нов формат, въведен с пълната реализация на SegWit. Тези адреси започват с „bc1q" и предлагат най-високото ниво на оптимизация по отношение на пространство и такси за транзакции.

- **Формат**: Адресите започват с „bc1q“, пример: bc1qw508d6qezt3cpr0ms8phh28u0a8kmzsav8zgn
- **Предимства**: По-ниски такси, по-малка вероятност за грешка при въвеждане на адреси и поддръжка на всички нови функции в Биткойн като Taproot.

Taproot Адреси (P2TR)

Taproot е последната значителна надстройка на Биткойн, въведена с цел подобряване на поверителността и гъвкавостта на мрежата. Taproot адресите, известни като P2TR (Pay to Taproot), започват с „bc1p“ и са съвместими с новия подписен стандарт Schnorr, както и с новите MAST (Merkelized Abstract Syntax Tree) договори.

- **Формат**: Адресите започват с „bc1p“, пример: bc1p5cyxnuxmeuwuvkwfem96l9pn8lwxszzltnpxy8
- **Предимства**:
  - **По-висока поверителност**: Всички транзакции, включително сложни скриптове, изглеждат идентични на едноподписните транзакции, което затруднява анализа на блокчейна.
  - **Подобрена мащабируемост**: Taproot използва новия Schnorr подписен алгоритъм, който позволява по-малки и по-ефективни транзакции.
  - **Гъвкавост**: Поддържа по-сложни логически договори чрез MAST, като същевременно се запазва пространствената ефективност на блокчейна.

Taproot адресите комбинират сигурността на SegWit с нови възможности за скрити скриптове и сложни договори, като същевременно намаляват таксите за транзакции и повишават сигурността.