Биткойн: Директна електронна парична система

Сатоши Накамото

Абстракт

Една чиста версия на електронни пари, работеща на принципа на равноправни участници (peer-to-peer), би позволила онлайн плащанията да се изпращат направо от един човек на друг, без да е необходимо да минават през финансова институция. Електронните подписи предлагат частично решение, но основните предимства изчезват, ако все пак се нуждаем от доверена трета страна, която да предотвратява двойното харчене. Ние предлагаме решение на проблема с двойното харчене, използвайки мрежа с пряка връзка. Мрежата датира всяка транзакция, като я записва в непрекъсната верига от криптографски[1] хешове[2], базирани на доказателство за извършена работа (proof of work). Така се създава невъзможен за промяна запис, освен ако не се извърши отново цялата работа по доказването. Най-дългата верига служи не само като доказателство за последователността на събитията, на които сме свидетели, но и като доказателство, че произлиза от най-големия обем изчислителна мощност. Докато по-голямата част от тази мощност се контролира от възли, които не си сътрудничат с цел атака на мрежата, те ще генерират най-дългата верига и ще надделеят над нападателите. Самата мрежа изисква минимална организация. Съобщенията се разпространяват според възможностите, а възлите могат да напускат и да се присъединяват отново към мрежата по всяко време, приемайки най-дългата верига от доказателства за работа като доказателство за събитията, случили се докато са отсъствали.

1 Въведение

Търговията в интернет разчита почти изключително на финансови институции, служещи като доверени трети страни за обработка на електронни плащания. Въпреки че системата работи достатъчно добре за повечето транзакции, тя все още страда от присъщите слабости на модела, основан на доверие. Напълно необратимите транзакции не са реално възможни, тъй като финансовите институции не могат да избегнат медиацията при спорове. Цената на медиацията увеличава транзакционните разходи, ограничавайки минималния практически размер на транзакцията и отрязвайки възможността за малки, случайни транзакции, и има по-широка цена от загубата на възможност за извършване на необратими плащания за необратими услуги. С възможността за отмяна, необходимостта от доверие се разпространява. Търговците трябва да бъдат предпазливи към клиентите си, като ги тормозят за повече информация, отколкото иначе биха им били необходими. Известен процент измами се приемат за неизбежни. Тези разходи и несигурност при плащането могат да бъдат избегнати лично чрез използване на физическа валута, но не съществува механизъм за извършване на плащания по комуникационен канал без доверена страна.

Необходима е електронна платежна система, базирана на криптографско доказателство, вместо на доверие, позволяваща на две желаещи страни да извършват директни транзакции помежду си, без да е необходима доверена трета страна. Транзакции, чието отмяна

[1] Криптографията е наука за методите за запазване на информацията в тайна и за удостоверяване на нейната автентичност.

[2] Хеш е еднопосочна функция, която преобразува входни данни с произволна дължина в изходен низ с фиксирана дължина (хеш стойност), често използван за проверка на целостта на данни или за сигурност.

е изчислително непрактично, биха защитили продавачите от измами, а рутинни механизми за ескроу биха могли лесно да бъдат внедрени за защита на купувачите. В тази статия предлагаме решение на проблема с двойното харчене, използвайки разпределен peer-to-peer сървър за времеви марки, за да генерира изчислително доказателство за хронологичния ред на транзакциите. Системата е сигурна, стига честните възли колективно да контролират повече процесорна мощност от която и да е сътрудничеща си група от атакуващи възли.

2 Транзакции

Дефинираме електронна монета като верига от цифрови подписи. Всеки собственик прехвърля монетата на следващия, като подписва цифрово хеш на предишната транзакция и публичния ключ на следващия собственик и ги добавя в края на монетата. Получателят може да провери подписите, за да потвърди веригата на собственост.