

В.Д. Бойко, М.Д. Василенко, В.П. Новіков, В.О. Рачук

Національний університет «Одеська юридична академія», Україна

## «РОЗУМНЕ МІСТО» В КОНТЕКСТІ РОЗВИТКУ ТЕХНОЛОГІЙ БЛОКЧЕЙН

*Стаття присвячена дослідженню реалізації «розумного міста» в контексті використання технологій блокчейн. У разі «розумного міста» для успішної цифрової трансформації виділені вимоги до вироблення стратегії, адаптації персоналу до нових команд і впровадження нових технологій, специфічних для міського середовища. При технологіях блокчейн використання криптографічних систем дозволяє створити нові можливості конфіденційності й швидкості обміну інформацією та керування, виявленими в проявах технологій блокчейн. Важливим компонентом такої системи стає «ключ», який представляє першу ланку в ланцюзі блокчейну. Він може зберігатися поза системою і використовуватися для різних перевірок в діяльності підрозділів апарату органів місцевого самоврядування та комунальних підприємств міста. З наукової точки зору використання технологій блокчейн веде до потреби в проведенні міждисциплінарних досліджень та застосування результатів для різних додатків з визначенням стратегій та соціальних наслідків таких заходів.*

**Ключові слова:** «розумне місто», міське господарство, комп'ютерні технології, Інтернет речей, блокчейн, застосування, кібербезпека.

### Постановка проблеми

За визначенням Британського інституту стандартів (BSI) «розумне місто» становить ефективну інтеграцію фізичних, цифрових і людських систем в штучному середовищі заради сталого, безпечного та всебічного майбутнього для громадян, що має проявлятися у вигляді системи пов'язаних між собою технологій, які керують міськими процесами. Технології контролюють роботу транспорту, рятувальних служб, медичних установ, а також допомагають вирішувати всі адміністративні та фінансові питання підприємств. Вважається, що впровадження блокчейну в міста допоможе позбутися від проблем з переповненими дорогами, неефективним транспортним сполученням і високою вартістю послуг житлово-комунального господарства. Фактично таке місто являє єдину систему, в якій органічно взаємопов'язані міські комунікації, інформаційні технології передачі даних та пристрої IoT (Інтернет речей), тобто безпосередньо пов'язане з автоматизацією життєдіяльності міста, в першу чергу, розвитком систем штучного інтелекту завдяки масовому доступу до мережі Інтернет та мініатюризації електроніки, розвитку новітніх технологій. «Розумне місто» передбачає інтеграцію інформаційно-комунікаційних технологій (ІКТ) та Інтернету речей (IoT) для управління майном міста; а, як відомо, його активи включають, зокрема, місцеві відділи інформаційних систем, системи транспорту та водопостачання, електростанції, соціальну та правохоронну інфосистему, управління відходами, а

також інші комунальні та громадські служби. Все це має робитися в кінцевому результаті для підвищення ефективності обслуговування і задоволення потреб жителів міст, і не тільки великих, покращуючи якість їх життя через застосування ІКТ, які дозволяють міській владі безпосередньо взаємодіяти й стежити за тим, що відбувається в місті та яким чином місто розвивається. Так, з появою Інтернет-технологій виникли проблеми, пов'язані з особливостями самої мережі Інтернет, де існує потенційна анонімність суб'єктів з невизначеністю їх юрисдикції, правдивістю отриманої інформації, часом здійснення транзакцій та рядом інших чинників [1]. Це стосується й застосування технологій блокчейну в різних галузях міського господарства. Наприклад, блокчейн знайшов чимало застосувань в транспортній справі: від складання транспортних накладних і журналів супроводження до розробки логістичних схем. Блокчейн в транспортному бізнесі являє собою діяльність з розмежуванням прав та із застосуванням відкритих та і закритих списків. У відкритих списках пріоритет віддається ідентифікації перед анонімністю, вибіркової перевірці перед протоколом докази роботи. Отже, на транспорті найбільше значення мають реєстр із загальним доступом, розумні контракти і привілеї, щоб можна було забезпечувати безпеку, автентичність і верифікацію поряд з консенсусом, принципом запевнення транзакції в якості легітимної усіма учасниками мережі. При цьому протягом існування всього циклу проблем ведеться пошук їх вирішення. Фактично саме технології блокчейн

формують сприятливі технологічні умови побудови розподілених систем міста для суб'єктів, що вступають транзакційні зв'язки між елементами системи у вигляді сукупного міського господарства.

### Аналіз останніх досліджень та публікацій

Існують роботи вітчизняних й іноземних авторів, в яких аналізується закордонний досвід впровадження IT-технологій в систему місцевого самоврядування для формування елементів в системі «розумне місто» (див., наприклад [2–5]). У роботі [5] її авторами досліджуються сучасні підходи до розуміння сутності понять «розумне місто» та електронне місто (е-місто) в контексті розвитку електронного урядування на місцевому рівні, однак такий підхід формує лише розуміння питань е-урядування на місцевому рівні. Так, авторами [6] цифрова трансформація міст розглядається вже як зміна наявних бізнес-моделей функціонування міських служб, створення розумної мобільності, організація розумного ресурсоспоживання. Там же зроблено висновок, що формування «розумних міст» в Україні гальмується відсутністю технічної бази для створення платформ інформаційних технологій; також не розроблена дорожня карта цифрової трансформації національної економіки, тобто наголошується на відсутність або недосконалість технічної складової проблеми. Цю складову автори цієї статті (В.Б., М.В.) раніше вже частково обговорювали в площині кібербезпеки та штучного інтелекту в своїх роботах [7, 8]. Автори [8] (В.Б. та М.В.) пропонують стратегії впровадження систем штучного інтелекту для обробки великих даних і підтримки прийняття рішень в роботі комунального господарства «розумного міста». Аналізуються і даються рекомендації щодо можливого використання систем штучного інтелекту для обробки даних і підтримки прийняття рішень для таких систем. Як було показано авторами в [8], при структуруванні міського середовища основними стейкхолдерами (зацікавленими сторонами), джерелами даних і бенефіціарами при роботі з системами «розумного міста» стають місцева влада і представники бізнесу з одного боку, і жителі та гості міста з іншого боку. У цій роботі докладно описано цей двосторонній процес як процес взаємодії та обміну даними між стейкхолдерами, на що було зроблено додатковий акцент, а також виявлені способи взаємодії між ними в рамках міської інформаційної екосистеми (оперативне високорівневе управління міським середовищем, мереживоцентрична низова самоорганізація, що випереджає міське управління і системи громадського інформування), про що вперше було прописано в [9], а також в [10, 11].

**Метою статті** є аналіз Інтернету речей (IoT) в «розумному місті» та виявлення проявів розвитку

технологій блокчейн з можливістю їх практичного застосування в системі та підсистемах такого міста.

### Виклад основного матеріалу дослідження

Можна впевнено говорити про те, що зазвичай, галузі, які покращують технологію «розумного міста», охоплюють державні та муніципальні послуги, управління міської транспортної мережі, раціональне використання електричної та іншої енергії, охорону здоров'я, раціональне використання води, і утилізація відходів тощо. Оптимальне використання всіх можливостей, що надаються цифровим містом, не зводиться до простого перенесення паперового діловодства в онлайн. При переході до «розумного міста» відбувається процес цифрової трансформації, який має на увазі не тільки установку сучасного обладнання або програмного забезпечення, але й передбачає фундаментальну зміну в робочих процесах, отриманні даних і наданні послуг [12, 13]. Впровадження цифрового робочого процесу має на увазі перехід, при якому багато процесів автоматизуються і часто виконуються взагалі без участі людини. При цьому цифрування і створення спільних баз даних дозволяє отримати системний ефект, а не просто економію паперу.

Отже, системне використання цифрових можливостей, що виникають при трансформації щодо покращення добробуту міста, може бути умовно поділено на наступні категорії. Вважаємо, що має сенс обговорити їх детальніше.

**Мінімізація бюрократії.** При використанні цифрових технологій замість отримання документів і надання перехресних довідок, перевірка здійснюється автоматично за допомогою робочих баз даних. Завдяки тому, що «розумне місто» (а, можливо, і «розумна держава») становлять інтегроване інформаційне середовище, дані одних підрозділів завжди доступні й готові до використання іншими підрозділами. При цьому істотно зменшується час і витрати на «перекладання паперу» замість отримання підтверджувальних документів в одному підрозділі (або установі в будь-якій міській організаційній одиниці) для передачі в дані в інше місце, а процес синхронізації відомостей виконується шляхом одного-двох запитів між базами даних або інформаційними системами підрозділів.

Прикладом може бути ситуація з переїздом і зміною адреси, коли контракти на комунальні послуги, інтернет та інше автоматично переформлюються на нову адресу, при цьому також автоматично відбувається перевірка заборгованості. Тоді вже зникає потреба відвідувати кожний підрозділ окремо і писати заяву або сповіщати про переїзд кожний підрозділ через його власний сайт.

Зміна адреси користувача системи автоматично змінює його у всіх пов'язаних базах даних.

Іншим прикладом є автоматична синхронізація історії хвороби пацієнта при потраплянні в лікарню, навіть якщо до цього пацієнт проходив лікування в іншій лікарні.

**Надання бізнесу відкритих інтерфейсів взаємодії.** Інтеграція інформаційних систем міста може бути також використана для спрощення взаємодії з бізнесом і надання додаткових послуг, що не тільки знімає навантаження з міських організацій обліку, але і може служити додатковим джерелом доходу.

Приклад використання демонструється покупкою і реєстрацією машини в перебігу п'яти хвилин, коли оформлення відбувається автоматично, за участю зареєстрованого в службі продавця, через API (Application Programming Interface, прикладний програмний інтерфейс) доступу до міської інфосистеми. При цьому, взаємодія може не обмежуватися простим доступом, продавець може перевірити кредитну історію покупця, наявність прав, паркувального місця та інше. Транспортний засіб покупця так само прозоро й автоматично стає на облік в службі міського руху, номер його машини, зв'язується з системами спостереження з оцінкою трафіку тощо.

**Можливість надання проактивних послуг.** При певних міських ініціативах і при досить щільній ув'язці інформаційних систем в рамках «розумного міста» можлива організація послуг, які взагалі не потребують початкової участі користувача. Наприклад, для отримання «дитячих» грошей батькам не потрібно нічого робити, гроші самі в потрібний час повинні приходити на рахунок.

Завдяки інтеграції міських інформаційних систем стає можливим швидке бронювання й обслуговування в готельному комплексі, виключи черги на стоянках, ще швидше введення системи цифрових проїзних на громадському транспорті [14]. Отже, розширюється доступ до проактивних послуг в міській інфраструктурі.

#### **Загальні вигоди від цифрової трансформації**

У роботі [15] наводиться приклад впровадження системи ET City Brain, яка дозволяє отримати суттєві ефекти від управління дорожнім трафіком і інтеграцією в міські системи інформаційних технологій. Наприклад, система дозволяє оптимізувати й поліпшити процес гасіння пожеж, надаючи для цього такі параметри як тиск води в системах пожежогасіння, наявність гідрантів в районі пожежі, наявність небезпечних матеріалів (типу залягання газових труб) та інше [14].

Машинам швидкої допомоги в регіоні Ханчжоу Сяошань більше не потрібно поліцейський ескорт для швидкого руху по вулицях. ET City Brain

дозволяє проаналізувати й спрогнозувати ситуацію на вулицях ще до виїзду швидкої допомоги, визначити оптимальну траєкторію руху і на всьому протязі маршруту забезпечити рух наскрізною роботою світлофорів на перехрестях. У порівнянні зі старим режимом руху (в супроводі дорожньої поліції) час в дорозі скоротився вдвічі.

Alibaba Cloud розробила додаток «Smart Healthcare», яке працює в хмарі й веде 8 мільйонів електронних медичних карт для 11 муніципальних лікарень. Це дозволяє економити в середньому по дві години під час прийому хворих. Особливої актуальності така система набуває зараз, через пандемію коронавірусу.

Забезпечення безпеки даних стало необхідною умовою цифрової трансформації. Перераховані вище переваги можуть бути реалізовані тільки при технічній можливості інтеграції інформаційних систем в єдину інформаційну екосистему «розумного міста» з відповідною кібербезпекою.

Зазвичай, серед вимог для успішної цифрової трансформації виділяють вимоги вироблення стратегії, вмотивованості команди, адаптації персоналу до нових команд і впровадження нових технологій, специфічних для міського середовища. У разі розумного міста до них додаються специфічні для його інформаційного ландшафту вимоги. Зокрема, йдеться про підвищені вимоги до швидкості реакції – наскільки швидко система розумного міста може виводити на ринок потрібні послуги і наскільки швидко дозволяє приводити їх до вимог чинного законодавства. Мається на увазі таке, як налагоджена система роботи з даними – датамайнінг, аналіз даних, широке залучення науки щодо роботи з даними (data science). При цьому одним з ключових чинників все ж таки залишається робота з даними, а кошти інформаційної екосистеми «розумного міста» повинні забезпечувати, крім "чотирьох V": volume, velocity, variety veracity – обсягу, швидкості, різноманітності й правдивості [16], ще і реальну безпеку оброблюваних даних. Суттєвим аспектом також стає розмежування доступу до інформації, розглянуте нами в роботі [17]. Безпека має на увазі як захист від зовнішніх атак, так і захист від внутрішніх атак, основною проблемою яких є можлива фальсифікація даних самими користувачами системи з метою отримання вигоди.

Практика показує, що в сучасних інформаційних системах недостатньо уваги приділяється питанням захисту від атак на систему з метою фальсифікації документів, доступу до потенційно цінної для конкурентів інформації тощо. Тому, при впровадженні та розгортанні систем «розумного міста» цьому аспекту безпеки слід приділити особливу увагу.

### Недостатність тривіального захисту додатків

В роботі [8] було показано, що системи «розумного міста» за своєю природою відкриті, тому їх бінарні файли в будь-який момент залишаються відкритими для дослідження, а отже, і для реверс-інжинірингу. Однак, практика, що використовується для захисту даних шляхом приховування і замовчування ("secure by obscure") не є ефективною: при достатній кількості часу і ресурсів аналіз бінарних файлів дозволить виявити будь-які спеціально залишені «бекдори» та «вразливі місця». Тому, захист такої системи не повинен покладатися на закритість вихідних кодів, хоча ніхто не забороняє використовувати це як додатковий рівень захисту, але слід розуміти всю ефемерність цього рівня. Якщо дані всередині програми не шифруються, то будь-які інші заходи захисту (паролі, «замки» і т.д.) є явно недостатніми. Будь-яке програмне забезпечення потенційно схильне до злому й можливих атак, тому слід виходити з того, що дані, які зберігаються у відкритій формі (наприклад, у вигляді окремих файлів або записів в базі даних), або зашифровані криптографічно предстають вже слабкою системою (запаролений zip-архів або пральний захист документа Microsoft Office), будуть рано чи пізно скомпрометовані [18]. Підкреслимо, що наведений в роботі [8] аналіз прикладу атаки Stuxnet показує, що сучасне шкідливе програмне забезпечення достатньо легко долає «повітряний проміжок» ("air gap"). Крім усього іншого, прагнення до створення "air gap" часто призводить до зниження загальної ефективності системи й підвищення витрат на її експлуатацію. Це особливо актуально для «розумного міста», де більшість систем розраховані на збір і обробку інформації в оперативному режимі й втрачають цінність для «офлайнових» контекстів. В цьому випадку організація "air gap" створює більше проблем, ніж вирішує їх.

Отже, специфіка роботи міської інформаційної екосистеми вимагає надійну систему, що дозволяє запобігти фальсифікації даних.

### Загальноприйняті підходи до захисту даних

В роботі [18] перераховані кілька загальноприйнятих підходів до ідеї захисту даних в додатках. Зокрема до них належать:

- захист даних в додатку з використанням сильної криптографічної системи з симетричними ключами;
- захист даних в додатку з використанням сильної криптографічної системи з асиметричними ключами, з можливою участю замовника;
- квітування обміну даними.

У згаданій вище роботі детально розглянуті їх переваги та недоліки. Зокрема при використанні сильної криптографічної системи з симетричними

або асиметричними ключами передбачається використання для зберігання даних системи симетричного або асиметричного шифрування. При цьому, в залежності, від ролі користувача, доступ до даних існує завжди, що робить систему вразливою для атаки з боку її користувача – отримавши доступ до даних він може використовувати свій ключ для «відкриття» системи й зміни її даних. Крім того, завжди існує ймовірність викрадення ключа, атак типу "man-in-middle" і так далі. Крім того, система не забезпечує можливості контролю загальної цілісності даних, тому може бути побудована схема фальсифікації при якій дані внесені в базу в присутності замовника, можуть бути пізніше просто видалені до того, як інформація буде синхронізована з центральною базою даних.

Варіантом використання криптографічної системи є використання системи відкритих ключів із залученням до процесу підписування документа замовника. В цьому випадку документація шифрується, або додатково завіряється кваліфікованим цифровим підписом з ключем замовника. Цей підхід отримує ширше поширення, однак на практиці його сильно обмежує неоднорідна оснащеність користувачів апаратним і програмним забезпеченням, питання, пов'язані з практикою законодавчих заборон сильної криптографії в різних країнах, вартістю і трудомісткістю впровадження інфраструктури й т.д.

Ще одним варіантом забезпечення верифікації є впровадження системи квітування транзакцій – інформаційного аналога паперової системи подвійного запису. В цьому випадку транзакції синхронно дублюються такими на центральному, або резервному сервері. Кожна дія фіксується відправленням повної або часткової «квитанції» про дії на зовнішній носій. Ведеться паралельно два журнали записів, всередині системи, та на зовнішньому сервері.

Така система також досить широко використовується, причому частина для економії та оптимізації передачі даних в процесі самої транзакції передається тільки «ключ» з контрольною сумою транзакції, а основна частина документа синхронізується пізніше, зі звіткою контрольних сум. Однак, така система також має свої уразливості й схильна до атак [18].

### Використання блокчейна для захисту даних в екосистемі розумного міста

Технологія блокчейн (blockchain, або просто блокчейн, блокчейн-технологія) отримала широку популярність завдяки використанню для децентралізованої експлуатації цифрових валют (криптовалюта) і в системах смартконтрактів (див. [18]). При цьому вона може бути використана не тільки в цих галузях, а й для контролю цілісності

даних в загальному випадку. Заснована на використанні блокчейнів система буде позбавлена недоліків щодо перерахованих вище систем, вона не буде вимагати дорогої й ненадійної системи квітування каналу зв'язку, буде пред'являти мінімальні вимоги до інфраструктури замовника. Вона може бути реалізована на різних рівнях захисту, а саме, в залежності від вимог до безпеки інформації, що використовується.

Це дозволить гнучко впроваджувати й розгортати цю систему при роботі в різних контекстах міської інформаційної екосистеми.

Важливим компонентом такої системи є «ключ», який представляє першу ланку в ланцюзі блокчейна і може зберігатися поза системою і використовуватися для різних перевірок при необхідності. При цьому контроль за цілісністю інформації може здійснюватися як на щоденній (щотижневій, щомісячній, щоквартальній) основі, коли кожна процедура має на увазі скидання "ланцюжка" блокчейна і заміну "ключа" новим, так і на основі безперервного контролю, коли вся інформація в системі замкнута на один глобальний ланцюжок даних протягом усього часу експлуатації системи й після відповідної сертифікації може служити в тому числі підтверджувальним документом для зовнішніх інстанцій-контролерів.

Отже, різні рівні реалізації пред'являють різні вимоги до інфраструктури, однак, в будь-якому випадку, ці вимоги будуть значно скромніше, дешевше й ефективніше, ніж перераховані вище традиційні системи захисту.

## Висновки

Оскільки технології блокчейн як система представляють собою мережу, що складається з підсистем у вигляді комп'ютерів, які утворюють ланцюжок блоків (списків), який містить набір транзакцій, можлива оптимізація (мінімізація) бюрократичного апарату, створюючи основу міського самоврядування зі створенням спільних баз даних синхронізацією інформації. Таку інтеграцію доречно використовувати для спрощення взаємодії з бізнесом і надання додаткових послуг, що знімає навантаження з міських організацій обліку і розподілу, а й може служити додатковим джерелом доходу внаслідок оптимізації роботи з даними. При технологіях блокчейн використання криптографічних систем дозволяє створити нові стратегії конфіденційності й швидкості обміну інформацією та керування, виявлення проявів розвитку технологій блокчейн. Важливим компонентом такої системи є «ключ», який представляє першу ланку в ланцюзі блокчейна і може зберігатися поза системою і використовуватися для різних перевірок в діяльності підрозділів апарату органів місцевого та комунальних підприємств міста.

Впровадження технологій блокчейн та їх практичне застосування в системі та підсистемах «розумного міста» відкривають принципово нові можливості для розвитку великих міст за допомогою цифровізації міського середовища. З наукової точки зору використання в майбутньому технологій блокчейн веде до потреби в проведенні міждисциплінарних досліджень та їх застосування для різних додатків для визначення стратегій і соціальних наслідків такого застосування, цілісністю і повнотою використаних даних, кібербезпекою суспільного, а також захистом приватності та конфіденційності приватного змісту міста.

## Література

1. Баранов А.А. Интернет: объект правоотношений и предмет регулирования : монография / А.А. Баранов. – К. : Ред. журн. "Право Украины", 2013. – 144 с.
2. Інституційні та організаційні засади впровадження електронного урядування: краці зарубіжні практики / За заг. ред.: С.А. Чукут, О.В. Загвоської. — К.: НАДУ — К., 2011. — 172 с. [Електронний ресурс]. — Режим доступу: [http://ktrpi.kpi.ua/?page\\_id=4160](http://ktrpi.kpi.ua/?page_id=4160)
3. Кунанець Н.Е., Небесний Р.М., Мацюк О.В. Особливості формування цілей соціальних та соціо-комунікаційних складових у проектах "розумних міст" // Вісник Національного університету "Львівська політехніка". Інформаційні системи та мережі. – 2016. – № 854. – С. 257–274.
4. Leo Hollis (2015) "Cities Are Good for You. The Genius of the Metropolis" [Електронний ресурс]. – Режим доступу: [http://citiesaregoodforyou.com/about/досвід\\_№13/2016](http://citiesaregoodforyou.com/about/досвід_№13/2016)
5. Чукут С.А., Дмитренко В.І. Смарт-сіті чи електронне місто: сучасні підходи до розуміння впровадження е-урядування на місцевому рівні. Інвестиції: практика та досвід. – 2016. – № 13. С. 89–93.
6. Єришова О.Л., Бажан Л.І. Розумне місто – концепція, моделі, технології, стандартизація. Статистика України. – 2020. – № 2–3. – С. 68–76.
7. Бойко В.Д., Василенко М.Д. Кібербезпека розумних міст: соціальні аспекти, ризики деанонізації і доксіну // Комунальне господарство міст. Сер.: технічні науки та архітектура. – 2020. – Вип. 6 (159). – С. 186–195.
8. Бойко В.Д., Василенко М.Д. "Розумне місто" в контексті системи штучного інтелекту та великих даних: можливі стратегії, ризики // Комунальне господарство міст. Сер.: технічні науки та архітектура. – 2021. – Вип. 1(161). – С. 241–249.
9. Lim, Chiehyeon, Kwang-Jae Kim, and Paul P Maglio. 2018. "Smart Cities with Big Data: Reference Models, Challenges, and Considerations." *Cities* 82: 86–99. <https://www.sciencedirect.com/science/article/pii/S0264275117308545#bb0165>.
10. Appio, Francesco Paolo, Marcos Lima, and Sotirios Paroutis. 2019. "Understanding Smart Cities: Innovation Ecosystems, Technological Advancements, and Societal Challenges." *Technological Forecasting and Social Change* 142: 1–14.
11. Kong, Lingqiang, Zhifeng Liu, and Jianguo Wu. 2020. "A Systematic Review of Big Data-Based Urban Sustainability

Research: State-of-the-Science and Future Directions.” *Journal of Cleaner Production*, 123142.

12. Perätalo, Sari, and Petri Ahokangas. 2018. “Toward Smart City Business Models.” *Journal of Business Models* 6 (2): 65–70.

13. Cocchia, Annalisa. 2014. “Smart and Digital City: A Systematic Literature Review.” In *Smart City*, 13–43. Springer.

14. “City Brain Now in 23 Cities in Asia.” 2020. Alibaba Cloud Community. [https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia\\_595479](https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479).

15. “The Chronicles of Cloud Building in Hangzhou: Part 2.” 2020. Alibaba Cloud Community. [https://www.alibabacloud.com/blog/the-chronicles-of-cloud-building-in-hangzhou-part2\\_594242?spm=a2c65.11461447.0.0.67f65385D3Cnxx](https://www.alibabacloud.com/blog/the-chronicles-of-cloud-building-in-hangzhou-part2_594242?spm=a2c65.11461447.0.0.67f65385D3Cnxx)

16. Saha, B., and D. Srivastava. 2014. “Data Quality: The Other Face of Big Data.” In *2014 IEEE 30th International Conference on Data Engineering*, 1294–97. <https://doi.org/10.1109/ICDE.2014.6816764>

17. Boyko, Viktor, and Nikolai Vasilenko. 2020. Cybersecurity of Smart Cities: Social Aspects, Risks of Deanonymization and Doxing. *Municipal Economy of Cities* 6 (159), 186–195. DOI: <https://doi.org/10.33042/2522-1809-2020-6-159-181-190>

18. Бойко, В.Д. 2018. “Верифікація Первичної Транспортної Документації с Исползованием Технологии Связных Списков.” *Електротехнічні системи та Комп’ютерні Системи*, no. 29(105): 127–35. <https://etks.opu.ua/?fetch=articles&with=info&id=1035>.

## References

1. Baranov A.A. Internet: the object of legal relations and the subject of regulation: monograph / A.A. Baranov. – K.: Ed. zhurn. “Law of Ukraine”, 2013. – 144 p.

2. Chukut, S.A. and Zahvojs’ka, O.V. (2011) Instytutsiyni ta orhanizatsiyni zasady vprovadzheniya elektronnoho uryaduvannya: krashchi zarubizhni praktyky, NADU, Kyiv, Ukraine. URL: [http://ktpu.kpi.ua/?page\\_id=4160](http://ktpu.kpi.ua/?page_id=4160).

3. Kunanets N.E., Nebesny R.M., Matsyuk A.V. Features of forming the goals of social and socio-communication components in Smart Cities projects. *Bulletin of the National University “Lviv politechnika”*. Information systems and networks. 2016. No. 854. pp. 257–274.

4. Hollis L. (2015) Cities Are Good for You. The Genius of the Metropolis. URL: <http://citiesaregoodforyou.com/about/>.

5. Chukut S.A., Dmitrenko V.I. Smart City or Electronic City: modern approaches to understanding the implementation of e-governance at the local level. *Investment: practice and experience*. 2016. No. 13. pp. 89–93.

6. Ershova O.L., Bazhan L.I. Smart City – concept, models, technologies, standardization. *Statistics of Ukraine*, 2020, No. 2–3. – Pp. 68–76.

7. Boyko V.D., Vasilenko M.D. (2020) Cybersecurity of smart cities: social aspects, risks of deanonymization and doxing. Scientific and technical collection. *Municipal Economy of Cities* 6(159). Pp. 186–195.

8. Boyko V.D., Vasilenko M.D. (2021) “Smart City” in the context of artificial intelligence and Big Data Systems: possible strategies, risks. *Municipal Economy of Cities* 1(161). Pp. 241–249.

9. Chiehyeon L., Kwang-Jae K., and Maglio P. (2018). “Smart Cities with Big Data: Reference Models, Challenges, and

Considerations.” *Cities* 82: 86–99. URL: <https://www.sciencedirect.com/science/article/pii/S0264275117308545#bb0165>.

10. Francesco Paolo A., Lima M., and Paroutis.S.(2019). “Understanding Smart Cities: Innovation Ecosystems, Technological Advancements, and Societal Challenges.” *Technological Forecasting and Social Change* 142: 1–14.

11. Kong L., Zhifeng L., and Jianguo W. (2020). A Systematic Review of Big Data-Based Urban Sustainability Research: State-of-the-Science and Future Directions. *Journal of Cleaner Production*, 123142.

12. Perätalo S., Ahokangas P. (2018). Toward Smart City Business Models. *Journal of Business Models* 6 (2): 65–70.

13. Cocchia A. (2014). “Smart and Digital City: A Systematic Literature Review.” In *Smart City*, 13–43. Springer.

14. City Brain Now in 23 Cities in Asia (2020) Alibaba Cloud Community. URL: [https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia\\_595479](https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479).

15. The Chronicles of Cloud Building in Hangzhou: Part 2 (2020) Alibaba Cloud Community. URL: [https://www.alibabacloud.com/blog/the-chronicles-of-cloud-building-in-hangzhou-part-2\\_594242?spm=a2c65.11461447.0.0.67f65385D3Cnxx](https://www.alibabacloud.com/blog/the-chronicles-of-cloud-building-in-hangzhou-part-2_594242?spm=a2c65.11461447.0.0.67f65385D3Cnxx).

16. Saha, B., and D. Srivastava (2014) Data Quality: The Other Face of Big Data. In *2014 IEEE 30th International Conference on Data Engineering*, 1294–97. URL: <https://doi.org/10.1109/ICDE.2014.6816764>.

17. Boyko V., Vasilenko.N. (2020). Cybersecurity of Smart Cities: Social Aspects, Risks of Deanonymization and Doxing. *Municipal Economy of Cities* 6(159). Pp. 186–195. DOI: <https://doi.org/10.33042/2522-1809-2020-6-159-181-190>

18. Boyko, V.D. (2018). Verification of Primary Transport Documentation Using The Technology Of Linked Lists. *Electrotechnical and Computer Systems*, No. 29 (105): 127–35. URL: <https://etks.opu.ua/?fetch=articles&with=info&id=1035>.

**Рецензент:** доктор технічних наук, професор В.М. Тупкало, Інститут інтелектуальної власності та права Національного Університету «Одеська юридична академія», Україна.

**Автор:** БОЙКО Віктор Дмитрович  
кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний університет «Одеська юридична академія»

E-mail – [boyko-work@ukr.net](mailto:boyko-work@ukr.net)

ID ORCID: <https://orcid.org/0000-0001-5929-657X>

**Автор:** ВАСИЛЕНКО Микола Дмитрович  
доктор фізико-математичних наук, доктор юридичних наук, професор, професор кафедри кібербезпеки, Національний університет «Одеська юридична академія»

E-mail – [nvas08@ukr.net](mailto:nvas08@ukr.net)

ID ORCID: <http://orcid.org/0000-0002-8555-5712>

**Автор:** НОВІКОВ В'ячеслав Пантелійович  
кандидат технічних наук, доцент, доцент кафедри  
кібербезпеки, Національний університет «Одеська  
юридична академія»  
E-mail – [novikovodessa0@gmail.com](mailto:novikovodessa0@gmail.com)  
ID ORCID: <https://orcid.org/0000-0003-2059-0581>

**Автор:** РАЧУК Валерій Олександрович  
асистент кафедри кібербезпеки  
Національний університет «Одеська юридична  
академія»  
E-mail – [rachuk960@gmail.com](mailto:rachuk960@gmail.com)  
ID ORCID: <https://orcid.org/0000-0003-1793-016X>

## SMART CITY IN THE CONTEXT OF BLOCKCHAIN TECHNOLOGY DEVELOPMENT

V. Boyko, M. Vasilenko, V. Novikov, V. Rachuk

National University "Odessa Law Academy", Ukraine

*The article analyzes how the use of digital technologies through working databases improves the infrastructure of the "smart city", improving the integrated information environment of the "smart city", synchronizing information between databases. The general benefits of digital transformation, the lack of trivial application protection, generally accepted approaches to data protection, and the use of blockchain to protect data in the smart city ecosystem are considered. It is shown that with certain urban initiatives and with a tight link between information systems within a "smart city", it is possible to organize services that do not require initial user participation at all. Among the requirements for successful digital transformation, there are requirements for developing a strategy, team motivation, adapting staff to new teams, and introducing new technologies specific to the urban environment. In particular, there are increased requirements for the speed of response, that is, how quickly the smart city system can bring the necessary services to the market and how quickly it allows them to comply with the legislation. Attention is drawn to the following generally accepted approaches to data protection: data protection in the application using a strong cryptographic system with symmetric keys, data protection in the application using a strong cryptographic system with asymmetric keys, with possible participation of the customer, flourishing data exchange. The use of cryptographic systems with blockchain technologies allows you to create new strategies for privacy and speed of information exchange and management. An important component of such a system is the "key", which represents the first link in the blockchain chain and can be stored outside the system and used for various checks in the activities of divisions of the apparatus of local and municipal enterprises of the city. From a scientific point of view, the use of blockchain technologies in the future leads to the need for interdisciplinary research and their application for various applications to determine the strategies and social consequences of such application.*

**Keywords:** "smart city", urban economy, computer technologies, blockchain, application, Internet of things, cybersecurity.