CRDFGLOBAL
INSPIRED BY PEOPLE | DRIVEN BY SCIENCE

Erasmus+

USAID
FROM THE AMERICAN PEOPLE

INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY

MATERIALS

of IXth International Scientific and Technical Conference

May 25–26, 2023

ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY

Ministry of Education and Science of Ukraine

National Academy of Sciences of Ukraine

Ministry of Science and Higher Education of the Republic of Poland

Lviv Polytechnic National University

Pidstryhach Institute for Applied Problems of Mechanics and Mathematics National Academy of Sciences of Ukraine

Odessa National Polytechnic University

University of Bielsko-Biała (Poland)

INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY

MATERIALS

of IXth International Scientific and Technical Conference

May 25–26, 2023

Lviv
Lviv Polytechnic Publishing House
2023

Міністерство освіти і науки України
Національна Академія наук України
Міністерство науки та вищої освіти Республіки Польща
Національний університет "Львівська політехніка"
Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України
Одеський національний політехнічний університет
Університет Бєльсько-Бяла (Польща)

ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

МАТЕРІАЛИ

IX Міжнародної
науково-технічної конференції

25–26 травня, 2023

Львів
Видавництво Львівської політехніки
2023

УДК 004.056.5
З 38

Conference organizers:

LVIV POLYTECHNIC NATIONAL UNIVERSITY

PIDSTRYHACH INSTITUTE FOR APPLIED PROBLEMS OF MECHANICS AND MATHEMATICS

ODESSA NATIONAL POLYTECHNIC UNIVERSITY

AKADEMIA TECHNICZNO-HUMANISTYCZNA, BIELSKO-BIAŁA (POLSKA)

З-38 **Захист** інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф. – Львів : Видавництво Львівської політехніки, 2023. – Режим доступу: https://drive.google.com/drive/folders/1z5BLogqaxwh4xgGk2eMLI8WcVNOXCFX6, вільний –Заголовок з екрана. – Мова укр. і англ.

ISBN 978-966-941-829-6

У збірнику опубліковано матеріали конференції, присвяченої проблемам у галузі захисту інформації і безпеки інформаційних систем. Видання призначено для науковців, аспірантів, студентів.

УДК 004.056.5

The collection includes texts of reports and theses of speeches prepared for the IX International Scientific and Technical Conference “Information Security and Information Systems Security”. The publication is intended for scientists, postgraduates and students.

Postal address of the Organizing Committee:

79005, Lviv, 5, Kn. Romana Str., 1, Information Protection Department, room. No. 204.

Responsible for the issue – Professor Dudykevych V.B.

Computer layout and layout – Opirskyy I.R.

The materials are presented in the author's wording

ISBN 978-966-941-829-6

HONORARY CHAIRMEN

BOBALO Yu.Ya. – *Rector of Lviv Polytechnic National University, D.Sc., Professor*

KUSHNIR R.M. – *Director of the Pidstryhach Institute for Applied Problems of Mechanics and Mathematics of the National Academy of Sciences of Ukraine, Academician of National Academy of Sciences of Ukraine, D.Sc., Professor*

OBORSKYY H.O. – *Rector of Odessa National Polytechnic University, D.Sc., Professor*

CO-CHAIRMEN

DEMYDOV I.V. – *Vice-Rector for Research at Lviv Polytechnic National University, D.Sc., Associate Professor*

DUDYKEVYCH V.B. – *Head of the Information Protection Department, Lviv Polytechnic National University, D.Sc., Professor*

KARPIŃSKI M. – *Head of the Department of Computer Science and Automation, The University of Bielsko-Biala (Poland), D.Sc., Professor*

KOBOZYEVA A.A. –*.Head of the Department of Informatics and Information Systems Security Management, Odessa National Polytechnic University, D.Sc., Professor*

PROGRAM COMMITTEE

BLINTSOV V.S. – Vice-Rector for Scientific Work of National University of Shipbuilding, Academician of the Academy of Sciences of Shipbuilding of Ukraine, D.Sc., Professor

HORBENKO I.D. – Professor of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, D.Sc., Professor

DIVIZINYUK M.M. – Head of the Department of Civil Defense and Innovation of the Institute of Environmental Geochemistry of the National Academy of Sciences of Ukraine, D.Sc., Professor

YEVSEYEV S.P. – Head of the cyber security department of the National Technical University University "Kharkiv Polytechnic Institute", D.Sc., Professor

ZHURAVEL I.M. – Professor of the Department of Information Technology Security, Lviv Polytechnic National University, D.Sc., Professor

ZADIRAKA V.K. – Head of Department nr 140, V.M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Academician of the National Academy of Sciences of Ukraine, D.Sc., Professor

ZAGORODNA N.V. – Head of the Department of Cyber Security, Ternopil Ivan Puluj National Technical University, Ph.D., Associate Professor

KOVELA S. – MBA PGCE CITP Senior Lecturer Accounting, Finance and Informatics, Kingston University London, Ph.D. (United Kingdom)

CARLSSON A. – General Manager of ENGENSEC Tempus Project, lecturer at Blekinge Institute of Technology, Ph.D. (Karlskrona, Sweden)

JUSTICE C. – Clinical Associate Professor, CERIAS, Purdue University, CISSP, D.Sc. (USA)

KORCHENKO O.H. – Head of the Department of Information Technology Security, National Aviation University, D.Sc., Professor

ESIN V. I. – Professor of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, D.Sc., Professor

MARAKOVA-BEGOC I. – Research Fellow at Bretagne Telecom, Dc.S (France)

MATVIYKIV O.M. – First Vice-Rector of Lviv Polytechnic National University, D.Sc, Professor

MACHUSKYY Ye.A. – Head of the Department of Physical and Technical Means for Information Protection, National Technical University of Ukraine "Kyiv Polytechnic Institute", D.Sc., Professor

MELNYK A.O. – Head of the Department of Computer Engineering, Lviv Polytechnic National University, D.Sc., Professor

MELNYK V.A. – Professor of the Department of Information Technology Security, Lviv Polytechnic National University, D.Sc., Professor

MYKYYCHUK M.M. – Director of the Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, D.Sc., Professor

MYCHUDA L.Z. – Professor of Information Technology Security, Lviv Polytechnic National University, D.Sc., Associate Professor

MOROZ L.V. – Wydział Mechaniczny Technologiczny, Politechnika Warszawska (Polska), dr hab. inż., profesor uczelni

NYEMKOVA O.A. – Associate Professor of the Department of Information Technologies Security, Lviv Polytechnic National University, D.Sc., Professor

OSTAPOV S.E. – Head of the Department of Software Computer Systems, Chernivtsi National University, D.Sc., Professor

PARKHUTS L.T. – Professor of Information Protection Department, Lviv Polytechnic National University, D.Sc., Professor

PETROV O. – Professor AGH, Department of Applied Computer Science, AGH University of Science and Technology Stanisława Staszica, Kraków (Poland), D.Sc..

POTIY O.V. – Deputy Head of the State Service for Special Communications and Information Protection of Ukraine, D.Sc., Professor

RUZHENTSEV V.I. – Professor of the Department of Information Technology Security, Kharkiv National University of Radio Electronics, Doctor of Technical Sciences, Associate Professor

RUSYN B.P. – Head of the Department of Methods and Systems for Images Processing, Analysis and Identification, G.V. Karpenko Physico-Mechanical Institute of the National Academy of Sciences of Ukraine, D.Sc., Professor

SAMOTYY V.V. – Professor of the Department of computerized systems of Automation, Lviv Polytechnic University, D.Sc., Professor

SACHENKO A.O. – Head of the Department of Information and Computing Systems and Management, Western Ukrainian National University, D.Sc, Professor

FEDASYUK D.V. – Head of the Software Department of the Lviv Polytechnic National University, D.Sc., Professor

KHOMA V.V. – Professor of the Institute of Automation and Informatics, Opole University of Technology, (Poland), D.Sc., Professor

KHOROSHKO V.O. – Professor of the Department of Information Technologies Security, National Aviation University, D.Sc., Professor

CHAPLYHA V.M. – Professor of the Department of Automation and Computer-Integrated Technologies of Lviv National Agrarian University, D.Sc, Professor

CHEVARDIN V.E. –Head of the Department of Information Protection and Cyber Defense of the Military Institute of Telecommunications and Informatization. Heroes Krut, D.Sc., Senior Researcher

YAREMCHUK Yu.Ye. – Director of the Center for Information Technologies and Information Protection, Vinnytsia National Technical University, D.Sc., Professor

YATSKIV V.V. – Head of the Department of Cybersecurity, Western Ukrainian National University, D.Sc., Associate Professor

GUSTAVSSON R. – Professor at Blekinge Institute of Technology (Karlskrona, Sweden) and at KTH Royal Institute of Technology (Stockholm, Sweden)

RASMUS J. – Managing Director of SERIAS (Center of Education and Research in Information Assurance and Security), Purdue University (USA)

LUZHETSKY V.A. – Head of the Information Protection Department, Vinnytsia National Technical University, D.Sc., Professor

ORGANIZING COMMITTEE CO-CHAIRMEN

MAKSYMOVYCH V.M. – Head of the Department of Information Technology Security, Lviv Polytechnic National University, D.Sc., Professor

MARCHUK M.V. – Head of Department №15, Ya. S. Pidstryhach Institute of Applied Problems of Mechanics and Mathematics of the National Academy of Sciences of Ukraine, D.Sc., Professor

ORGANIZING COMMITTEE

BORTNIK L.L. – Senior lecturer of the Department of Information Protection of Lviv Polytechnic National University, Ph.D.

VOYTUSIK S.S. – Associate Professor of the Department of Information Technologies Security, Lviv Polytechnic National University, Ph.D.

HORPENYUK A.Ya. – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D., Associate Professor

ESINA M.V. – Professor of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, D.Sc., Professor.

KOROBEYNIKOVA T.I. – Associate Professor of the Department of Information Technology Security, Lviv Polytechnic National University, Ph.D., Associate Professor

KOSTIV Yu.M. – Associate Professor of the Department of Information Technology Security, Lviv Polytechnic National University, Ph.D., Associate Professor

KUTEN R.B. – Assistant of the Department of Information Protection, Lviv Polytechnic National University

CHUBYK R.V. – Associate Professor of Information Protection, Lviv Polytechnic National University, Ph.D., Associate Professor

LAH Yu.V. – Associate Professor of Information Protection, Lviv Polytechnic National University, Ph.D.

SHABATURA M.M. – Associate Professor of the Department of Information Technology Security, Lviv Polytechnic National University, Ph.D., Associate Professor

SOVYN Ya.R. – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D., Associate Professor

STAKHIV M.Yu. – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D.

TYSHYK I.Ya. – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D.

SECRETARY

OPIRSKYY I.R. – Professor of the Department of Information Protection, Lviv Polytechnic National University, D.Sc., Professor

МЕХАНІЗМИ ДОСЯГНЕННЯ НАДІЙНОСТІ В БЛОКЧЕЙНІ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Валерія БАЛАЦЬКА[a], Іван ОПІРСЬКИЙ[a]

[a] *Національний Університет "Львівська Політехніка", Львів, Україна*

Анотація. *Технологія блокчейну вдосконалюються швидкими темпами та створює можливості для обміну та об'єднання даних у спосіб, який раніше не передбачався. Водночас прогрес у цій технології відкриває нові можливості для етичного використання даних. Передача персональних даних створює головоломку для компаній і окремих осіб, що може принести цінні переваги, але також може створити великі ризики та витрати.*

Ключові слова. *Блокчейн, алгоритм консенсусу, персональні дані, конфіденційність.*

Вступ

Дані у блокчейні повинні бути цілісні та добре захищені від зловмисників. Алгоритми консенсусу якраз виконують такі функції, тому вони є чи не найважливішим елементом технології блокчейн. Оскільки дані у блокчейні розподілені і немає якогось одного серверу, розподілені учасники системи повинні якось узгоджувати валідацію транзакцій, що надходять до мережі [1]. Консенсус означає, що всі сторони погоджуються щодо конкретного рішення. Що стосується мережі блокчейн, члени мережі досягають консенсусу щодо вмісту блокчейну.

Блокчейн – це децентралізована система, що складається з різних суб'єктів, які діють в залежно від власних інтересів та наявної у них інформації. Всякий раз, коли нова транзакція транслюється по мережі, вузли можуть включити цю транзакцію в копію свого реєстру або проігнорувати її. Коли більшість учасників мережі приймають рішення про прийняття певного стану, досягається консенсус. Фундаментальною проблемою в розподілених обчисленнях і багатоагентних системах є досягнення загальної надійності системи при наявності ряду неробочих процесів. Найчастіше для цього потрібно, щоб процеси узгодили між собою деяке значення, яке знадобиться під час обчислення. Ці процеси писуються як консенсус. Щоб консенсусний протокол був безпечним, він повинен бути відмовостійким [2].

Алгоритми консенсусу

Наразі існує безліч алгоритмів консенсусу, що використовуються в різноманітних протоколах блочейнів, розглянемо декілька найпопулярніших з них.

Proof-of-Work (PoW) – один з найпопулярніших консенсусів, для того аби отримати доступ до загального ресурсу, користувач повинен обчислити достатньою складну, але обчислювальну задачу, аби запобігти зловживанням ресурсів [3]. Суть концепції така, що усім майнерам дається задача, яку вони повинні порахувати за певний проміжок часу. Задача – «Знайти таке значення x, щоб хеш SHA(x) містив N старших нульових біт».

Proof-of-Stake (PoS) – другий за популярністю алгоритм консенсусу. У цьому підході майнерам теж доводиться хешувати дані, але тут складність знову ж таки залежить від балансу. У порівнянні з Proof-of-Work, цей алгоритм не потребує великих енерговитрат. Також до переваг можна віднести те, що задля проведення атаки на таку мережу, зловмиснику необхідно отримати більше токенів і тоді йому стане просто невигідно знецінювати власний токен [4].

Delegated-Proof-of-Stake (DPoS) – ще одна альтернатива Proof-of-Work та разом з тим вдосконалення Proof-of-Stake. Суть алгоритму полягає у тому, що учасник може делегувати свій голос іншому учаснику мережі і той буде підтримувати роботу мережі від імені іншого. Оскільки це удосконалий PoS, то чим більше баланс токенів, тим більшу вагу має голос учасника.

Proof-of-Authority (PoA). Блоки записують перевірені валідатори, що завчасно обираються та по факту є модераторами системи [5]. Тут мають цінність не кількість токенів, а репутація. Таким чином блокчейн за певним алгоритмом обирає валідатора, який запише наступний блок.

Proof-of-Importance (PoI) – цей алгоритм надає перевагу користувачам, які отримали хорошу репутацію у мережі – «спочатку ви працюєте на репутацію, потім вона на вас». Репутація зростає з активним життям у екосистемі блокчейну та взаємодії з іншими учасниками. Чим краща репутація – тим більший шанс на створення наступного блоку.

Для порівняння наведених вище алгоритмів пропонується дивитись у таблицю 1.

Таблиця 1

Порівняльний аналіз різних алгоритмів знаходження консенсусу

Алгоритм	Ціль	Переваги	Недоліки
Proof of Work, PoW	Забезпечення складності у формі обчислювального завдання, щоб надатиможливість обміну даними між ненадійнимиучасниками.	Важко досягти відмови в обслуговування (атака DDoS неефективна). Відкритий для всіх, у кого є обладнання, щоб вирішити обчислювальне завдання.	Високе обчислювальне навантаження, високе енергоспоживання. Потенціал для 51% атаки, отримавши достатню обчислювальну потужність.
Proof of Stake, PoS	Забезпечення менш складної у обчислювальному плані перешкоди для додавання нових блоків, ніж у PoW, щоб надати можливість обміну даними між ненадійними учасниками.	Менш вимогливий у обчисленнях, ніж PoW. Відкритий для всіх.	Зацікавлені сторони контролюють систему. Існує можливість формуванню пулу зацікавлених сторін для створення централізованої влади. Потенціал для 51% атаки
Delegated PoS	Створення механізму консенсусу через «демократію», де учасники голосують (використовуючи криптографічно підписані повідомлення), щоб вибрати та відкликати права делегатів	Вибрані делегати економічно мотивовані залишатися чесними. Менш вимогливий у обчисленнях, ніж PoW	Менша різноманітність вузлів, ніж у PoW або в чистих реалізаціях PoS. Всі делегати «відомі», у виробників блоків може бути стимул змовлятися, ставлячи під загрозу безпеку
Proof of Authority/ Identity, PoA, PoI	Створити централізований процес погодження, щоб мінімізувати час створення блоків та швидкість підтвердження	Швидкий час підтвердження. Дозволяє збільшити темпи виробництва блоків. Може використовуватися в sidechain	Вважається, що валідуючий вузол не був скомпрометований Існує центральна точка відмови
Round- robin	Забезпечити систему для додавання блоків серед довірених вузлів	Низька обчислювальна потужність. Ідея проста в розумінні.	Вимагає великої довіри серед вузлів.

Будучи децентралізованою та розподіленою системою, блокчейн потребує певного механізму перевірки блоків, які мають бути доданим до існуючого блокчейну. Механізми досягнення консенсусу життєво важливі для функціонування розподілених систем. На сьогоднішній день найбільшим вдалим введення було використання Proof of Work, що дозволяє користувачам погоджуватися із загальним набором фактів.

Висновки

Алгоритми консенсусу сьогодні лежать в основі не лише систем цифрових грошей, а й блокчейнів, що дозволяють розробникам запускати код у розподіленій мережі, що у свою чергу дає можливість якісніше та надійніше захищати персональні дані користувачів. В даний час алгоритми є наріжним каменем блокчейн-технології та мають вирішальне значення для довгострокової життєздатності різних існуючих мереж.

Персональні дані і взагалі конфіденційні дані не повинні бути довірені стороннім особам, де вони будуть вразливі до атак і неправильного використання. Натомість користувачі повинні володіти і контролювати свої дані без шкоди для їх безпеки. Алгоритм консенсусу у свою чергу від користувачів не вимагає довіряти будь-яким третім сторонам та завжди користувачі можуть бути у курсі про дані, які збираються про них і як вони використовуються.

У додаток, блокчейн розпізнає користувачів як власників своїх персональних даних. З усіх алгоритмів консенсусу, Proof of Work залишається домінуючим. Більш надійної та безпечної альтернативи поки що не запропоновано. Тим не менш, існує величезна кількість досліджень і розробок в області заміни PoW у майбутньому.

Список літератури

[1] Camenisch, J., Dubovitskaya, M., Enderlein, R., Lehmann, A., Neven, G., Paquin, C., & Preiss, F. (2020) Concepts and languages for privacy-preserving attribute-based authentication. Working Conference on Policies and Research in Identity Management (IFIP). (Vol. 19, pp. 25-44).

[2] Bitcoin: A Peer-to-Peer Electronic Cash System, 2020 URL: https://bitcoin.org/bitcoin.pdf

[3] Camenisch, J., Kiayias, A., & Yung, M. (2019). On the Portability of Generalized Schnorr Proofs. EUROCRYPT 2019 (LNCS), (5479), 425-442.

[4] Coinmarketcap, 2023. URL: https://coinmarketcap.com/

[5] Creating a Trusted Experience with Blockchain, 2022. URL: https://blockchain.sonyged.com/