

ПРОБЛЕМИ БЕЗПЕКИ СИСТЕМИ BITCOIN

Забезпечення безпеки bitcoin – це складне завдання через те, що криптовалюта схожа на готівку або золото, тільки в цифровому вигляді. Володіння ключами еквівалентно володінню пачкою готівки або шматком дорогоцінного металу. Bitcoin можна втратити, він може бути вкрадений, а також можливо випадково видати комусь невірну суму. У кожному з цих випадків, користувачі не можуть розраховувати на чиюсь допомогу. Тому безпека цієї системи на сьогоднішній день та у майбутньому викликає занепокоєння.

Однією з проблем безпеки є: як не допустити централізацію біткоїн-мережі, так як це зробило б криптовалюту більш вразливою для кібератак або шахрайської діяльності. Зараз мережа децентралізована, оскільки нею керують майнери - численні люди і підприємства, які видобувають нові біткоїни і підтримують систему. Їх праця оплачується за рахунок винагород за створення блоків і комісій за транзакції, і це становить практично весь їх дохід. Згодом розмір винагород буде знижуватися, і це означає, що якщо комісії за транзакції не будуть збільшуватися, майнери перестануть отримувати прибуток і почнуть виходити з системи. Якщо їх стане менше, система стане більш централізованою, отже, більш вразливою. Крім того, централізація мережі дозволить одному зловмиснику або групі таких людей, контролюючих значну частину майнінгових потужностей атакувати механізм консенсусу з метою порушення безпеки і доступності мережі Bitcoin (атака 51%). Атака 51% означає, що атакуючий зможе не підтверджувати чужі блоки, а підтверджуючи тільки свої, отримувати 100% всіх нових біткоїнів і блокувати за своїм розсудом будь-які транзакції (однак проводити будь-які транзакції на свій розсуд він не зможе, оскільки у нього не буде чужих приватних ключів, щоб ці транзакції підписати).

Ще однією проблемою є те, що електронний гаманець слабо захищений від крадіжок. За замовчуванням гаманець незашифрований. З цієї причини він стає легкою здобиччю для шахраїв. Однак останні версії клієнтів Bitcoin вже містять шифри для захисту даних гаманця, але користувач повинен вручну підключити шифр.

Атака Сивілли означає, що зловмисник може спробувати наповнити мережу підконтрольними йому вузлами, і інші користувачі зможуть

підключитися тільки до блоків, що створені для шахрайства. Це може відбуватися коли атакуючий блокує транзакції від інших користувачів, від'єднавши вас від загальної мережі. Далі зловмисник під'єднує вас тільки до блоків, які створює він, в окремій мережі. В результаті цього будуть з'являтися транзакції, які будуть пересилати гроші повторно (double-spending). Зловмисник може бачити всі ваші транзакції за допомогою спеціальних програм.

Стару копію гаманця зі старим паролем можна відновити за допомогою створення програми відновлення (наприклад, Apple Time-Machine), таким чином виникає проблема відкриття нового електронного гаманця старим паролем через бекапи. Рішенням такої проблеми може бути внесення таких змін, щоб зміна пароля до гаманця автоматично створювала новий гаманець з новим паролем, і накопичені заощадження автоматично переносилися на новий гаманець. При цьому копії будуть неробочими у разі спроби відновлення старого гаманця і пароля.

Наступною проблемою є атаки Denial-of-Service (DoS). Відправлення великої кількості "сміттєвих" даних на вузол, що обробляє транзакції, може ускладнити його роботу. Bitcoin має вбудований захист від атак типу «відмова в обслуговуванні», але сучасні атаки такого типу з кожним разом стають все складніші для блокування.

Існує також проблема відстеження історії грошових транзакцій. Відстеження історії грошових переказів може бути використано для ідентифікації адреси. Так як bitcoin не є повністю анонімним засобом оплати.

Не менш важливою є проблема багів. Наприклад, в вузлі інформація повинна оновлюватися за короткий відрізок часу. Якщо через баг це не відбулося, в ланцюжку не з'явилася потрібна інформація, неправильні дані почали поширюватися по мережі і т.д. Все це може стати причиною зупинки роботи мережі на кілька годин.

Так як спокуса вивести гроші з біткоїн-гаманців велика, зловмисники намагаються вигадувати і створювати різноманітні способи відмивання грошей. Таким чином можна зробити висновок, що не існує повністю захищених систем, і електронна система грошових коштів Bitcoin не є виключенням.