Freeman Family

4 липня 2019

EPIC CASH

EPIC приватна інтернет валюта

EPIC

Електронна готівкова система P2P

Засіб зберігання цінності + засіб обміну + облікова одиниця

1,7 мільярда людей не мають доступу до світової фінансової системи, а для ще 1,3 мільярда осіб - цей доступ обмежений. Epic Cash збільшує потенціал людини, підключаючи нових людей до світового ринку. Це швидка, практично безкоштовна у використанні та відкрита для всіх система.

Version 7.1b Ukrainian

Зміст

I. Анотація

Epic Cash - це останній крок на шляху до справжньої інтернет-готівки P2P, базової основи приватної фінансової системи.
Основна мета Epic Cash - стати найефективнішою приватною цифровою валютою.
Для досягнення цієї мети система повинна відповідати трьом базовий аспектам:

1. **Засіб зберігання цінності** - можна зберігати, отримувати та обмінювати валюту з передбачуваним значенням при її отриманні;
2. **Засіб обміну** - спроможність бути прийняте як те, що представляє собою ціннісний стандарт і обмінюється на товари чи послуги;
3. **Облікова одиниця** - одиниця, за якою враховується і порівнюється вартість речей.

	$ USD	BTC	EPIC
Засіб зберігання цінності	✗	✓	✓
Засіб обміну	✓	✗	✓
Облікова одиниця	✓	✗	✓

У 2009 році Bitcoin першою цифровою валютою на основі блокчейн технології, та запровадив три визначаючі характеристики, за якими оцінюються інші криптоактиви:

- **Відсутність необхідності у довірі** – нікому не потрібно довіряти будь-якому централізованому об'єкту чи контрагенту для того, щоб мережа функціонувала;
- **Незмінність** – транзакції не можуть бути скасовані;
  a. Можливість змін в історії транзакцій дуже важка та має низьку ймовірність;
  b. Ніхто, окрім власника приватного ключа не може перемістити кошти, що пов'язані з ним;
  c. Всі транзакції пишуться в блокчейн.
- **Децентралізація** – «блокчейни є політично децентралізованими (їх ніхто не контролює) та архітектурно децентралізованими (немає єдиної інфраструктурної точки відказу) ...» [1].

Bitcoin відкрив нові технологічні горизонти, при цьому дотримуючись перевірених часом основ у структурі грошової політики. Успіх Bitcoin сильно пов'язаний з його обмеженою пропозицією в поєднанні з незмінним і децентралізованим блокчейном, який не вимагає довіри між учасниками мережі. Epic Cash використовує грошову політику Bitcoin щодо зменшення інфляції та обмеженої пропозиції, та може гарантувати, що Epic може використовуватися як ефективний засіб збереження цінності. Незважаючи на успіх Bitcoin, з моменту його створення 10 років тому, були виявлені певні недоліки Інші проекти намагалися подолати ці недоліки, та наші спеціалісти аналізують найкращі з них, щоб використовувати їх як вихідну точку. Ми вирішили використовувати кодову базу Grin та досвід декількох інших проектів, який може допомогти нам подолати недоліки попередників. Epic Cash має ключові якості, які дають йому змогу бути ідеальною валютою:

- **Гнучкість** –Вартість конкретної одиниці Epic завжди має дорівнювати іншій одиниці Epic , подібно до того, як одна Йена або Юань завжди дорівнює іншій Йені або Юаню. Досягнення гнучкості значною мірою залежить від конфіденційності.
- **Масштабованість** – Epic Cash підтримує просторовий блокчейн, на якому створюються нові ноди які можна легко встановити без ресурсомісткого обладнання. Блокчейн Epic Cash здатний принаймні вдвічі перевищувати пропускну здатність Bitcoin.
- **Конфіденційність** – Блокчейн Epic Cash захищає анонімність власників та користувачів Epic, захищаючи особливості транзакцій від сторонніх осіб, його можна використовувати у відкритому та приватному режимах.
- **Швидкість** – The транзакції Epic Cash виконуються набагато швидше, ніж у попередніх поколіннях технології блокчейн. У той час як Bitcoin потребує шести 10-хвилинних блоків для повного підтвердження транзакції, Epic-транзакції формуються в межах одного блоку підтвердження, як тільки блок буде видобуто (1 хвилина).

[1] Buterin, Vitalik, *Значення децентралізації*, 6 лютого 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Конфіденційність

Використання грошей у сучасному світі можна розуміти як колективне переміщення цінності між людьми та установами. Баланс грошей у будь-який момент часу можна відстежити, відповівши на наступні запитання:

1. Хто тримає гроші, і скільки вони тримають?

2. Хто проводить пересилання грошей, куди і скільки?

Для традиційних фіатних валют, а також і для Bitcoin, ми можемо відповісти на ці питання. Коли ми робим дослідження, мі можемо доволі багато узнати про життя людей, їх особливості споживання, права власності та транзакційних контрагентів. Можна зробити досить точні висновки про інтереси та наміри людини, простеживши передачу цінності. Без конфіденційності дані транзакцій можуть бути небезпечною інформацією в руках третіх осіб, що мають деструктивні наміри.

Використання криптовалюти за останнє десятиріччя демонструє зростання стандартів “конфіденційності” у різних реалізаціях блокчейн. Якщо врахувати, спектр конфіденційності - від повністю відкритого стану з одного боку до анонімного з іншого. Коли руйнується конфіденційність - один із важливих аспектів криптовалюти - відсутність необхідності у довірі - погіршується. Як свідчить успіх служб аналізу блокчейн Bitcoin, він відноситься більше до прозорого сегменту конфіденційності. Користувачі повинні все частіше вживати заходів для того, щоб переконатися, що вони ненавмисно не працюють з проблемним Bitcoin сегментом. Рішення Epic Cash зосереджує увагу на анонімності і відновлює цю важливу властивість криптовалюти, забезпечуючи, щоб приватність особи та конфіденційність транзакцій були вбудовані в систему на фундаментальному рівні.

Конфіденційність особи

Конфіденційність транзакції

Конфіденційність особи

Більшість криптовалют, таких як Bitcoin , зберігаються у гаманцях, адреси посилаються на відкриті ключи, які формуються з приватних ключів гаманця. Ці адреси можна вважати ідентифікаторами приватного сховища в цифровому світі. Блокчейн Epic Cash повністю усуває адреси і замість цього застосовує один великий мультипідпис з якого генеруються всі відкриті та приватні ключі на основі одноразового використання.

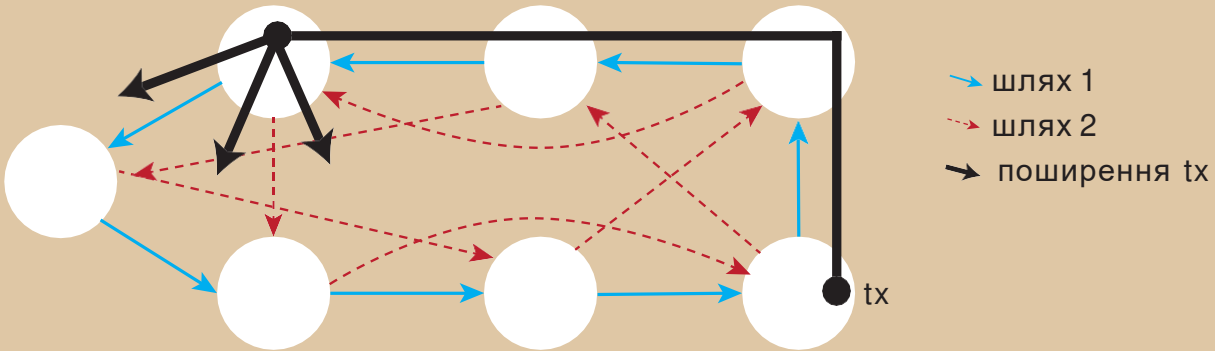
Оскільки адреси гаманця Bitcoin є локатором сховища в цифровому світі, цей гаманець можна відстежити за допомогою (IP) власника, який прив'язує власник до комп'ютера в унікальному місці в даний момент часу. Пояснюється це просто: коли відбувається транзакція з Bitcoin, транзакція транслюється з вузла зв'язку, який називається «вузол», а потім поширюється на інші вузли, які називаються «однорівневими». Потім ця інформація швидко поширюється до кожного з цих вузлів послідовно по всій мережі. Цей процес влучно названий «Протокол пліток». Простіше кажучи, кожен Bitcoin має видиме місце в Інтернеті та фізичне місце, де його можна знайти, точніше власника Bitcoin. Як зазначила журналістка Грейс Каффін, Bitcoin "не є більш секретним, ніж пошук Google із домашнього інтернет-з'єднання" [2]

Окрім усунення адрес гаманця, блокчейн Epic Cash забезпечує конфіденційність ідентичності, гарантуючи, що IP-адреси не відстежуються. Це відбувається завдяки інтеграції протоколу Dandelion++. Вдосконалюючись за попереднім, оригінальним протоколом, Протокол Dandelion++ є результатом продовження роботи семи дослідників щодо боротьби з атаками деанонімізації на блокчейн. Через Dandelion++ транзакції передаються випадковими переплетеними шляхами, а потім раптом розповсюджуються на велику мережу вузлів, як стручки квітки кульбаби при здутті з їх стебла (мал. 1). Це майже унеможливлює відстеження транзакції до їх призначення, а отже, і їхніх початкових IP-адрес.

Малюнок 1: *Анонімізація транзакцій з протоколом Dandelion++.*

Dandelion++ пересилає повідомлення по одному з двох переплетених контурів на графіку, а потім транслює за допомогою дифузії. На малюнку транзакція поширюється на суцільний шлях. Цей процес унеможливлює відстеження транзакції до її джерела, тим самим зберігаючи конфіденційність.

.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Конфіденційність транзакції

Блокчейн Epic Cash гарантує конфіденційність транзакцій, приховуючи суми та відносини відправник-одержувач у рамках транзакції. Це досягається завдяки застосуванню ідей, відомих як Confidential Transactions (CT) 4 та CoinJoin 5; ці методи у їх значній частині були розроблені Грегорі Максвеллом (розробник Bitcoin Core, співзасновник та CTO компанії Blockstream).

CT, спочатку створений Адамом Беком, а згодом уточнений Максвеллом, працює шляхом розбиття транзакцій на більш дрібні складові частини за допомогою гомоморфного шифрування, методу виконання розрахунків за зашифрованою інформацією, не розшифровуючи її для збереження конфіденційності.

Розділившись, спостерігачі не можуть побачити фактичну кількість транзакцій через засліплюючі фактори, систему, яка кидає випадкові числа в суміш фрагментів транзакцій, щоб приховати значення цих фрагментів. Зрештою, лише трансакційні сторони знають коди комунікації, тоді як транзакція перевіряється мережею лише через підтвердження того, що сума вихідних данних дорівнює сумі вхідних.

Щоб ще більше ускладнити завдання «допитливих очей», усі транзакції Epic Cash кодуються CT і потім змішуються, щоб приховати зв'язки між учасниками транзакції. Це робиться використовуючи іншу концепцію Максвелла, CoinJoin

Можемо спрощено проілюструвати CoinJoin - уявіть, що A, B і C посилають транзакції Epic у напрямку відповідно X, Y і Z. Все, що відомо, у рамках CoinJoin - це те, що A, B і C надсилають, а X, Y і Z отримують, тоді як суми транзакцій залишаються приватними. Система CoinJoin включена в Epic Cash за допомогою One-Way Aggregate Signatures (OWAS), інструментів, що об'єднують усі транзакції всередині блоку в одну.

Конфіденційність: Підсумок

Блокчейн Epic Cash захищає конфіденційність приватних осіб та їх транзакцій:

- **Відсутність адреси гаманця - в блокчейні немає ідентифікаторів місцезнаходження цифрових сховищ. Операції будуються безпосередньо між сторонами на основі "гаманець-гаманець";**
- ***Протокол Dandelion++* – приховує цифрові шляхи транзакції з IP-адреси відправника транзакції;**
- ***Confidential Transactions* – розділяє транзакції на кілька частин і вводить засліплюючи фактори в передачу цих фрагментів, так що значення параметрів транзакцій не можуть бути відстежені;**
- **CoinJoin –поєднує транзакції в пакети, щоб замаскувати відносини між транзакційними сторонами.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Гнучкість

Чарлі Лі, творець Litecoin, заявив, що гнучкість це єдине надбання часних грошей, відсутніх у Bitcoin та Litecoin, визнавши, що конфіденційність та стійкість стануть наступними полями битви для цих монет[6]. Андреас Антонополос, один із головних світових блокчейн експертів, стверджував, що "... проблемні монети є руйнівними. Якщо ви порушуєте гнучкість та конфіденційність, ви втрачаєте валюту."[7]

Гнучкість, або адаптивність - це властивість набору товарів або активів, яка забезпечує, те що окремі одиниці цього набору мають однакову цінність і є взаємозамінними. Саме це відрізняє найбільш ранні форми валюти від попередніх систем бартеру. Без впевненості у адаптивності ці гроші швидко втрачають свою корисність. Як буде показано нижче, адаптивність більшості криптовалют є невизначеною, тоді як архітектура конфіденційності Epic Cash гарантує, що вона не має такої загрози.

Більшість криптовалют, схожих на Bitcoin, за характером блокчейнів, на яких вони існують, можна відстежити через кожен гаманець, в якому вони зберігалися. Приватні треті сторони та уряди вже контролюють блокчейн Bitcoin, цей процес характеризується більш досконалими засобами для швидкого виявлення монет, використовуваних у попередніх транзакціях. Це, звичайно, призводить до занепокоєння тим, що проблемні монети колись можуть бути заборонені до здійснення транзакцій, що стане проблемою для їх наступних добросовісних власників.

У березні 2018 року U.S. Office of Foreign Asset Control (OFAC) оголосило, що розглядає питання про включення цифрових валютних адрес (гаманців) до списку «спеціально визначених громадян» (SDNs), які є суб'єктами, з якими особам або підприємствам США заборонено здійснювати операції. Ще більш тривожно, OFAC не виключає оприлюднення переліку адрес що тримають проблемні монети, що фактично може включити невинних власників проблемних криптовалют у чорні списки через походження монет, які їм належать. Це призвело до того, що професор юридичного факультету Нью-Йоркського університету Ендрю Хінкс відмовився від " Kiss fungibility goodbye", і що громадськість повинна очікувати "премії за щойно добуті монети або простежені «чисті» монети ..." [8].

Приймаючи до уваги ці події, не важко уявити потенційні проблемі у криптовалюті та зниження активності чи навіть банкрутство багатьох криптовалют. Однак Epic - одна з небагатьох криптовалют, яка цілком уникає цієї проблеми завдяки сильним особливостям конфіденційності, описаним раніше у цій статті. Видаляючи зв'язок між особою та власністю та відносинами між транзакційними сторонами, Epic ніколи не може бути ототожнений до конкретної людини чи діяльності. Таким чином, вартість Epic залишається незалежною від особливостей поведінки його користувачів та забезпечує високий ступінь конфіденційності та безпеки, що унеможливлює втручання учасників злочинних, фінансових чи політичних угрупувань.

.

> **“ … ПРОБЛЕМНІ МОНЕТИ ДЕСТРУКТИВНІ. ЯКЩО ВИ ВТРАЧАЄТЕ ПРИВАТНІСТЬ І ГНУЧКІСТЬ, ВИ ВТАЧАЄТЕ ВАЛЮТУ. ”**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Масштабованість

Epic Cash - це блокчейн MimbleWimble, він дає можливість досягти масштабування через викидання викидає зайвих даних транзакцій.

Функціональність Cut-Through гарантує, що цей блокчейн здатний масштабуватися ефективніше більшості криптовалют, включаючи Bitcoin, і що нові вузли можна створювати з мінімальними інвестиціями в апаратне забезпечення. Залишаючись ефективним з точки зору масштабування, він спиряє формуванню розсіяної мережі та децентралізації. Крім того, кожна нода Bitcoin повинна зберігати весь блокчейн (всі блоки), проте ноди Epic Cash можуть внести свій внесок у мережеву безпеку на основі невеликого набору блоків.

Більшість криптовалют потребують безстрокового зберігання всіх даних про транзакції у своїх блокчейнах. В даний час блокчейн Bitcoin за обсягом зростає на 0,1353 ГБ кожен день, в той час як блокчейн Ethereum збільшується ще швидше, ця цифра становить 0,2719 ГБ на день. Якщо блокчейн Bitcoin продовжить зростати зі своїми поточними темпами, він досягне обсягу у 6 ТБ до моменту видобутку останнього блоку винагороди в 2140 році. Ethereum до такої ж дати складе 10 ТБ. У більшості блокчейнів без використання MimbleWimble транзакції повинні перевірятись вузлами по всьому світу. Зі збільшенням обсягу даних збільшується навантаження на кожен вузол.

Навіть у випадку 200 Гб (приблизний розмір блокчейну Bitcoin у поточному стани) для синхронізації даних потрібна стабільна мережа та можливість швидкого читання та запису диска.

Отже, майнінг стає все більш централізованим, це бізнес великих пулів, які використовують дорогі обчислювальні ресурси. Якби вся історія блокчейну Bitcoin зберігалася на Epic Cash, вона займала б майже на 90% менше місця. Менший обсяг – це виграш у швидкості, тому що для кожної транзакції потрібно менше часу для оброблення, передачі та захисту.

.

MimbleWimble вирішує цю дилему за допомогою інноваційного методу блокчейн обрізки, яка називається "Cut-Through". Щоб зрозуміти, як працює "Cut-Through", найкраще спочатку подивитися, як формуються транзакції та блоки в блокчейні MimbleWimble.

.

Вхідні дані:

Посилання на старі вихідні дані;

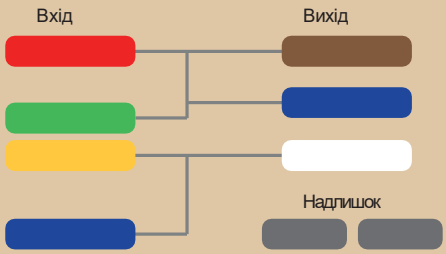
Вихідні дані:

Confidential Transaction вихідні дані та **перевірка діапазону**;

Надлишок:

Різниця між входом на виходом, плюс **підписи** (для аутентифікації)

Малюнок 2:
Транзакції MimbleWimble.



[9] Li, Crypto, *Blockchain's Big Data Problem*, 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Всі блоки Epic Cash складаються:

Дерево Merkle транзакційних входів;

Дерево Merkle транзакійних виходів та доказів;

Список надмірних значень та підписів

На малюнках 2 і 3, адаптованих з презентацій Ендрю Поельстра, ми бачимо щойно видобутий Epic, представлений білими вхідними клітинками. Також кольорові клітинки представляють результати з відповідними витраченими входами. За допомогою процесу вирізання видаляються входи та відповідні витрачені виходи, щоб звільнити місце в блоці, що зменшує кількість даних, які потрібно зберігати у блокчейні. Хоча транзакції видаляються з реєстру, інші зайві ядра (всього 100 байт) постійно підтверджують, що транзакції відбулися.

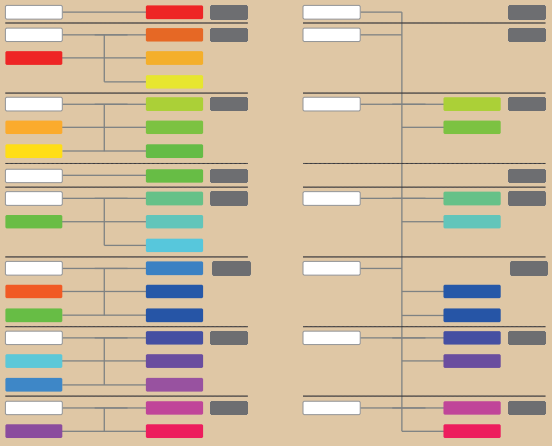
Оскільки блоки продовжують створюватися, MimbleWimble застосовує Cut-Through, так що в довгостроковій перспективі все, що залишається - заголовки блоків (приблизно 250 байт), невитрачені транзакції та ядра транзакцій (приблизно 100 байт). Grin, друга реалізація MimbleWimble, що вже була запущена, показала, що блокчейн MimbleWimble із аналогічною кількістю транзакцій як у чейні Bitcoin буде складати десь 10% від розміру чейна Bitcoin. Крім того, розмір вузла буде декілька ГБ для чейна Bitcoin і потенційно може бути оптимізований до кількох сотень мегабайт.[12]

Це – помітний контраст з Bitcoin, де весь блокчейн повинен зберігатися кожним вузлом. З часом, коли ефективність блокчейну Epic Cash зростатиме відносно блокчейну Bitcoin, також зростатиме ефективність витрат щодо участі вузлів у мережі Epic Cash. Більш низькі бар'єри для участі допомагають забезпечити вирішальну стійкість на рівні вузла базової мережі.

Завдяки впровадженню MimbleWimble та застосуванню обрізки ланцюга за допомогою процесу Cut-Through, блокчейн Epic Cash пропонує масштабованість способом, який часто не помічається спільнотою криптовалют. Проте, який відображає суть проектів Bitcoin та їх однодумців: децентралізацію. Незалежно від того, скільки транзакцій за секунду монета може обробити, яка користь, якщо її не можна підтримувати широкою та різноманітною мережею? Якщо вимоги до пам'яті такі, що перевірка в кінцевому рахунку тяжіє до сильних майнінг конгломератів, тоді усі зусилля створити децентралізовану екосистему марні. Щоб забезпечити додаткову пропускну спроможність, запровадження Lightning-style Layer2 – це короткострокова мета в дорожній мапі розвитку Epic Cash.

Малюнок 3: Транзакції MimbleWimble перед та після Cut-Through.

Вирізання транзакційних складових



[10] SFBitcoin Developers, *MimbleWimble with Andrew Poelstra,* 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, *Grin Blockchain Size,* December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, *Introduction to Mimblewimble and Grin,* 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Грошова політика

Грошова політика Epic Cash і Bitcoin дуже схожа. Циркуляція Epic Cash спочатку швидко зростає, а потім синхронізується з циркулюючою пропозицією Bitcoin в 2028 році. Згодом вона зростає зі зниженням швидкісті до досягнення максимальної пропозиції в 21 мільйон Epic в 2140 році. Epic Cash має змогу стати безпечним довгостроковим активом, оскільки загальна циркуляція відома в будь-якій момент часу протягом життєвого циклу монети і завершується фіксованою максимальною емісією. Грошова політика Epic Cash характеризується наступними чотирма ознаками:

- Швидка емісія за дев'ять років життєвого циклу, протягом яких потрібно видобути 20,343,750 Epic (96,875% від загальної кількості). Точні показники майнінга викладені в розділі Графік емісії цього документу;
- Максимальний запас в 21 мільйон Epic буде досягнуто в 2140 році, приблизно в той самий час, коли Bitcoin досягне максимальної пропозиції в 21 мільйон одиниць;
- Швидкість емісії та майнінгу Epic синхронізується зі швидкістю Bitcoin в Epic Singularity близько 24 травня 2028 р. Після цього швидкість зменшується зі зростаючою інтенсивністю, в той час як циркуляційна пропозиція зростає зі зменшенням швидкості;
- Epic має розрядність 8, так що: 1 Epic дорівнює 100000000 freeman (так само, як 1 Bitcoin дорівнює 100000000 сатоші).

Грошова політика Epic Cash моделюється за моделлю Bitcoin з наступних причин:

- Узгодженність з економічними основами Bitcoin, а саме, що дефіцит та передбачуваність циркуляційного постачання лежать в основі характеристик;
- Громадськість вже знайома з моделлю Bitcoin та обладає певним досвідом за останні десять років з моменту створення. Приблизно синхронізувавшись з циркулюючою пропозицією Bitcoin та відображаючи структуру максимальної пропозиції та поділу Bitcoin, Epic має менше проблем для масового прийняття.

VI. План емісії

Epic Cash налічує в цілому 33 етапи видобутку, кожний визначається зменшенням винагороди за блок, у порівнянні з попереднім етапом. Генезіс Epic Genesis, дата блоку №1 – це серпня 2019. Блоки видобуваються за одну хвилину. Перші п'ять етапів дадуть майже 97% максимальної пропозиції Epic, що синхронізує 20 років майнінгу Bitcoin приблизно за дев'ять років. Це шанс "повернути час" для тих, хто пропустив вражаючий підйом Bitcoin.

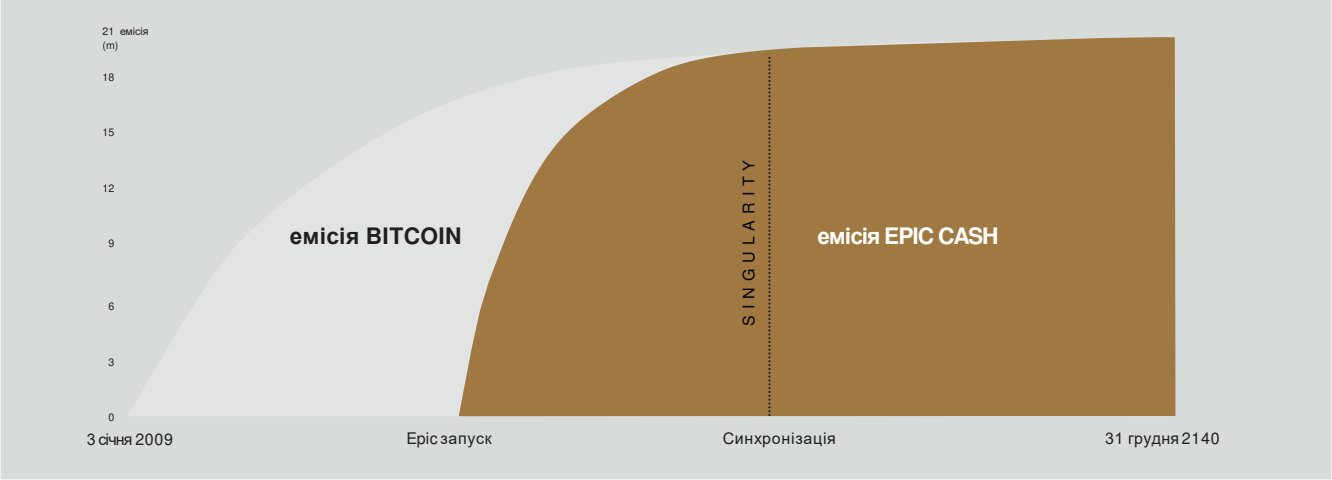
The emission schedule in table 1 outlines the start and end dates of the first seven mining eras, their corresponding block rewards, and the ensuing circulating supplies for each era. The eras 8 to 33 are not included in the table for brevity's sake. For those eras, it should suffice to understand that each subsequent era will have a block reward that is half the amount of the reward of the preceding era, exactly as in Bitcoin. The amount of Epic emitted during each of these eras will be the sum of block rewards within the 4-year era (approximately 1460days).

У Epic Singularity (2028) циркулююча пропозиція Epic перетинає кількість циркулюючої пропозиції Bitcoin, і в цей момент Epic Cash приймає схему винагороди та зменшення нагороди як у моделі Bitcoin, за якою винагорода за блок зменшується вдвічі кожні чотири роки. Єдиним винятком є те, що блоки Epic продовжують видобуватись зі швидкістю 1 хвилина, порівняно зі швидкістю Bitcoin 1 блок кожні десять хвилин. Приймаючи це, циркулююча пропозиція Epic синхронізує приблизні співвідношення з циркулюючою пропозицією Bitcoin до кінця їх майнінгу.

Таблиця 1: Графік емісії для перших семи майнінг етапів. Дати - це більш близькі наближення.

Етап	1	2	3	4	5	SINGULARITY	6	7
Винагорода за блок	16	8	4	2	1		0.15625	0.078125
Початок	Сер. 1, 2019	Чер.29, 2020	Жов.11, 2021	Чер. 3, 2023	Сер. 10, 2025		Трав. 24, 2028	Трав. 22, 2032
Закінчення	Чер.29, 2020	Жов.11, 2021	Чер. 3, 2023	Сер. 10, 2025	Трав. 24, 2028		Трав. 22, 2032	Трав. 20, 2036
Строк (днів)	334	470	601	800	1019		1460	1460
Початкова циркуляція	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Кінцева циркуляція	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% від максимальної емісії	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Figure 4: Epic and Bitcoin emission schedules.



VII. Майнінг

Блокчейн Epic Cash сприяє децентралізації, вітаючи широкий спектр обладнання для майнінгу. Майнінг Epic спочатку буде доступний для CPU, GPU, та ASICs з використанням алгоритмів: RandomX, ProgPow, та CuckATоо31+. Algorithms can be trivially hot-swapped without compromising the integrity of the chain.

1 RandomX та CPU

RandomX це алгоритм Proof-of-Work (PoW) оптимізований під CPU. Він використовує рандомізоване виконання програм за допомогою декількох memory-hard методів для досягнення наступних цілей: :

- Запобігання розвитку одночипових ASICs;
- Мінімізація переваги ефективності спеціалізованого обладнання перед процесорами.

Mining Майнінг Epic за допомогою процесорів вимагає постійного виділення 2 ГБ(RAW), 16 КБ кешу L1, 256 КБ кешу L2 та 2 МБ кешу L3. Для пристроїв на Windows 10 потрібно 8 Гб або більше оперативної пам'яті. Можливо, що одного дня в не надто віддаленому майбутньому мобільні телефони можуть стати життєздатними вузлами манінгу. Рання інтеграція процесорів у мережу майнінгу Epic Cash - це відмінна можливість для багатьох людей лише за допомогою скромних обчислювальних засобів заробити винагороди за блок, допомагаючи забезпечити роботу у мережі Epic Cash.

2 ProgPow та GPU

Programmatic Proof-of-Work (ProgPow) це алгоритм який залежить від пропускної здатності пам'яті та основного обчислення рандомізованих математичних послідовностей, які використовують переваги багатьох обчислювальних функцій GPU і тим самим ефективно фіксують загальну енерговитрату обладнання. Оскільки ProgPow розроблений спеціально для того, щоб повністю використовувати переваги графічних процесорів, досягти значно більшої ефективності за допомогою спеціалізованого обладнання важко і дорого. Як такий, алгоритм ProgPow знижує стимули для великих пулів ASIC для випередження конкурентних графічних процесорів, як це часто трапляється з багатьма іншими алгоритмами PoW, такими як SHA-256 Bitcoin. Графічні процесори, хоча і не такі поширені, як процесори, все ще є загальнодоступними. Завдяки технологічному розвитку, керованому Nvidia та AMD, GPU можуть паралельно обробляти багато кратних рішень. Саме завдяки такому поєднанню розвовсюдженності та високої потужності процесори GPU забезпечать основу більшої частини майнінг діяльності протягом початкових етапів, як наведені в таблиці 2.

3 CuckATоо+31 та ASIC

CuckATоо31

+ це ASIC версія алгоритму Cuckoo Cycle, розробленого голландським комп'ютерним вченим Джоном Тромпом. Близький стійкого до ASIC CuckARоо29, CuckATоо31+ генерує випадкові двосторонні графи та представляє майнерам завдання знайти петлю заданої довжини 'N', що проходить через вершини цього графа.

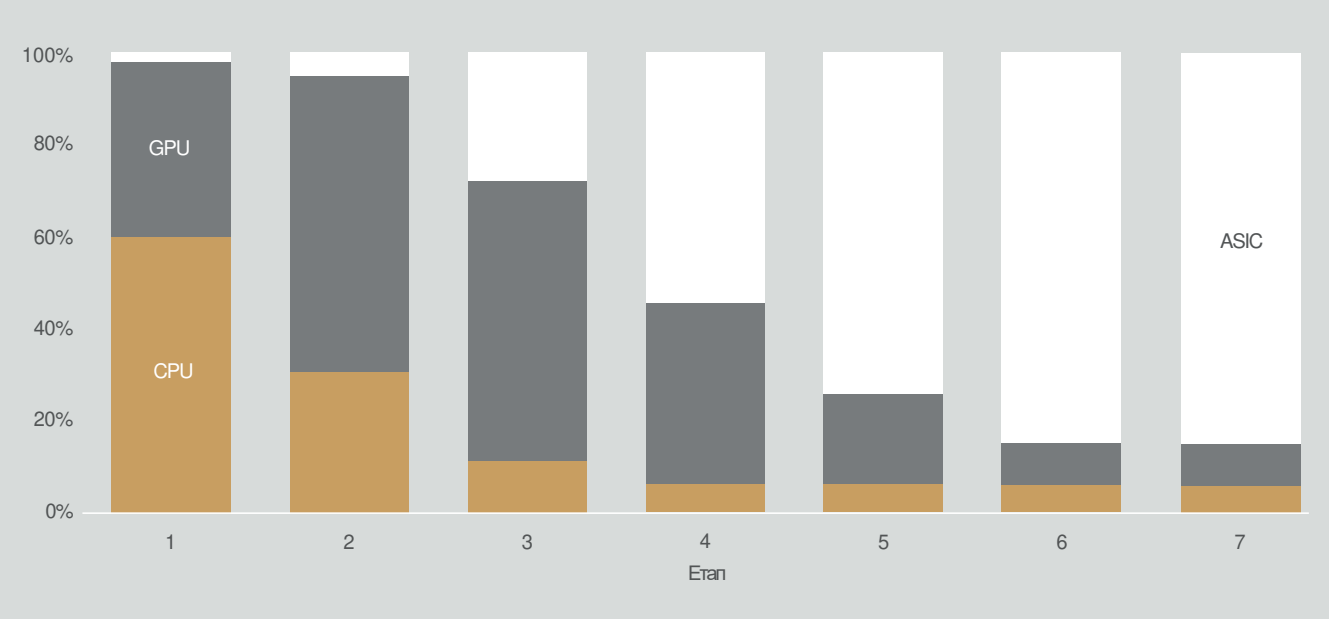
[13] Tevador, *RandomX*, 28 March, 2019, https://github.com/tevador/RandomX

This Це завдання, пов'язане з пам'яттю, та це означає, що час, потрібний на рішення пов'язаний з пропускною здатністю пам'яті, а не швидкістю процесора або GPU. В результаті алгоритми Cuckoo Cycle виробляють менше тепла і споживають значно менше енергії, ніж традиційні алгоритми PoW. Зручний ASIC CuckATоо31 + дозволяє покращити ефективність роботи графічних процесорів, використовуючи сотні МБ SRAM, залишаючись вузьким місцем пам'яті I/O 14. Зрештою, ASIC пропонують найбільшу потенційну економію з трьох варіантів майнінгу. В інтересах інклюзивності, однак, хоча їм на початку виділяється невелика частка винагороди за видобуток відносно CPUs і GPUs, зрештою ASIC візьме на себе мажоритарний пакет винагород, припускаючи, що екосистема виробників пристроїв для CuckATоо31 + буде конкурентоспроможною.

Таблиця 2: Розподіл нагород за майнінг. Підлягає перегляду. Пропорції спрямовані на досягнення максимальної децентралізації, відповідно до довгострокових інтересів мережі.

Етап	1	2	3	4	5	6	7
Днів	334	470	601	800	1019	1460	1460
CPU	60%	30%	10%	5%	5%	5%	5%
GPU	38%	65%	62%	40%	20%	10%	10%
ASIC	2%	5%	28%	55%	75%	85%	85%

Маліюнок 5: Виплати винагороди за кожний етап згідно таблиці 2 (може змінюватись).



[14] Le Sceller, Quentin, *An Introduction to Grin Proof-of-Work*, 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Видатки на майнінг

Починаючи з Epic Genesis (2019) і закінчуючи Epic Singularity (2028), під час процесу майнінгу відбувається розподіл Epic, який перенаправляється, як видатки від майнингу, до Фонду EPIC Blockchain.

Фонд EPIC Blockchain сформований для сприяння технічному розвитку та популярізаціїпроекту Epic Cash протягом перших років від його створення шляхом ведення маркетингової діяльності та розвитку партнерських відносин у галузі фінансових технологій.

Після Singularity роль Фонду EPIC візьме на себе Розподілена автономна корпорація EPIC (EPIC), яка буде розроблена фондом до цієї дати.

Фонд EPIC Blockchain фінансується у відсотках від видобутку, що віднімається від винагороди за блок відповідно до наступних річних ставок:

Таблиця 3: Щорічні розміри внесків до Фонду у відсотках від винагороди за майнінг.

Рік	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
%від винагороди	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Висновок

Мета Epic – бути визнаним «децентралізованим цифровим сріблом», з позицією Bitcoin як «децентралізоване цифрове золото». Завдяки повторному впровадженню гнучкості на набагато більш енергоефективної апаратну основу обладнання, Epic Cash повертає баланс потужності на користь окремих користувачів, на відміну від останніх тенденцій централізації. Поєднання економіки Bitcoin, теорії ігор та перевіреної формули підтвердження роботи з найкращими сучасними блокчейн технологіями призводить до надійної, незмінної та децентралізованої валюти (Epic), яка є масштабованою та захищає конфіденційність її користувачів. Блокчейн Epic Cash відкритий, публічний, без кордонів. Він зберігає конфіденційність та гроші своїх користувачів і винагороджує тих, хто розгортає своє обладнання в підтримку мережі через майнінг. Кожна монета Epic видобувається через підтвердження роботи. Постачання починається з нуля, і мережа вважається справною, запущеною функціональною тестовою мережею.

Основні фактори Epic Cash:

- **Початок майнінгу серпня 2019.**
- **Блокчейн Epic Cash базується на MimbleWimble.**

  Визначальними рисами протоколу є:

  1. **Cut-Through** – вилучення зайвої інформації з блокчейну для підвищення ефективності використання простору, заохочення широкої участі у валідації мережі та децентралізації управління;
  2. ***CoinJoin*** – групування транзакцій всередині блоку для забезпечення гнучкості криптовалюти Epic;
  3. ***Протокол Dandelion++*** – розповсюдження транзакцій шляхом спілкування по переплетених каналах та розповсюдження по широкій мережі вузлів, розривання зв'язків між транзакціями та їх походженням;
  4. ***Без адреси гаманця*** – використання великої багатосигнатури для генерування приватних ключів одноразового використання для трансакційних сторін, виключення потреби в адресах гаманця.

- **Грошова політика Epic Cash** покликана синхронізувати пропозицію монет у циркуляції Epic з пропозицією Bitcoin приблизно за дев'ять років і досягти такої ж максимальної пропозиції в 21 мільйон одиниць одночасно з Bitcoin у 2140 році. Ця зменшувана інфляційна політика гарантує прозорість, передбачуваність поставок та дефіцит, сприяючи безпеці довгострокового зберігання цінності.

- Майнінг, який включає в себе CPU, GPU, і ASIC що працюють за участі відповідних алгоритмів RandomX, ProgPow та CuckATоо31 +, з метою полегшити масове прийняття та ефективність мережі.

IX. Технічні специфікації

Найменування: EpicCash

Найменування монети: Epic

Час блоку: 60 секунд

Розмір блоку: 1 MB

Початкова циркуляція: 0

Кінцева циркуляція : 21,000,000

Генезіс блок: серпня 2019

Консенсус: RandomX (CPUs), ProgPow (GPUs) and CuckAToo31+ (ASICs)

Поислання:

www.epic.tech

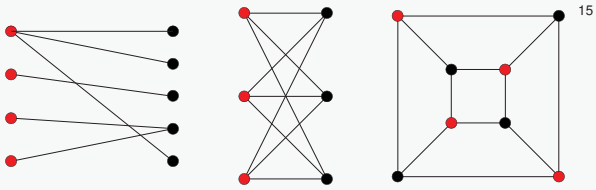
t.me/EpicCash – Telegram

t.me/EpicCashUkrainian

X. Словник

ASIC Application Specific Integrated Circuits; чипи, розроблені для майнінгу певної монети

Bipartite граф набір графічних векторів, розкладених на два роз'єднані набори, жоден не є суміжним.



Засліплюючий фактор випадковий елемент, що вводиться в цифрове повідомлення для полегшення шифрування; загальна угода між двома сторонами, яка шифрує входи та результати в цій конкретній транзакції, а також публічні та приватні ключі транзакційних сторін[16].

Винагорода за блок новий Epic, що поширюється мережею, як винагорода за обчислення, виконані для перевірки транзакцій у новому блоці.

Кеш апаратний чи програмний компонент, який зберігає дані, щоб майбутні запити на ці дані могли бути швидше оброблені.

Циркуляція кількість Epic, що існує в даний момент часу.

CPU Central Processing Unit: комп'ютерний компонент, відповідальний за інтерпретацію та виконання більшості команд з іншого апаратного та програмного забезпечення.

Cut-Through Процес MimbleWimble за допомогою якого видаляються входи та відповідні виходи, щоб звільнити місце в блоці, зменшивши кількість даних, необхідних для зберігання на блокчейн.

Децентралізація форма розповсюдженості операцій та управління мережею.

Емісія створення нового Epic, за заробляється майнерами через винагороду за блок. Epic створюється кожні 60 секунд, оскільки транзакції підтверджуються в блокчейні.

Epic Singularity момент часу, в який циркулююча пропозиція Epic синхронізується з циркуляцією Bitcoin (травень 2028 р.).

Надлишок (MimbleWimble) різниця між виходами та входами, плюс підписами (для автентифікації та перевірки відсутності інфляційних процесів).

Гнучкість властивість товару або товару, завдяки якому окремі одиниці по суті є взаємозамінними, і кожна його частина не відрізняється від іншої частини.

Genesis (подія) майнінг першого блоку, запуск блокчейну.

GPU Graphics Processing Unit: що містить програмований відео чіп (процесор) для функцій відображення. Споживчі графічні процесори можуть бути дуже зручними для майнінгу криптовалют.

Халвінг (Bitcoin) виникає кожні 4 роки. винагорода зменшується на 50% після кожної події.

Хеш значення, обчислене з базового вхідного блоку за допомогою функції хешування.

Алгоритм хешування (функція) математичний алгоритм, який відображає дані довільного розміру на хеш фіксованого розміру, що використовується для генерації та перевірки цифрових підписів, кодів аутентифікації повідомлень (MAC) та інших форм аутентифікації.

Незмінність гомоморфного шифрування метод виконання обчислень за зашифрованою інформацією, не розшифровуючи її, (в програмуванні) стан, в якому об'єкт не може бути змінений після його створення.

Input (MimbleWimble) компонент транзакції MimbleWimble, що представляє сторону, що відсилає транзакцію; створену за результатами попередніх транзакцій.

I/O input/output; зв'язок між системою обробки інформації, такою як комп'ютер, та зовнішнім світом, можливо, людиною чи іншою системою обробки інформації.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, *Grin Coin and MimbleWimble: An Introductory Guide*, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Максимальна емісія	кількість Epic, яку потрібно досягти , сума кінцевої циркуляції фіксована , вона не буде перевищувати певну суму (21 млн. Epic).
Memory-Hard	використання великої кількості оперативної пам'яті для запобігання спроб запуску паралельних з'єднань. Функції з Memory-Hard - це алгоритми, у яких час обчислень визначається в основному наявною пам'яттю для зберігання даних.
Дерево Merkle	структура даних, що використовується в програмах. У блокчейнах дерева Merkle дозволяють ефективно та безпечно перевіряти вміст у великих структурах даних.
MimbleWimble	протокол викладений учасником, що стоїть за посередником Томом Елвісом Джедусором, у чаті розробників Bitcoin.
Мультіпідпис	схема цифрового підпису, яка дозволяє групі користувачів підписати один документ. Зазвичай алгоритм створює спільний підпис, який є більш компактним, ніж колекція різних підписів від усіх користувачів [17].
Нода	елемент системи, комп'ютер, який підключається до мережі блокчейн і розгалужується на інші вузли всередині мережі, щоб поширювати інформацію про транзакції та блоки одночасно.
One Way Aggregate Signature (OWAS)	підпис транзакції, що складається з нескінченого числа підписів, який зашифрований таким чином, що дуже важко виявити окремі підписи, що входять до сукупності.
Output (MimbleWimble)	компонент транзакції MimbleWimble, що представляє отримання транзакції; використовується як вхід для подальших транзакцій.
Схема Pedersen Commitment	криптографічний примітив, який дозволяє доказувачеві взяти вибране значення, не розкриваючи жодної інформації про нього, і без того, щоб довідник міг скасувати поступку на значення.
Приватний ключ	невеликий обсяг коду, який поєднується з відкритим ключем для встановлення алгоритмів для шифрування інформації. Це частина складової відкритого ключа під час шифрування асиметричного ключа та використовується для перетворення у формат, що можна прочитати.
Proof of Work (PoW)	фрагмент даних, який складний для формування (дорогий та забирає багато часу, але його легко перевірити іншим. Докази роботи часто використовуються при генерації блоку (майнінг).
Публічний ключ	публічний ключ створюється шляхом шифрування відкритого ключа, який використовує алгоритми шифрування асиметричного ключа. Відкриті ключі використовуються для перетворення повідомлення у нечитабельний формат.
RAM (Random Access Memory)	мікросхеми швидкого доступу до даних в обчислювальному пристрої, де зберігаються операційна система (ОС), прикладні програми та дані в поточному використанні, основна мета – швидке отримання за допомогою процесора.
Rangeproof	перевірка діапазону, яка підтверджує, що сума вхідних транзакцій більша за суму транзакції і що всі значення транзакції є додатними. Діапазони безпеки гарантують, що грошова маса не була підроблена.
(Цифровий) підпис	стандартна частина блокчейн протоколу, в основному використовується для забезпечення транзакцій, передачі інформації, управління контрактами та у інших випадках, коли важливе виявлення та запобігання зовнішним втручанням. Вони забезпечують три переваги зберігання та передачі інформації на блокчейні : • Підписи виявляють, чи були підроблені дані; • Перевіряють участь певної сторони в угоді; • Можуть бути юридично обов'язковими.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) Пам'ять з випадковим доступом, яка зберігає системи даних у своїй пам'яті до тих пір, поки в систему подається живлення.
Пропускна здатність	кількість транзакцій в секунду, які можуть бути забезпечені заданим криптовалютним протоколом.
Trustlessness (відсутність необхідності довіри)	якість криптовалютної мережі криптовалют дотримуватись правил протоколу без виконання перевірки централізованою стороною.

[17] Bellare, Mihir, Neven, Gregory, 2007, *Identity-based Multi-signatures from RSA*, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC - приватна інтернет валюта