Біткоін

СТУДЕНТ:
НЕЧВОГЛОД С.А


bitcoin

ЩО ТАКЕ БІТКОЙН

- **Bitcoin** також **Біткойн** — електронна валюта, концепт якої був озвучений у 2008 році Сатосі Накамото, і предствлений ним у 2009 році, базується на самоопублікованому документі Сатосі Накамото. Повна капіталізація ринку біткоїнів зараз становить 7,865,298,695 USD (5,742,527

ЗАСНОВНИК BITCOIN

Сатоси Накамото

Гэвин Андрисен

Перший випуск	4 лютий 2009року

Тип:Електроні гроші

ВЗАГАЛІ

- Bitcoin не має централізованого управління та емітентів. Транзакції із цифровим підписом між двома вузлами передаються до всіх вузлів peer-to-peer мережі, а самі дані про переміщення коштів зберігаються у розподіленій базі даних. Для запобігання можливості трати чужих грошей або використання своїх коштів двічі використовуються криптографічні методи.

ПРИНЦИПИ РОБОТИ

- BitCoin покладається на криптографічні принципи, щоб створити унікальні, невідтворювані, і ділені маркери валюти. Користувачі зберігають криптографічні ключі до своїх власних грошей локально на своєму власному комп'ютері, і проводять транзакції безпосередньо один з одним через пірингову мережу, перевіряючи за допомогою мережі достовірність грошових переказів. Фізично, кожна монета в системі має свій унікальний ключ.

- При здійсненні транзакції користувач додає до монети відкритий ключ адресата і підписує її своїм особистим закритим ключем. Щоб виключити подвійне списання однієї монети, всі транзакції транслюються іншим учасникам, а повний список транзакцій в анонімному вигляді зберігається в розподіленій мережі. При кожній новій транзакції ключі перевіряються за списком попередніх транзакцій. Інакше кажучи, BitCoin заснований на записі переміщень грошових коштів з використанням асиметричного шифрування.

- Для запобігання багаторазової витрати однієї і тієї ж суми мережа реалізує щось подібне розподіленому серверу часу, використовуючи ідею ланцюжка хешів, кожен з яких обчислюється на базі попереднього. Для зменшення розміру розподіленої мережевої БД використовується деревоподібне хешування.

- В даний момент кількість монет в обігу системи становить трохи більше 1 млн. Фактично на даний момент, BitCoin — це хмарна мережа розподілених обчислень. Дохід в BitCoin монетизується за рахунок валюти, цінність якої забезпечує електрична енергія і робота процесора. Фактично, номінал однієї монети дорівнює певній кількості процесорного часу. На практиці вартість її визначається співвідношенням біржових пропозиції та попиту, що з певною затримкою впливає на необхідні комп'ютерні ресурси для генерації монети.

КОНФЕДЕЦІЙНІСТЬ

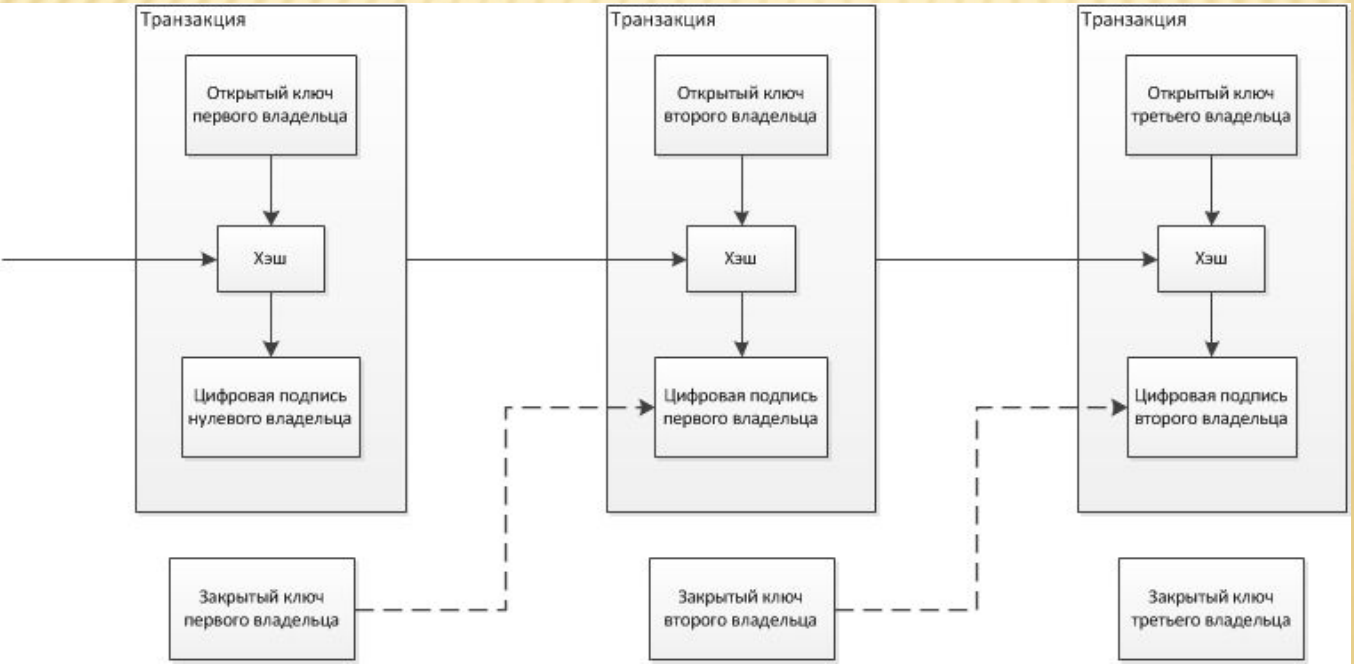
- Традиційна модель досягає секретності шляхом обмеження доступу до інформації. Про угоду можуть знати тільки дві сторони і банк. У системі «Біткойн» всі транзакції публічні, зберігаються у відкритому нешифрованном вигляді, а таємність досягається відсутністю персоніфікації власників.

  На думку ряду авторів, біткойн-адреси є псевдонімами користувачів[23] системи. Якщо зв'язати біткойн-адресу з конкретною людиною, то зникає анонімність всіх транзакцій з використанням цієї адреси.

Порівняння традиційної моделі з моделлю приватності приватності в системі Біткойн

ТРАНЗАКЦІЇ

- Біткойни можуть бути передані будь-кому, хто повідомить коректний біткойн-адреса або відкритий ключ. Мінімальну передану величину 10-8 біткойн називають «сатосі» — на честь творця Сатосі Накамото, хоча сам він використовував для позначень мінімальної величини переданої слово «цент». Для передачі біткойнів поточний власник створює нову транзакцію, яка крім вказівок про кількість переданих біткойнів підписаний ініціатором містить геш попередньої транзакції, за якою біткойни були отримані. Попередня транзакція стає «входом» поточної транзакції. Також вказується публічний ключ або біткойн-адресу нового одержувача («вихід»)



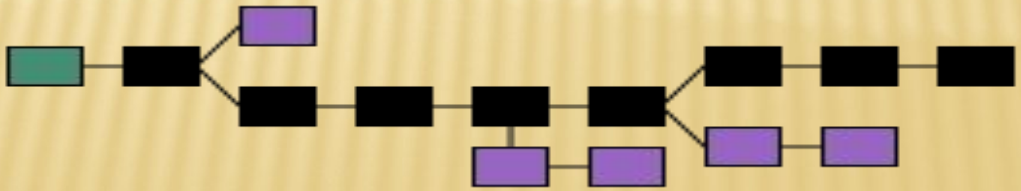
Спрощена структура послідовних транзакцій з одним входом і одним виходом

БЛОКИ ТРАНЗАКЦІЇ

- Окремі транзакції об'єднують разом з іншими транзакціями в спеціальну структуру — блок. Інформація в блоках відкрита, не шифрується, її можна швидко перевірити.

  Кожен блок завжди має свій порядковий номер і хеш попереднього блоку. Всі блоки можна вибудувати в один ланцюжок, яка містить інформацію про всі вчинені коли-небудь операції з біткойнами. З ними можна ознайомитися, наприклад, на спеціалізованих сайтах — браузерах ланцюжків блоків

  Перша транзакція в блоці завжди формується автоматично і передає винагороду за створення блоку. Решта наповнення блоку беруть з черги транзакцій, які ще не були записані в попередні блоки. Створює блок учасник може сам відібрати включаються в блок транзакції, наприклад, не взяти в блок транзакції без комісії



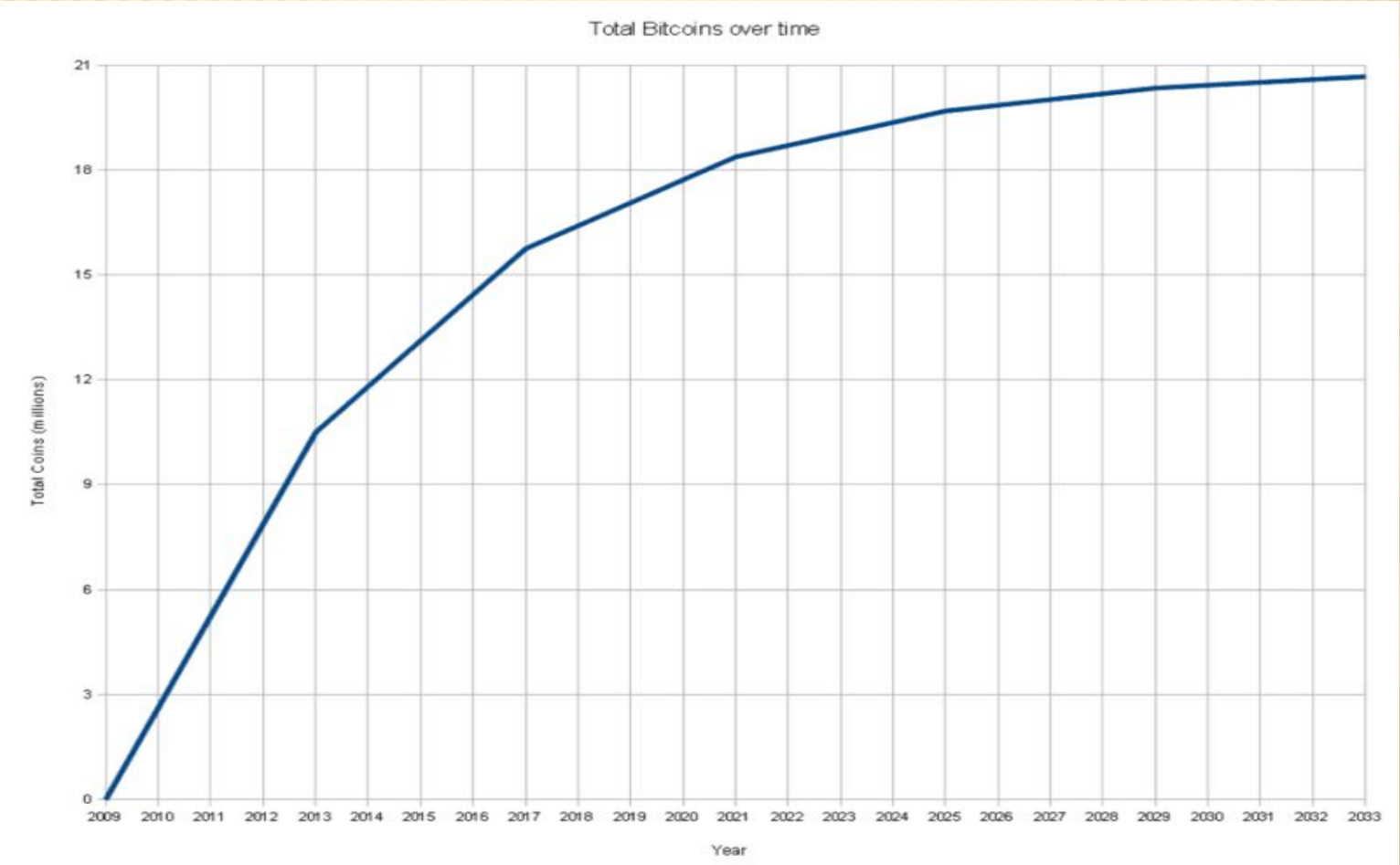
ПРИНЦИП ФУНКЦІОНУВАННЯ

- Всі дані про кількість біткоїнів користувача зберігаються у бінарному файлі, який називають гаманцем (англ. *wallet*). Гаманець показує поточний баланс, історію транзакцій та адреси, що доступні для надсилання коштів. Так як усі транзакції зберігаються у розподіленій базі даних, то комп'ютер користувача не повинен мати постійного підключення до мережі, щоб отримувати біткоїни.

- Біткоїнові платежі зазвичай показуються одержувачу майже миттєво, але спочатку як «непідтверджені», тому що система поки не може гарантувати постійність даної транзакції. Транзакція може бути недійсна через конфлікт транзакцій (наприклад, коли два одержувача отримують однакові біткоїни). Це може статися коли у програмному забезпеченні відправника відбувається неполадка або коли він навмисно робить спробу шахрайства. Коли мережа Bitcoin обробляє транзакцію, до черги, що включає транзакцію додається все більше підтверджень. Зрештою, клієнт Bitcoin показує транзакцію як «підтверджену».

ЕМІСІЯ

- Випуск нових біткойнів децентралізований, не залежить від будь-яких регулюючого органу, обсяг емісії відомий заздалегідь Стандартна порція нових біткойнів додається до суми комісій з транзакцій, включених в черговий блок. Підсумкову суму в якості винагороди отримує той, хто додав черговий блок до бази транзакцій.



Кількість біткойнів з плином часу (роки з 2009 по 2033)

ФЕРМИ BITCOIN

- З 2013 року з'являються репортажі про «фабриках біткойнів» — спеціалізованих безлюдних підприємствах, на яких «працюють» тисячі HBIC-процесорів. Місячний дохід фабрики може перевищувати мільйон доларів (кілька тисяч біткойнів). У 2015 році, навіть якщо припустити, що всі майнеры використовують енергозберігаючі процесори, сумарний витрата електроенергії на майнінг оцінювався в 1,46 терават-годин на рік, що еквівалентно річному споживанню 135 000 американських будинків.

СТАДІЇ РОЗВИТКУ

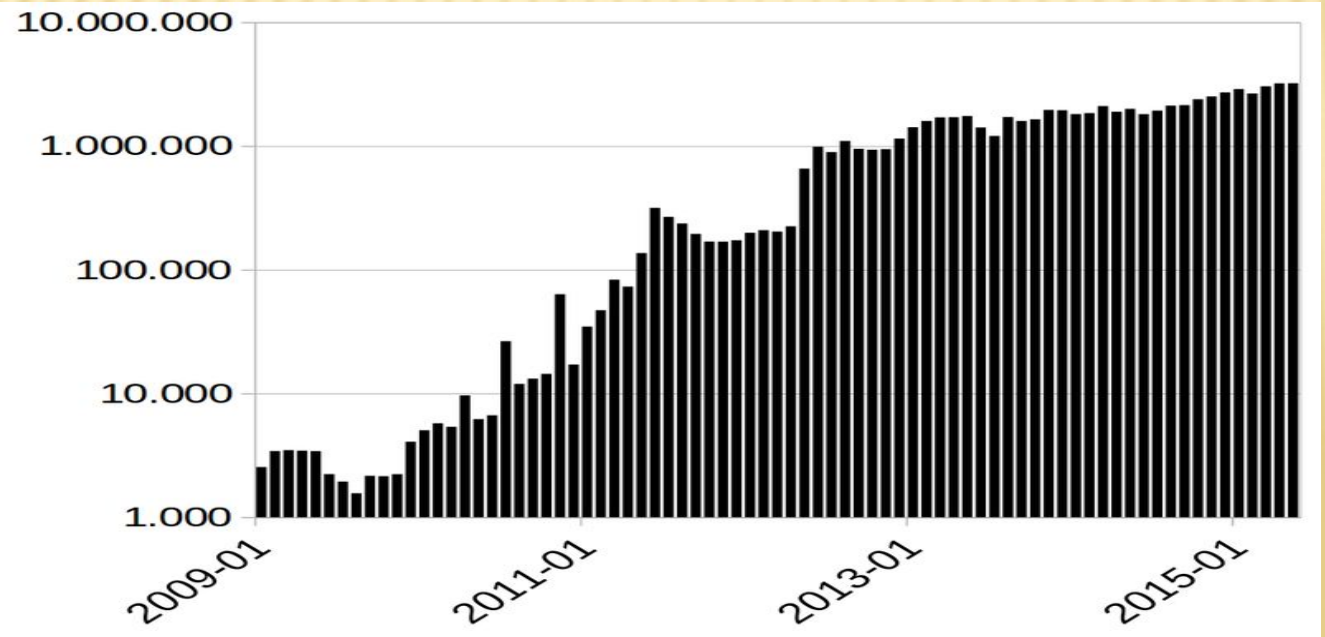
- За задумом творця системи — японця Сетоші Некемото, — будь-яка центральна емісія повинна бути скасована і замінена на персональну (особисту) емісію самих громадян.
- Коли загальна валютна база системи досягне суми 21 млн монет, то будь-який тип емісії буде повністю технічно зупинений (щоб уникнути інфляції), після чого система увійде в третю заключну фазу — стабілізація. Зараз можна бачити, що повністю в згоді з теорією BTC знаходиться в заключній частині фази bootstrap, входячи в другу фазу — зокрема, це ознаменувався дуже сильним пожвавленням біржових торгів по BTC останнім часом. Незважаючи на те що дармові монети в системі вже майже закінчилися, все ж трохи зупинимося на цьому моменті детальніше.

УСТАНОВКА І ВИКОРИСТАННЯ ГАМАНЦЯ

- Програма-гаманець BitCoin — це **звичайний** десктоповий додаток, на кшталт всім звичного WebMoney Classic. Для роботи програми потрібно, щоб у вас був відкритий мережевий порт номер 8333, тому якщо у вас активовано захисний екран Windows або встановлено інший сторонній брендмауер, варто про це подбати заздалегідь. Є версії гаманця для Windows, Linux, MacOS X, Android, IOS

ЕКОНОМІКА

- Біткойни приймаються в обмін на мережні послуги і реальні товари. Багато організації приймають пожертви у биткойнах На грі Університетської ліги США в об'єктиви телекамер потрапив плакат одного з студентів «Мама, прийшли грошей!» зі знаком биткойна і з QR-кодом біткойн-адреси студента. За добу студент отримав пожертвувань на 20 тисяч доларів. У випадку з Вікілікс, прийом біткойнів став вимушеним заходом після того, як Віза, Мастеркард, Банк Америки припинили приймати пожертвування на адресу сайту WikiLeaks, а через PayPal і деякі інші платіжні системи — заморозили рахунки. Надання можливості оплати через біткойни може служити додатковою рекламою, навіть якщо така оплата жодного разу не проводилася.
Ряд брокерів пропонують торгівлю на умовах маржинальної торгівлі безпоставковими контрактами CFD-контрактами на курс «біткойн — долар США» (БТД/доларів США).



Кількість транзакцій біткойнів в місяць

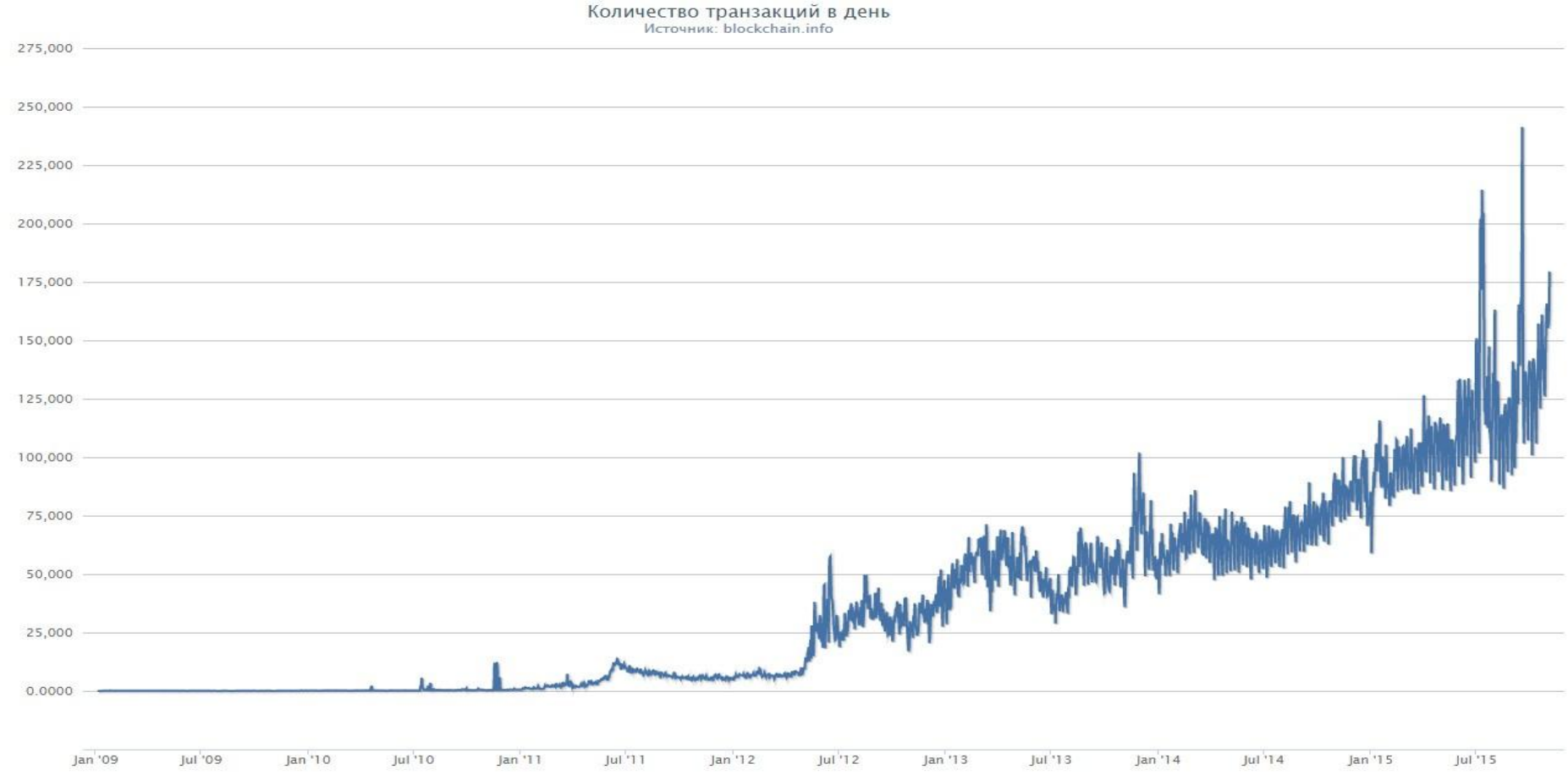
ЦІНОВА ВОЛАТИЛЬНІСТЬ

- Котирування биткойна залежить виключно від балансу попиту і пропозиції, вона ніким не регулюється. Ні різкий ріст, ні різке падіння не обмежується, як це відбувається на фондових біржах шляхом зупинення торгів.
- З 2009 по квітень 2010 року біткойни лише накопичувалися. 25 квітня 2010 року відбулася перша офіційна продаж 1000 біткойнів по 0,3 цента, а в травні 2010 року за 10 000 біткойнів купили дві піци. Лише в лютому 2011 року за біткойн почали давати долар або близько того. Перша велика стаття про биткойнах в Форбс 20 квітня 2011 року пробудила широкий інтерес. До кінця травня за біткойн давали майже 9 доларів, 9 червня 2011 року ціна досягла 29,57 долара, після чого пішла вниз приблизно до двох доларів і повернулася тільки 19 лютого 2013 року. У квітні 2013 року стався новий різкий підйом до 266 доларів і подальший обвал до рівня 50 доларів.
- У середині листопада 2013 року ціна перевищила 1000 доларів. Після низки сплесків і падінь, з січня 2014 року ціна мала тенденцію до зниження. В січні 2015 року ціна знизилася до 200 доларів, після чого почала коливатися в межах 200-300 доларів.
  Значні коливання котирувань викликали багато обговорень. З'явилися прогнози, що ціна биткойна в майбутньому досягне 40 тис. доларів. і навіть 100 тис. доларів

ОБМІННИЙ КУРС БІТКОЙН/ДОЛАР. ПРАВОРУЧ ВИДНО СУТТЄВЕ РОЗХОДЖЕННЯ ЦІНИ НА МТ.ЛАЙТ З ЦІНАМИ НА ІНШИХ МАЙДАНЧИКАХ

НЕЗВАЖАЮЧИ НА ТЕ, ЩО КІЛЬКІСТЬ БИТКОИНОВ СТАЄ КОЖЕН ДЕНЬ ВСЕ БІЛЬШЕ, АЛЕ ЇХ КУРС ДО РЕАЛЬНИХ ГРОШЕЙ ЗА ОСТАННІЙ ЧАС ДОСИТЬ РІЗКО ЙДЕ ВГОРУ:

- Вартість одного биткоина доходила до 1200$ в грудні 2013 року, а ще влітку 2013 валюта коштувала в 100 разів дешевше. Це колосальний зростання, на якому можна було заробити 10000%. Про те, що до биткоинам є великий інтерес свідчить постійний ріст кількості транзакцій здійснюваний у цій валюті:



ГЛОБАЛЬНІ ПЕРСПЕКТИВИ

- Сьогодні BTC приймають сотні західних магазинів електроніки, косметики, компанії з надання послуг хостингу, замовлення їжі, лотереї, віртуальні ігри та інші сервіси. В результаті переговорів з Amazon було досягнуто домовленості про використання BTC в її інтернет-магазинах (сума покупки повинна перевищувати в еквіваленті $ 30).

- У лютому 2011 року BitCoin взяла дуже важливу психологічну планку — вперше за її існування курс обміну BTC до USD досяг стійкого паритету, а в деякі вдалі дні за 1 монету BitCoin давали більше 1 долара. В середині 2011 року, на піку зростання, за одну монету цієї електронної валюти пропонували вже 18 доларів.

- Слід згадати і про політичний компонент, який вже починає проявлятися у BTC: після численних випадків закриття рахунків у традиційних грошових системах у проекту WikiLeaks, цей проект тепер продовжив збір грошей в системі BitCoin.

ЦІКАВІ ФАКТИ ПРО БІТКОІНИ!

- За весь час може бути створено не більше 21 мільйона біткоіни.
- • Один біткоіни може бути розділений на 0,00000001 частин.
- • біткоіни створюються в результаті комп'ютерних обчислень, званих «добуванням», - з часом це може перетворитися на конкурентоспроможну галузь.
- • біткоіни - це інтернаціональна система, що дозволяє дешево переводити будь-які грошові суми в будь-яке місце в будь-який час.
- • біткоіни-транзакції є незворотними.
- • Усі транзакції, що здійснюються в мережі, записуються в так звану ланцюжок блоків, яка на 100% прозора.
- • Мережа також стежить за тим, щоб не було шахрайських транзакцій. За всю історію існування мережі в ній не було транзакційних помилок.
- • біткоіни не є анонімними за замовчуванням, але це найбільш приватний спосіб
- • Вартість біткоіни регулюється вільним ринком.
- • Вартість біткоіни дуже нестійка, але це якість і дозволяє збільшувати їх цінність.
- • біткоіни - найбільш безпечна валюта!

ЦІННА ЗА ОДИН БІТКОЇН 389 ДОЛАРІВ НА07.11.2015

КРИТИКА

- Анонімність системи «Біткойн» заважає державі контролювати фінансові потоки, в тому числі через кордон. У вересні 2014 року Банк Англії висловив побоювання, що якщо системи «Біткойн» збільшиться популярність, то в крайньому варіанті можна втратити контроль над інфляцією

- Використання біткойнів в тіньовій економіці дозволяє забезпечити непідконтрольність національним органам влади торгівлю такими товарами, як зброя, наркотики і т. д. як приклад подібної торгівлі ЗМІ найчастіше розглядають історію інтернет-магазину "Шовковий шлях". При цьому під час слухань у Сенаті США з приводу віртуальних валют зазначалося, що готівкові гроші для нелегальних операцій використовують набагато частіше, але це не стає підставою для критики або заборони готівки.

- колишній старший радник Казначейства США і Міжнародного валютного фонду Нуріель Рубіні в березні 2014 року заявив, що «Біткойн» є варіантом фінансової піраміди. У цьому переконаний і Джонатан Тругман з Нью-Йорк пост[138].

  У 2012 році Європейський центральний банк у доповіді зазначив, що поки немає можливості оцінити, чи є робота системи «Біткойн» фінансовою пірамідоюУ 2014 році глава Банку Естонії обережно відзначав відсутність доказів того, що «Біткойн» не є фінансовою пірамідою.

  2014 року У звіті Світового банку зазначається, що «всупереч широко поширеній думку, „Біткойн“ не є навмисною фінансовою пірамідою. На думку Еріка Познера, професора права в Університеті Чикаго, фінансова піраміда зазвичай має ознаки шахрайства, а ситуація з «Биткойном» більше схожа на колективну ілюзію. Економіст Джеффрі Такер стверджує, що «є кілька ключових відмінностей між фінансовою пірамідою і „Биткойном“». У звіті 2014 року Ради Федерації (Швейцарія) у відповідь на неодноразово порушувалося питання, чи є «Біткойн» фінансовою пірамідою, робиться висновок, що система «Біткойн» не робить типові обіцянки прибутку, тому «Біткойн» пірамідою не є.

CONCLUSION

- Bitcoin is often compared to "electronic gold". In the real world gold is just a metal that has its value because it has a great demand. Bitonti have the same meaning, but only as-to touch or not to support them - it's all still virtual. They will have some value until then, until there is a demand. And the demand for the new currency yet consistently growing, and this gives great prospects bitcoins, and this further increases the interest in them. By the way, in the future it is possible to manufacture real coins of BitCoin, but it's still only prospects.