

## **ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВПРОВАДЖЕННЯ БЛОКЧЕЙН -ТЕХНОЛОГІЙ В ІНТЕРНЕТІ РЕЧЕЙ**

*Запорізька державна інженерна академія, кафедра ПЗАС*

Нещодавні прогнози по потенційному зростанню Інтернету Речей (IoT) говорять про те, що до 2020 року збільшиться кількість підключених до Інтернету пристроїв до 20,4 млрд. Деякі інші джерела навіть говорять, що це скромний прогноз. Незалежно від точної кількості пристроїв, у всіх нас буде шанс стати свідками того, як світ стане ще більш взаємозалежним в наступні роки. Це експоненціальне зростання в даний час кидає виклик двом великим проблемам, безпеці і масштабованості, і жодна з них не має легкого рішення.

IoT створює нові можливості та надає конкурентну перевагу підприємствам на сучасних та нових ринках. Він торкається всього, а не лише даних – а як і коли, де і чому ви їх збираєте. Технології, які створили Інтернет речей, не лише змінюють Інтернет, але змінюють речі, підключені до Інтернету - пристрої та шлюзи на краю мережі, які тепер можуть запитувати послугу або запустити дію без втручання людини на багатьох рівнях.

Оскільки генерація та аналіз даних є настільки важливими для ІТ, необхідно враховувати захист даних протягом всього його життєвого циклу. Керування інформацією на всіх рівнях є складним, оскільки дані будуть проходити через багато адміністративних кордонів з різними політиками та намірами.

Враховуючи різні технологічні та фізичні компоненти, які дійсно становлять екосистему IoT, доцільно розглянути IoT як систему систем. Архітектура цих систем, що забезпечують бізнес-цінність організаціям, часто стає складною задачею, оскільки архітектори підприємств розробляють інтегровані рішення, що включають в себе кращі пристрої, програми, транспорт, протоколи та аналітичні можливості, що складають повністю функціонуючу систему IoT. Ця складність вказує на проблеми, пов'язані з підтримкою безпеки IoT, і гарантування того, що окремих екземплярів IoT не може використовуватися в якості точки переходу, щоб атакувати інші системи інформаційних технологій (ІТ) підприємств.

Технологія Blockchain - це кращий метод для вирішення проблем масштабованості, конфіденційності та надійності в Інтернеті речей. Технології Blockchain можуть стати головним рішенням, необхідним для вирішення проблем в галузі IoT. Технологія Blockchain може використовуватися для відстеження мільярдів підключених пристроїв, забезпечення обробки транзакцій та координації між пристроями, вона забезпечує значні заощадження для виробників галузі IoT. Цей децентралізований підхід дозволить виключити окремі пункти відмови, створюючи більш стійку екосистему для роботи пристроїв. Криптографічні алгоритми, які використовуються Blockchain, зроблять дані споживачів більш приватними.

Метою роботи є дослідження можливих способів впровадження Blockchain в Інтернет речей з урахуванням специфіки обчислювальних потужностей пристроїв IoT.

Була проаналізована проблема візантійських генералів, яка є класичною проблемою децентралізованих обчислень. В рамках цього дослідження було проведено аналіз алгоритмів досягнення консенсусу в децентралізованій мережі, і її стійкість до зовнішніх і внутрішніх загроз безпеки.

І було встановлено які алгоритми консенсусу слід використовувати для такого об'єкта, як екосистема Інтернету речей, на базі технології Blockchain. Можна виділити наступні алгоритми консенсусу, які можуть вирішити проблему візантійських генералів:

- Proof Of Work / PoW

- Proof of Stake / PoS
- Nothing at Stake в PoS / Нічого втрачати
- Proof of Stake Time / PoST
- Delegated Proof Of Stake / DPOS
- TAPOS / Транзакції, як доказ частки
- dBFT / Делегована задача візантійських генералів
- BFT алгоритм
- Proof Of Activity / Доказ діяльності
- Proof of Capacity и Proof of Storage
- Proof of Importance / Доказ важливості
- Directed Acyclic Graphs / Спрямований ациклічний граф

#### **Висновки:**

- Проведено дослідження проблеми безпеки і масштабованості екосистеми Інтернет речей.
- Проведено дослідження можливості впровадження Blockchain технології в існуючі екосистеми IOT на базі протоколу MQTT.
- Був зроблений аналіз алгоритмів, які вирішують проблеми візантійських генералів в децентралізованих обчислювальних системах.
- Проаналізовано існуючі платформи для створення децентралізованих сервісів на базі Blockchain.
- В рамках цього дослідження була розроблена архітектура системи, яка дозволяє підключити мікроконтролер ESP32 до різних технологій Blockchain, таким як Ethereum і Hyperledger fabric.
- Доведено актуальність розвитку та реалізації теми роботи в подальшому.

#### **Література**

1. Raval S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology – O'Reilly Media, 2016. — 118 p.
2. Understanding Cryptography: A Textbook for Students and Practitioners – Springer-Verlag, 2010. — 372 p.
3. Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners - Apress, 2017. — 185 p.
4. Hands-On Blockchain with Hyperledger - Packt Publishing, 2018. — 663 p
5. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations – CRC, 2016 – 586 с.