УДК 004.056.55 DOI: 10.31673/2518-7678.2020.014045

Гулін В.О.

УДОСКОНАЛЕННЯ СУЧАСНИХ СИСТЕМ ДОКУМЕНТООБІГУ ТА ДОКУМЕНТООБМІНУ НА ПРИВАТНИХ ПІДПРИЄМСТВАХ ЗА ДОПОМОГОЮ КРИПТОГРАФІЇ

Hulin V.O. Improvement of modern systems of workflow and document exchange in private enterprises with the help of cryptography and blockchain technology. This article addresses the use of advanced encryption technologies in software development such as EDS, Mobile ID, and the use of blockchain technology for document sharing. It has been concluded that blockchain technology is a versatile way of storing and processing information in almost every field of activity, contributing to the formation of new crypto-institutions and crypto-industries. It is already clear that this technology and the changes it brings about are revolutionary and will lead to global change. This technology can give government agencies new tools to reduce fraud, reduce errors and reduce paperwork costs; great potential for creating new ways to secure property rights and to confirm the origin of goods and intellectual property.

Technology influences the development and creation of services for the sale of certain services, creates specialized blockchain consortia that help in the study of technology and its introduction in the crypto industry.

Keywords: digital signature, electronic signature, private key, electronic document, public key, electronic digital signature, document, signature, secret key, symmetric scheme, use of hash functions, signature verification, encryption, Mobile ID, Ukraine, blockchain, message digest

Гулін В.О. Удосконалення сучасних систем документообігу та документообміну на приватних підприємствах за допомогою криптографії. У цій статті мова йде про застосування сучасних технологій шифрування при розробці програмного забезпечення на прикладі ЕЦП, Mobile ID та використання технології blockchain для обміну документами. Зроблено висновок, що Технологія blockchain є універсальним способом зберігання і обробки інформації майже в будь-якій сфері діяльності, що сприяє формуванню нових крипто-інститутів і крипто-індустрій. Вже очевидно, що ця технологія і ті зміни, які вона в собі несе, революційна і призведе до глобальних світових змін. Ця технологія може дати державним органам нові інструменти, які дозволять скоротити обсяги шахрайства, число помилок і зменшити витрати на паперовий документообіг; великий потенціал для створення нових способів забезпечення прав власності і підтвердження походження товарів та інтелектуальної власності.

Технологія впливає на розробку і створення сервісів для продажу певних послуг, створюються спеціалізовані блокчеїн-консорціуми, які допомагають у вивченні технології та впровадженні її в крипто-індустрію.

Ключові слова: цифровий підпис, електронний підпис, закритий ключ, електронний документ, відкритий ключ, електронний цифровий підпис, документ, підпис, секретний ключ, симетрична схема, використання хеш-функцій, перевірка підпису, шифрування, Mobile ID, Україна, blockchain, хеш-сума

Гулин В.О. Совершенствование современных систем документооборота и документообмена на частных предприятиях с помощью криптографии. В этой статье речь идет о применении современных технологий шифрования при разработке программного обеспечения на примере ЭЦП, Mobile ID и использование технологии blockchain для обмена документами. Сделан вывод, что технология blockchain является универсальным способом хранения и обработки информации почти в любой сфере деятельности, способствует формированию новых крипто-институтов и крипто-индустрий. Уже очевидно, что эта технология и те изменения, которые она в себе несет, революционная и приведет к глобальным мировых изменений. Эта технология может дать государственным органам новые инструменты, которые позволят сократить объемы мошенничества, число ошибок и уменьшить расходы на бумажный документооборот; большой потенциал для создания новых способов обеспечения прав собственности и подтверждения происхождения товаров и интеллектуальной собственности.

Технология влияет на разработку и создание сервисов для продажи определенных услуг, создаются специализированные блокчеин-консорциумы, которые помогают в изучении технологии и внедрении ее в крипто-индустрию.

Ключевые слова: цифровая подпись, электронная подпись, закрытый ключ, электронный документ, открытый ключ, электронная цифровая подпись, документ, подпись, секретный ключ, симметричная схема, использование хеш-функций, проверка подписи, шифрование, Mobile ID, Украина, blockchain, хеш-сумма

Вступ

У сучасному світі люди цінують час, легкість використання чого-небудь, зручність взаємодії з різним технологіями і побутовими речами. Так робота з документацією займає багато часу, є дуже важливою і вимагає величезної захищеності. Будь-який витік інформації веде за собою великі проблеми. І якщо раніше криптографія і шифрування здавалося долею виключно спеціальних служб, то зараз їх необхідно застосовувати в бізнесі.

Що ж таке шифрування? Це перетворення інформації, що робить її нечитаною для сторонніх. При цьому довірені особи можуть провести дешифрування і прочитати вихідну інформацію. Існує безліч способів шифрування / дешифрування, але секретність даних заснована не на таємному алгоритмі, а на тому, що ключ шифрування (пароль) відомий тільки довіреним особам.

На допомогу при роботі з документацією приходить електронний цифровий підпис. Електронні підписи полегшують життя керівникам, співробітникам відділу кадрів і менеджерам в різних галузях.

Технологія дозволяє цим працівникам збирати підписи від клієнтів і співробітників і управляти ключовими документами і записами з мінімальними зусиллями. Більше немає необхідності друкувати, надсилати поштою або сканувати фізичні копії документів. Проте, рішення для електронного підпису не отримали широкого розповсюдження, але основна технологія використовується для стимулювання інновацій навіть в деяких з найжорстокіших секторів бізнесу.

Підвидом електронних підписів є цифровий підпис. Цифрові підписи є одними з найбільш важливих компонентів програми електронного підпису, і вони можуть забезпечити безпеку, юридичну силу і ефективність управління записами при використанні методу електронного підпису. Таким чином, створення електронного підпису не повинно відбуватися без підтримки цифрового підпису.

Цифровий підпис — це конкретна технічна реалізація електронного підпису, що включає криптографічні методи з використанням ключів підпису, пов'язаних з підписала стороною. Цифровий підпис посилається на підписаний документ або транзакцію, так що будь — яка наступна модифікація може бути виявлена.

Цифровий підпис це дуже добре, але якщо ми хочемо забезпечити приватність та захист своїх документів на більшому рівні ніж підпис, захистити усю систему? На допомогу прийде технологія blockchain.

Існує два визначення терміна Блокчейн (Blockchain): розподілена база даних та безперервний послідовний ланцюжок блоків, що містять інформацію.

Організація мережі першим способом має на увазі централізований контроль за всім: додатки, дані, доступ. Вся системна логіка і інформація приховані всередині сервера, що дозволяє знизити вимоги до продуктивності клієнтських пристроїв і забезпечити високу швидкість обробки даних. Саме цей метод набув найбільшого поширення в наші дні.

З юридичної точки зору ця технологія може повноцінно використовуватися в бізнес-процесах та досягти максимально можливого рівня захисту. Технології blockchain дозволять оптимізувати витрати корпоративного і державного управління обміном інформації.

Виклад основного матеріалу дослідження

При розмові про документації, почнемо з опису. Електронний документ це:

• документ, зафіксований на електронному носії (у вигляді набору символів, звукозапису або зображення) і призначений для передачі в часі і просторі з використанням засобів обчислювальної техніки та електрозв'язку з метою зберігання та громадського використання;

• форма подання інформації з метою її підготовки, відправлення, отримання або зберігання з допомогою електронних технічних засобів, зафіксована на магнітному диску, магнітній стрічці, лазерному диску і іншому електронному матеріальному носії;

• документована інформація, представлена в електронній формі, тобто у вигляді, придатному для сприйняття людиною з використанням електронних обчислювальних машин, а також для передачі по інформаційно — телекомунікаційних мереж та обробки в інформаційних системах;

Юридичну значимість електронного документа надає електронний підпис, який на території України рівнозначна власноручного підпису в документі на паперовому носії при одночасному дотриманні наступних умов:

• сертифікат ключа підпису, що відноситься до цієї електронного цифрового підпису, не втратив силу (діє) на момент перевірки або на момент підписання електронного документа;

• при наявності доказів, що визначають момент підписання;

• підтверджена справжність електронного цифрового підпису в електронному документі;

• електронний цифровий підпис використовується відповідно до відомостей, зазначених у сертифікаті ключа підпису;

Для забезпечення конфіденційності (секретності) сполучення електронного документу застосовується шифрування. Для шифрування і дешифрування повідомлення використовується пара ключів — Відкритий і закритий ключі. Вони використовуються і для формування електронного підпису (ЕЦП) [7].

Для шифрування повідомлення використовується Відкритий ключ одержувача і Закритий ключ відправника. Отримане зашифроване повідомлення розшифровується одержувачем з використанням свого Закритого ключа і Відкритого ключа відправника. Навіть відправник, тільки що зашифрував повідомлення, не може його розшифрувати[6].

ЕЦП і шифрування повідомлень за бажанням користувача можуть використовуватися як спільно, так і окремо. Наприклад, Наказ директора повинен бути підписаний ЕЦП для підтвердження його достовірності, але не повинен бути зашифрований.

Сертифікат ключа підпису (СКП) служить для підтвердження належності Відкритого ключа конкретному користувачеві. У разі компрометації Закритого ключа Сертифікат відгукується і автоматично потрапляє в розряд недійсних. У такому випадку користувачеві необхідно буде отримувати новий Сертифікат. Для підтвердження достовірності інформації, що міститься в Сертифікаті, використовується електронний підпис засвідчується центру (УЦ).

Існує кілька схем побудови цифрового підпису:

• на основі алгоритмів симетричного шифрування;

• на основі алгоритмів асиметричного шифрування;

Оскільки документи, які підписували — змінного обсягу, в схемах ЕП часто підпис ставиться не на сам документ, а на його хеш. Для обчислення хешу використовуються криптографічні хеш — функції, що гарантує виявлення змін документа при перевірці підпису [6].

Використання хеш-функцій дає наступні переваги:

• обчислювальна складність. Зазвичай хеш цифрового документа робиться у багато разів меншого обсягу, ніж обсяг вихідного документа, і алгоритми обчислення хешу є більш

швидкими, ніж алгоритми ЕП. Тому формувати хеш документа і підписувати його виходить набагато швидше, ніж підписувати сам документ;

• сумісність. Більшість алгоритмів оперує з рядками біт даних, але деякі використовують інші уявлення. Хеш- функцію можна використовувати для перетворення довільного вхідного тексту в потрібний формат;

• цілісність. Без використання хеш-функції великий електронний документ в деяких схемах потрібно розділяти на досить малі блоки для застосування ЕП. При верифікації неможливо визначити, чи всі блоки отримані і в правильному вони порядку;

Отримати ЕЦП можливо в АЦСК – акредитовані центри сертифікації ключів. Перелік акредитованих центрів сертифікації ключів (далі — АЦСК), які видають ЕЦП в Україні, ведеться Центральним засвідчувальним органом Мін'юсту.

При цьому, замовнику необхідно з'ясувати в службі підтримки електронного майданчика, через який замовник планує здійснювати електронні закупівлі, які саме АЦСК підтримує цю площадку.

Зокрема, всі майданчики підтримують АЦСК Державної фіскальної служби (далі — ДФС) і АЦСК органів юстиції України.

Що стосується процедури отримання ЕЦП, то це замовник може з'ясувати безпосередньо в АЦСК, зокрема на його веб-сайті.

Крім простого ЕЦП використовують нову технологію Mobile ID. Mobile ID — послуга Електронної ідентифікації та кваліфікованого електронного підпису, за допомогою якої можна авторизуватися на Електронний ресурс і створювати електронні документи. При цьому електронний підпис записується безпосередньо SIM-карту. Mobile ID можна використовувати у корпоративних ринках, державних установах, електронній комерції, охороні здоров'я, фінансових установах.

Завдяки Mobile ID, ЕЦП можна використовувати де завгодно: на телефоні, планшеті, смартфоні.

Не потрібно відвідувати установи, що б скористатися послугами цифрового підпису. Для використання підпису не потрібно мати спеціальне обладнання, тільки симкарту з mobile ID. Видається Унікальний ПІН-код для авторизації та підпису.

SIM-карта, яку ви використовуєте для дзвінків, не підтримує послугу Mobile ID. Лише спеціальна SIM-карта здійснює криптографічні алгоритми генерації пар ключів для створення кваліфікованого електронного підпису та для зберігання персонального ключа.

Для розуміння роботи Mobile ID, наведемо приклад, щоб авторизуватись на сайті:

1. Зайдіть на потрібний сайт
2. Оберіть варіант ідентифікації Mobile ID
3. Введіть свій номер телефону. Після цього вам надійде повідомлення-підтвердження автентифікації.

Щоб підписати документ:

4. Зайдіть на ресурс, де вам потрібно підписати документ
5. Клікніть на кнопку «Підписати» біля потрібного файлу
6. Оберіть Mobile ID із запропонованого переліку способів підписання
7. Введіть ваш PIN — код, щоб підписати документ

Від початку 2019 року всі електронні адміністративні послуги та сервіси створюють із можливістю електронної ідентифікації за допомогою технології MobileID. Окрім того, згодом до всіх уже наявних е-послуг теж буде додана така опція.

Mobile ID найкращий метод підписи для забезпечення цілісності та походження електронного документа на даний час, але є ще один спосіб — технологія blockchain.

Технологією blockchain називають послідовний ланцюжок блоків. У кожному міститься інформація, яка зберігається не на центральному сервері, а у всіх учасників мережі. Децентралізація допомагає учасникам зберігати актуальну інформацію, а спеціальні механізми перевіряють та не дають записам в блоках суперечити один одному[2].

Blockchain вміє зберігати хеш-суми (набор символів, який отримується шляхом шифрування початкового документу). Один документ завжди має туж саму хеш-суму. Якщо в початковому документі зміниться хоча б один символ – хеш зміниться. Хеш може додаватися учасниками в блоки, після чого він остається там назавжди.

Існує два визначення терміна Блокчейн (Blockchain): розподілена база даних та безперервний послідовний ланцюжок блоків, що містять інформацію.

Всього існує два типи архітектур: клієнт-серверна мережа та тимчасова (пірінгова) мережа [3].

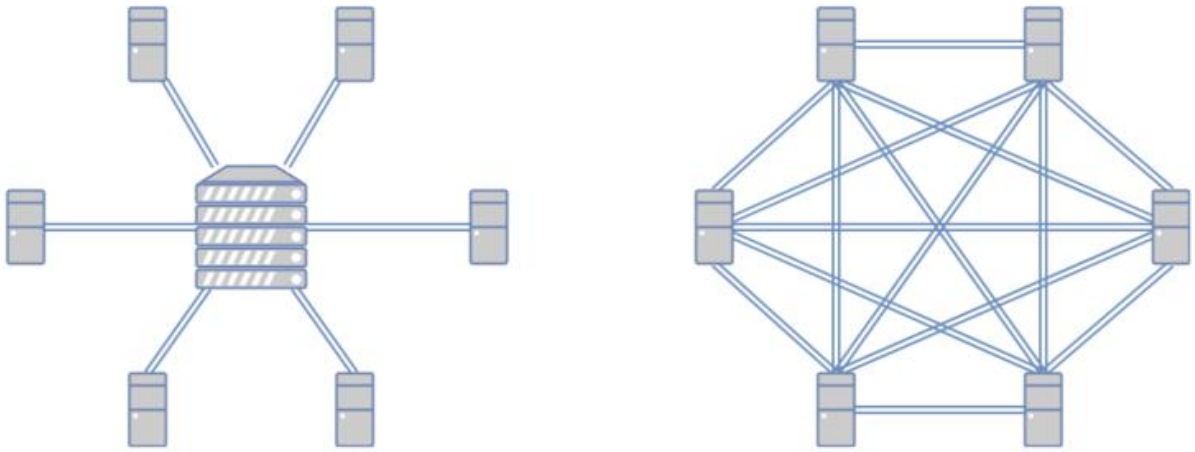

Рис. 1. Типи архітектур мережі

Організація мережі першим способом має на увазі централізований контроль за всім: додатки, дані, доступ. Вся системна логіка і інформація приховані всередині сервера, що дозволяє знизити вимоги до продуктивності клієнтських пристроїв і забезпечити високу швидкість обробки даних. Саме цей метод набув найбільшого поширення в наші дні[1].

З юридичної точки зору ця технологія може повноцінно використовуватися в бізнес-процесах та досягти максимально можливого рівня захисту. Технології blockchain дозволять оптимізувати витрати корпоративного і державного управління обміном інформації.

Прикладом вирішення проблеми нотаріальних затверджень підпису: не потрібно мати підтвердження справжності документа особи-посередника, тому що blockchain гарантує точність інформації.

Але у цієї технології є свої недоліки, такі як: повільна швидкість, технологічні обмеження та важкість впровадження і масштабування.

Головна особливість блокчейн – децентралізація[4]. Немає ніякого основного сервера, на якому тримається вся інформація. Даними володіють одночасно всі учасники блокчейн-мережі. Тобто абсолютно в усіх учасників рівні права, тому здійснення операцій проводиться між ними безпосередньо.

Висновки

З огляду на сучасний стан інформаційних технологій, це найкращий метод підписи для забезпечення цілісності та походження електронного документа.

У разі успішної реалізації Mobile ID, держава зможе використовувати його в якості основи для надання різних адміністративних послуг. У перспективі, через Mobile ID можна буде отримати всі послуги, доступні також і через цифровий електронний паспорт, через систему авторизації bank ID, захищену електронно-цифровий підпис.

У перспективі приватні підприємства зможуть використовувати технологію blockchain як більш надійне та захищене середовище документообігу та документообміну. Але на зараз ця технологія ще не доскональна та має свої недоліки які потрібно вирішити.

Технологія blockchain є універсальним способом зберігання і обробки інформації майже в будь-якій сфері діяльності, що сприяє формуванню нових крипто-інститутів і крипто-індустрій. Вже очевидно, що ця технологія і ті зміни, які вона в собі несе, революційна і призведе до глобальних світових змін.

Застосування blockchain знизить витрати компанії на підготовку звітності, підвищивши її прозорість. Багато галузей вже мають пілотні проекти, які здатні скоротити витрати бізнес-процесів і підвищити ефективність транзакцій. Blockchain технологія генерує абсолютно нові бізнес-сценарії, які в майбутньому не тільки повністю перетворять цілі галузі, а й призведуть до зникнення деяких, наприклад, таких як посередництво. Радикальні зміни охоплять бізнес-моделі і процеси, ланцюжки поставок і відносини компаній з клієнтами у всіх секторах економіки.

Список використаної літератури

1. Distributed Ledger technology: beyond block chain. A report by the UK Government Chief Scientific Advicer // Government Office for Science, London 2016. - [Електронний ресурс]. - Режим доступу - https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain (Дата звернення - 24.11.2019).

2. Yaga D., Mell P., Roby N. Blockchain Technology Overview. – [Електронний ресурс]. - Режим доступу – https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf (Дата обращения – 24.11.2019).

3. Buterin V. «An Introduction to Futarchy [as Applied with Block-chain Technology]». – [Електронний ресурс]. - Режим доступа – https://blog.ethereum.org/2014/08/21/introductionfutarchy/ (Дата звернення: 14.11.2019).

4. Hanson R. «Futarchy: Vote Values, but Bet Beliefs». – [Електронний ресурс]. - Режим доступу - http:// hanson.gmu.edu/futarchy2013.pdf (Дата звернення 14.11.2019).

5. Дуброва Ярослава, Застосування електронного цифрового підпису в публічних закупівлях — [Електронний ресурс]. — Режим доступу до ресурсу: https://i.factor.ua/ukr/journals/bb/2016/june/issue — 24/article — 19093.html (Дата звернення 14.11.2019).

6. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие / 2 — е изд., испр. и доп. – М.: Гелиос АРВ, 2002. — 480 с. ил.

7. Margaret Rouse, Digital signature — [Електронний ресурс]. — Режим доступу до ресурсу: https://searchsecurity.techtarget.com/definition/digital-signature (Дата звернення 14.11.2019).

Автори статті

Гулін Владислав Олегович – студент Державного університету телекомунікацій, Київ, Україна.

Authors of the article

Hulin Vladyslav Olehovich – student at the State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 31.01.2020 р. Рецензент: д.т.н., доц. А.О. Макаренко