УДК: 004.043

АНАЛІЗ ОСНОВНИХ ПРИНЦИПІВ ТЕХНОЛОГІЇ BLOCKCHAIN

Данильчук Р. К., кандидат технічних наук, Жураковська О. С.
Національний технічний університет Україїни «Киіївський політехнічний інститут імені Ігоря Сікорського», Україїна, Киіїв

В даній статті наведено детальний аналіз принципів технології Blockchain. На сьогоднішній день переважна кількість інформації про цю мережу являється поверхневою [10, 11, 13, 14, 17]. У своїй роботі я аналізую, яким чином ця технологія забезпечує захищеність, розподіленість і відкритість. А також, на відміну від попередніх дослідників, які розглядають лише прості атаки на блокчейн [1, 3, 12, 15, 16,], я приводжу приклад найнебезпечніших дій зловмисних учасників. Данна стаття буде достатньо цікавою для читачі, що уже "в темі", адже відкриває нові горизонти в розумінні Blockchain.

Ключові слова: технологія blockchain, блокчейн, технологія Накомото, блок, майнер, учасники, записи, ключ, принципи.

Данильчук Р. К., кандидат технических наук, Жураковская О. С. Анализ основных принципов технологии blockchain / Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Украина, Киев

В данной статье приведен подробный анализ принципов технологии Blockchain. На сегодняшний день подавляющее количество информации об этой сети является поверхностной [10, 11, 13, 14, 17]. В своей работе я анализирую, каким образом эта технология обеспечивает защищенность, распределенность и открытость. А также, в отличие от предыдущих исследователей, рассматривающих только простые атаки на блокчейн [1, 3, 12, 15, 16,], я привожу пример опасных действий вредоносных участников. Данная статья будет достаточно интересной для читателей, которые уже "в теме", ведь открывает новые горизонты в понимании Blockchain.

Ключевые слова: технология blockchain, блокчейн, технология Накомото, блок, майнер, участники, записи, ключ, принципы.

R. Danylchuk, PhD, senior lecturer, O. Zhurakovska Analysis of the basic principles of blockchain technology / National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Ukraine, Kyiv

This article provides a detailed analysis of the principles of Blockchain technology. To date, the vast majority of information on this network is superficial. In my work, I analyze how this technology provides security, distribution and openness. And also, unlike previous researchers who consider only simple attacks on blockade, I give an example of the most

dangerous actions of malicious participants. This article will be interesting enough for the reader, which is already "in the topic", because it opens new horizons in the sense of Blockchain.

Key words: technology blockchain, blockade, technology Nakomoto, block, minaret, participants, records, key, principles.

Вступ. Blockchain - технологія зберігання інформації, яка змінить світ не менше, ніж у свій час це зробив Інтернет.

Все частіше люди по всьому світу стикаються з терміном "блокчейн", але далеко не всі розуміють як саме побудований механізм системи.

Данна технологія може зробити досить вагомий внесок у розвиток сучасного бізнесу і полегшення життя суспільства, тому заслуговує на увагу і доскональне її вивчення.

Аналіз консенсусу ланцюжку блоків Blockchain (консенсус Накамото) був свідомо важким завданням. Попередні дослідження технології, а саме роботи Гарая, Кіаяса і Леонардоса, стверджують, що мережеві канали повністю синхронні, тобто дані миттєво передаються, без затримок. Але вони розглядають лише конкретні атаки на систему (Nakamoto'08; Sampolinsky і Zohar, FinancialCrypt'15) [8].

У цій роботі я аналізую максимально сильну атаку і показую, що механізм консенсусу Blockchain задовольняє принцип розподіленості в асинхронній мережі із певними затримками, які апріорно обмежені.

Також, на прикладі досліджень Декера і Ваттенхофера, аналіз доводить, що блокчейн Накамото відповідає принципам безпечності і відкритості, тому заслуговує на застосування на загальнодержавному рівні [6].

Зарубіжні країни уже доволі давно оцінили значущість блокчейн, поступово ця технологія запроваджується і в Україні.

Зокрема, 21 червня 2017 року була прийнято постанова про перехід Державного земельного кадастру України на технологію Blockchain.

Мета статі: ознайомити читача с детальним аналізом основних принципів технології Blockchain.

Завдання статті: донести до читача сутність принципів роботи технології "Blockchain" на прикладі їх детального аналізу та показати механізм забезпечення відкритості, безпечності і розподіленості.

Виклад основного матеріалу. Технологія Blockchain дозволяє досягти консенсусу в так званому дозволі застосування - будь-хто може приєднатися (або залишити) систему, а її функціонування не залежать від ідентичності учасників. Така геніальна технологія запобігає «атаки Сібіл» (де противник породжує будь-яку кількість нових учасників), покладаючись на обчислювальні головоломки.

Розподілені системи історично аналізувалися в закритому режимі, в якому обидва учасники системи, а також їх особистості, є загальновідомими. Відхід від цієї моделі почався з розробки тимчасових систем для обміну файлами, таких як Napster і Gnutella.

Успіх цих систем привів до створення академічно розроблених систем: Freenet, CAN, Chord і Pastry, які пропонують надлишкове файлове сховище, розподілене хешування, вибір найближчих серверів і ієрархічне присвоєння імен.

Новим аспектом цих тимчасових систем є те, що вони не потребують дозволу - кожен може приєднатися до системи, або залишити її (без отримання дозволу від централізованого або розподіленого органу).

Оскільки учасники можуть безперервно приєднуватися і виходити з системи, успішні технології «без дозволу» мають певні дефекти. На жаль, згадані системи, хоча і надійні з одного боку, але вони не були розроблені, щоб терпіти атаки зловмисних учасників. До того ж, не було ніякої гарантії, що два учасники, які запитують один і той же файл, не отримають різні його версії, навіть не дізнавшись про це.

На перший погляд можна подумати, що використання стандартного консенсусу / візантійського (наприклад, CL99, MA05, Lam10, Lam11) можуть допомогти подолати цю проблему. Та суть в тому, що такі системи потребують, щоб значна частина учасників була добросовісною. Але в системах, які не потребують «дозволу для установки», зловмисник може просто встановити так звану «атаку sybil», створюючи безліч учасників (які він контролює) і, таким чином, зможе контролювати більшість учасників системи.

У 2008 році Накамото запропонував свою технологію Blockchain, реалізовану в системі Bitcoin, яка долає вищезгадані проблеми, спираючись на ідею обчислювальних блоків.

Замість того, щоб намагатися забезпечити надійність, коли більшість учасників чесна (так як учасники можуть бути легко створені в режимі «без дозволу»), він намагається забезпечити надійність, спираючись на обчислювальні потужності технології.

Такий принцип захищеності технології Blockchain досить важливий для підтримки системи фінансових транзакцій.

Цифрова валюта bitcoin Накамото має сильні потужності для запобігання шахрайства та подвійних атак. Ряд наступних цифрових валют та схем мікро-платежів, засновані на ідеї ланцюжка блоків.

Крім того, фінансові компанії оголосили про наміри використовувати блокчейн для зниження витрат транзакцій, усунення геополітичних бар'єрів для передачі активів і узгодження відмінностей між системами.

Блокчейн, грубо кажучи, є методом підтримки публічної,

незмінною і впорядкованої книги записів (наприклад, в додатку біткойн ці записи є лише транзакціями); тобто, записи можуть бути додані в кінець книги в будь-який час (але тільки в кінець ланцюжка).

Аспектом консенсусного механізму Накамото є те, що він функціонує в умовах «без дозволу».

Грубо кажучи, кожен учасник системи блокчейн зберігає свій власний «ланцюжок» «блоків», записів / повідомлень.

Кожен блок складається з, так званої, трійки (h-1, η, m), де h-1 – ключ попереднього блок, m - запис блоку, а η – ключ блоку, отриманий з пари h-1 і m (рис.1).

Рис.1 Структура блоку Blockchain

Технологія Накамото характеризується параметром *p*, який називається параметром «складності» і являється доказом правильного функціонування системи, якщо η-ключ, такий як H (h-1, η, m) < D*p*, де H - хеш-функція (змодельована випадковим чином), а D*p* встановлюється так, що ймовірність того, що вхідні дані задовольняють співвідношення, менше *p*.

Так як обчислювальні потужності мережі непостійні, цей параметр перераховується учасниками мережі через кожні 2016 блоків таким чином, щоб підтримувати середню швидкість формування блоків на рівні 2016 блоків в два тижні. Таким чином, 1 блок повинен створюватися приблизно раз в десять хвилин. На практиці, коли обчислювальна потужність мережі зростає - відповідні часові проміжки коротше, а коли знижується - довше.

Перерахунок складності з прив'язкою до часу можливий завдяки наявності в заголовках блоків часу їх створення. Воно записується в Unix-форматі з системних годинах автора блоку (якщо блок створюється в пулі, то по системним годинам сервера цього пулу).

До того ж раніше додані записи не можуть бути видалені або змінені. Записи кожного блоку відкриті для всіх користувачів Blockchain. Учасники можуть легко переглянути дані будь-якого з блоків. Зміну інформації в них легко відстежити, так як при цьому змінюється цифровий підпис. Це захищає дані від недобросовісних учасників. В цьому полягає принцип відкритості технології Blockchain.

Щоб перевірити дані, після її отримання, учасники для деякого запису m обирають випадкову η і перевіряють, чи є η дійсним доказом роботи w.r.t. m і h-1, де h-1 - показник останнього блоку поточного ланцюжка. Якщо це так, учасник розширює власний ланцюжок блоків і передає блок всім іншим учасникам.

Основне питання з таким підходом полягає в тому, чи закінчуються в кінцевому підсумку чесні учасники чи система переходить в стан, коли учасники мають нерозподілені локальні мережі.

Вимога, щоб всі учасники погодилися з усім ланцюжком, є занадто сильною вимогою для мережі з затримкою даних (що передбачено технологією блокчейн). Наприклад, деякі учасники отримали «останній блок», а інші - ні.

Як стверджував Накамото, відповідне поняття розподіленості для ланцюжка блоків, яке називається T-consistency - повинно вимагати, щоб чесні учасники погоджувалися з поточним блоком, за винятком потенційно невеликого числа T, «непідтверджених» блоків в кінці ланцюжка.

Так як в системі Blockchain можуть знаходитися, як добропорядні, так і зловмисні учасники, відповідно розповсюджуються справжні і підроблені дані.

Але, так як кожен учасник перевіряє коректність даних, що передаються і тому підроблена інформація блукає лише серед зловмисників (Рис. 2).

Накамото розробив початковий аналіз розподіленості, припускаючи, що зловмисник тільки розробляю конкретну стратегію атаки, а саме, намагається створити ланцюжок швидше, ніж чесні учасники.

Але його аналіз не розглядає більш складні стратегії атаки, адже зловмисний учасник може спробувати «розділити гравців» і змусити їх працювати в різних ланцюгах.

Прекрасна недавня робота Гарая, Кіаяса і Леонардоса забезпечує більш формальну модель для вивчення блокчейна Накамото [8]. Однак, їх аналіз розглядає тільки синхронну мережу з

поспішним зловмисником, тобто дані, відправлені ним, прибувають без будь-яких затримок.

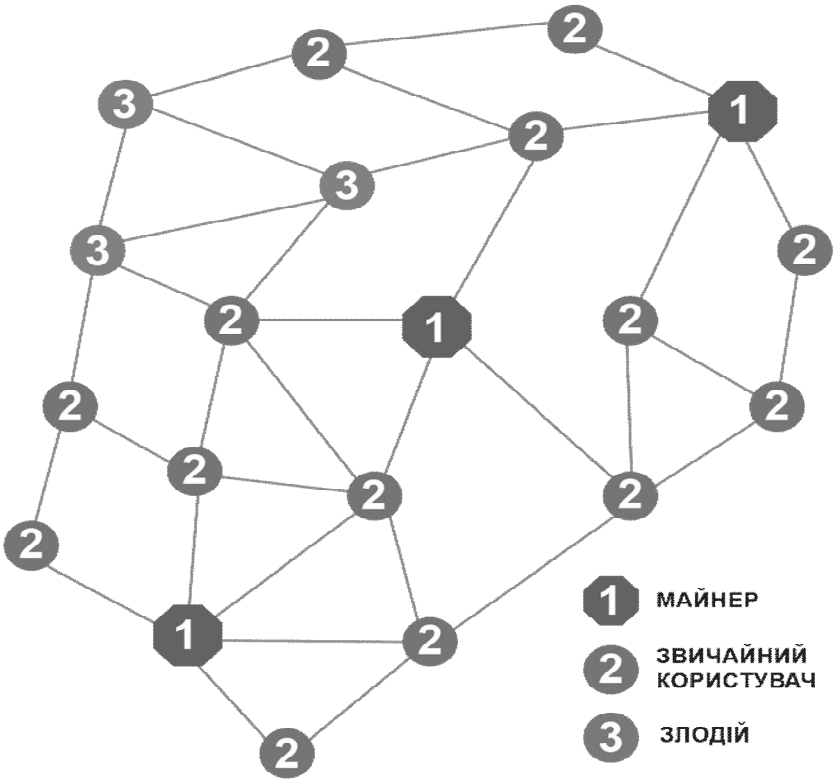

Рис.2 Структура мережі Blockchain

Але зловмисник отримує всі дані, відправлені чесними учасниками, щоб змінити або видалити їх.

У цій моделі вони демонструють, що технологія blockchain задовольняє принцип розподіленості і захищеності в налаштуванні з фіксованою кількістю гравців. Але, слід відзначити, технологія не має точної кількості учасників.

Однак припущення про розподіленість технології дуже вагоме. Дійсно, технологія Накамото розроблена для роботи в мережі з затримками передачі даних і функціонує в такій мережі (тобто в Інтернеті).

Пропоную детальний аналіз принципу розподіленості та безпечності технології Blockchain, беручи до уваги певні затримки мережі.

Розглянемо систему Накамото зі стійкістю до майнінг-«складності» *p* (тобто один випадковий ключ є успішним в процесі майнінгу з ймовірністю *p*) з n-кількістю учасників, кожен з яких має ідентичну обчислювальну потужність. Припустимо, процес видобутку блоків проходить в кілька етапів і в кожному з них добросовісні учасники отримують один випадковий ключ, а кожен зловмисник *p*-

фракції отримує ρn випадкових ключів. Чесні учасники повинні робити свої запити паралельно, але я в своєму аналізі припускаю, що зловмисник робить запити послідовно.

Нехай $\alpha = 1 - (1-p)^{(1-\rho)n}$ - ймовірність того, що якийсь чесний учасник досягне успіху у видобутку ключа на першому етапі (тобто з першого разу), і нехай β = ρnp - очікувана кількість блоків, які може створити зловмисник на першому етапі.

Коли *p ≤ 1/n* (що розглядається на практиці), ми отримуємо, що *α ≈ p (1 - ρ) n* і, отже, $\frac{\alpha}{\beta} \approx \frac{1-p}{p}$.

Припустимо, що існує таке δ > 0, що α (1 - (2Δ + 2) α) ≥ (1 + δ) β.

Тоді, за винятком показово маленької вірогідності (в T), технологія Накамото задовольняє T-консистенції у випадковій моделі видобутку ключів, припускаючи, що затримка мережі обмежена Δ.

Як наслідок, ми маємо, що до тих пір, поки ρ <12 (тобто, зловмисник контролює менше половини обчислювальної потужності), для кожного Δ існує деякий (досить малий) p такий, що технологія Blockchain задовольняє принцип розподіленості.

Нехай $\gamma = \frac{\alpha}{1 + \Delta\alpha}$ «дисконтована» версія α через затримки в мережі. Інтуїтивно, затримуючи повідомлення, зловмисник отримує додатковий час для обчислень.

Припустимо, що існує таке δ> 0, що α (1 - 2 (Δ + 1) α) ≥ (1 + δ) β.

Нехай g = $\frac{\gamma}{1 + \delta i}$ і μ = 1 - (1 + δ)$\frac{\beta}{\gamma}$, тоді технологія блокчейн задовольняє послідовності, майбутню однорідність, якість μ-ланцюга і зростання g-ланцюга.

Слід зауважити, що коли p ≪ 1/*n*Δ (що розглядається на практиці), ми маємо, що γ ≈ α ≈ (1 - ρ) np і, отже, $\frac{\gamma}{\beta} \approx \frac{1-\rho}{\rho}$.

Як наслідок, маємо наступне:

Припустимо, що ρ < $\frac{1}{2}$. Тоді для кожного n, Δ, існує деякий досить малий $\rho_0 = (\frac{1}{\Delta n})$, так, що технологія Blockchain з параметром min p ≤ p0 задовольняє узгодженість 1 - $\frac{\rho}{1-\rho}$ – якість ланцюга і $\frac{\rho n}{2}$ - ріст.

Таким чином, до тих пір, поки ρ <12, система гарантує, що нові дані потрапляють в кінець ланцюга блоків, і до тих пір, поки ρ <13, половина цих даних будуть вноситися чесними учасниками.

Відзначимо, що якість ланцюжка блоків, встановлена Гараєм не допускає затримок (тобто Δ = 1) при майнінг-атаках.

Але залишається відкритим питання чи існують технології, що задовольняють наше абстрактне поняття блочного ланцюга, які покращують параметри, досягнуті технологією блокчейн, тобто чи дійсно система Blockchain Накамото є отпимальною?

Я хочу навести експериментальну інтерпретацію принципу безпечності та розподіленості, використовуючи оцінки параметрів в реальному світі. На початку 2017 року мережа Bitcoin колективно виконувала 1018 операцій хешування в секунду.

Сьогодні компанії продають обладнання для майнінгу, яке працює при 1012 хеш-операціях в секунду. Щоб відповідати цим значенням, розглянемо n = 105 учасників і Δ = 1013, що відповідає приблизно 10-секундної затримки для мережі при заданому хешуванні. Оцінка 10с заснована на припущенні, що велика частина обчислювальної потужності, внесеної в мережу Bitcoin, працює зі з'єднанням, яке перевищує 1 мб / с, таким чином, кожен блок займає приблизно 1 с для передачі, а діаметр мережі менше 10 переходів.

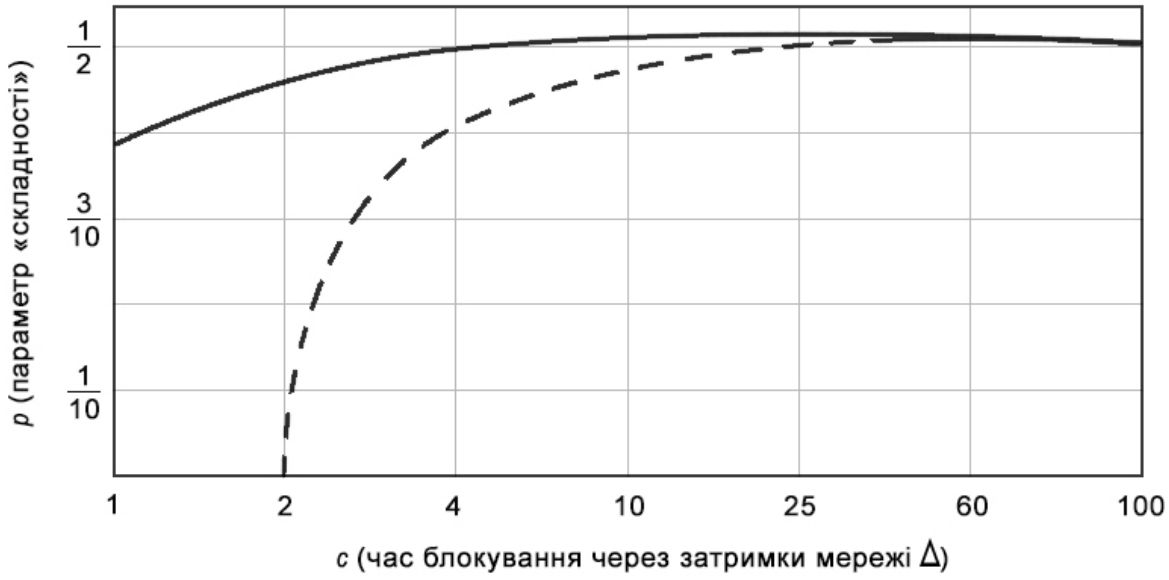

Рис.3

Відповідно до графіку (рис.3), для n = 10^5 і Δ =10^{13} (тобто 10с затримки на 1TH /с для комерційно доступної майнінг-техніки - ці параметри приблизно збігаються з оцінками хештрату станом на лютий 2017 року), встановлюю параметр «складності»$\rho = \frac{1}{c\text{-}n\Delta}$, де *c* змінюється уздовж осі *x*.

Можна інтерпретувати *c* як очікуваний час блокування через затримки мережі Δ.

Пунктирна лінія графіку показує значення ρ, для якого α (1 - (2Δ + 2) α)> β, тобто параметри, при яких показується розподіленість технології блокчейн.

Суцільна лінія графіку показує, коли атаці вдалося порушити розподіленість. При c = 60 «складність» приблизно відповідає очікуваної 10-хвилинній зупинці, що вказує на те, що Blockchain

витримує атаку p <49,57%, і найсильніша атака досягає успіху при ρ> 49,79%.

Дані припущення збігаються з емпіричними вимірами, зробленими Кристианом Декером і Роджером Ваттенхофером [6]. Протягом літа 2012 року, вони вирахували середній час затримки приблизно 10,55 м і «середньозважену» Δ ~ 11,37 с.

Їх вимірювання підтримуються сайтом bitcoinstats.com за 2016 рік [9]. Однак, в обох випадках вони вимірюють з'єднання за кількістю вузлів, а не відповідно до обчислювальних ресурсів; таким чином, їх оцінки більш упереджені, оскільки включають в себе безліч вузлів, які пов'язані повільними мережевими з'єднаннями і не вносять ніякого помітного обчислення до мережі.

Слід відзначити, що даний аналіз розглядає максимально неблагополучні умови. Адже в ньому припускається, що зловмисний учасник зможе повністю контролювати ланцюг.

Висновок

Blockchain – це спосіб зберігання даних, який полегшить життя суспільства і позбавить від багатьох проблем.

Тенологія блокчейн - це крок в надійне життя.

В данній статті Ви ознайомились с механізмом роботи Blockchain, що заснований на принципах відкритості, безпечності і розподіленості.

Було вивчено структуру системи блокчейн та розглянуто аналіз максимально сильної атаки з боку зловмисних учасників. На прикладі графіку видно, що Blockchain витримує атаку p <49,57%, і найсильніша атака досягає успіху при ρ> 49,79%.

Ці вимірювання збігаються з емпіричними вимірами, зробленими Кристианом Декером і Роджером Ваттенхофером.

Масштаби технології дуже великі, тому багато аспектів ще досі не було проаналізовано. Інтерес до геніальної системи не вщухає, що говорить про велику ймовірність появи нових досліджень.

Отже, Blockchain — це ланцюжок із блоків даних, що зберігаються на серверах комп'ютерів учасників. Доступ до цих блоків відкритий для кожного. Але ніхто не може змінити записи в них, так як система одразу покаже невідповідність. Це і є основою надійності.

На сьогодняшній день, вже багато країн оцінили широкі можливості цієї технології. Її масштаби доволі швидко зростають і все більше країн, в тому числі Україна, запроваджують блокчейн.

Література:

1. Цифровое Золото. Невероятная история биткойна или о том, как идеалисты и бизнесмены изобретают деньги заново / Натаниэль Поппер — 2016. - 350 с.

2. Bitcoin. Больше чем деньги / Алекс Форк — 2014. — 280 с.

3. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott //Alex Tapscott — 2016. — 324 с.
4. Blockchain: Blueprint for a New Economy / Melanie Swan - 2015.— 152 с.
5. «Bitcoin in Brief» / Ben Isgur — 2014. - 23 с.
6. Bitcoin Transaction Malleability and MtGox / Christian Decker// Roger Wattenhofer – 2016. – 14 с
7. The Bitcoin Backbone Protocol: Analysis and Applications /Juan A. Garay – 2017. – 44 с.
8. The bitcoin backbone protocol: Analysis and applications / Juan Garay//Aggelos Kiayias // Nikos Leonardos – 2015. – 310
9. Інтернет-ресурс http://bitcoinstats.com.
10. Інтернет-ресурс https://dsec.ru/security-analysis/the-security-analysis-of-the-blockchain-projects/
11. Інтернет-ресурс https://bitnovosti.com/2017/03/02/chto-takoe-tehnologija-blokchein-posagovoe-rukovodstvo-dlja-novichkov-1/
12. Блокчейн. Схема новой экономики / Мелани Свон - 2017. – 240
13. Сторінка в Wikipedia: https://ru.wikipedia.org/wiki/Биткойн
14. Криптовалютний інформаційний портал: http://bits.media/
15. Документальний фільм «Криптовалюты»: https://www.youtube.com/watch?v=Aybt-UZb4kk
16. Інтернет-ресурс https://forklog.com/big-data-i-blokchejn-proryv-v-oblasti-analiza-dannyh/
17. Биткойн-комьюнити в Facebook: https://www.facebook.com/bitcoinru/

References:

1.«Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money»/Nathaniel Popper - 2016. - 350 p.
2.Bitcoin. more than money/ Alex Fork – 2014. – 280 p.
3. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott //Alex Tapscott — 2016. — 324 с.
4. Blockchain: Blueprint for a New Economy / Melanie Swan - 2015. — 152 с.
5. «Bitcoin in Brief» / Ben Isgur — 2014. - 23 с.
6. Bitcoin Transaction Malleability and MtGox / Christian Decker// Roger Wattenhofer – 2016. – 14 с
7. The Bitcoin Backbone Protocol: Analysis and Applications /Juan A. Garay – 2017. – 44 с.
8. The bitcoin backbone protocol: Analysis and applications / Juan Garay//Aggelos Kiayias // Nikos Leonardos – 2015. – 310
9. Internet resource http://bitcoinstats.com.

10. Internet resource https://dsec.ru/security-analysis/the-security-analysis-of-the-blockchain-projects/
11. Internet resource https://bitnovosti.com/2017/03/02/chto-takoe-tehnologija-blokchein-posagovoe-rukovodstvo-dlja-novichkov-1/
12. "Blockchain: Blueprint for a New Economy" / Melanie Swan - 2017. – 240
13. Page in Wikipedia: https://ru.wikipedia.org/wiki/Биткойн
14. Crypto-currency information portal: http://bits.media/
15. Documentary film "Cryptocurrency":https://www.youtube.com/watch?v=Aybt-UZb4kk
16. Internet resource https://forklog.com/big-data-i-blokchejn-proryv-v-oblasti-analiza-dannyh/
17. Bitcoin Community on Facebook: https://www.facebook.com/bitcoinru/