Онтології блокчейн-технологій

Виконав: Лесик Богдан Олександрович

студент групи ДА-62

Науковий керівник: Булах Богдан Вікторович

Предмет дослідження

- Онтологія – це один зі способів формалізації знань. Онтології предметної області концептуалізують модель із реального світу у спеціальний формат, з яким можуть працювати комп’ютери. Ці системи також здатні на логічні міркування на основі фактів та аксіом, які були явно записані до них.
- Блокчейн – це послідовно криптографічно пов’язані між собою блоки інформації (зазвичай транзакційної). Ця структура використовується для обліку фінансових операцій в мережі користувачів, які, взагалі кажучи, можуть не довіряти один одному, при цьому надійність операцій гарантується.
- Онтологія блокчейн-технологій – формалізована модель блокчейн-технології, яка на тому чи іншому рівні абстракції описує концепти блокчейну та їх взаємодію між собою, а також класифікує та структуризує технологію

Актуальність

Широке розповсюдження блокчейну та його безсумнівна популярність очікувано призводять до різноманіття таких технологій. Варіативність в архітектурах породжує ряд проблем:

- Суперечності в розробці законів та політик, пов’язаних з регулюванням блокчейн-технологій
- Зростаюча неоднозначність у застосуванні законів та правил захисту прав споживачів
- Зменшення точності академічних досліджень концепцій, які лежать в основі розробки нових програм та рішень

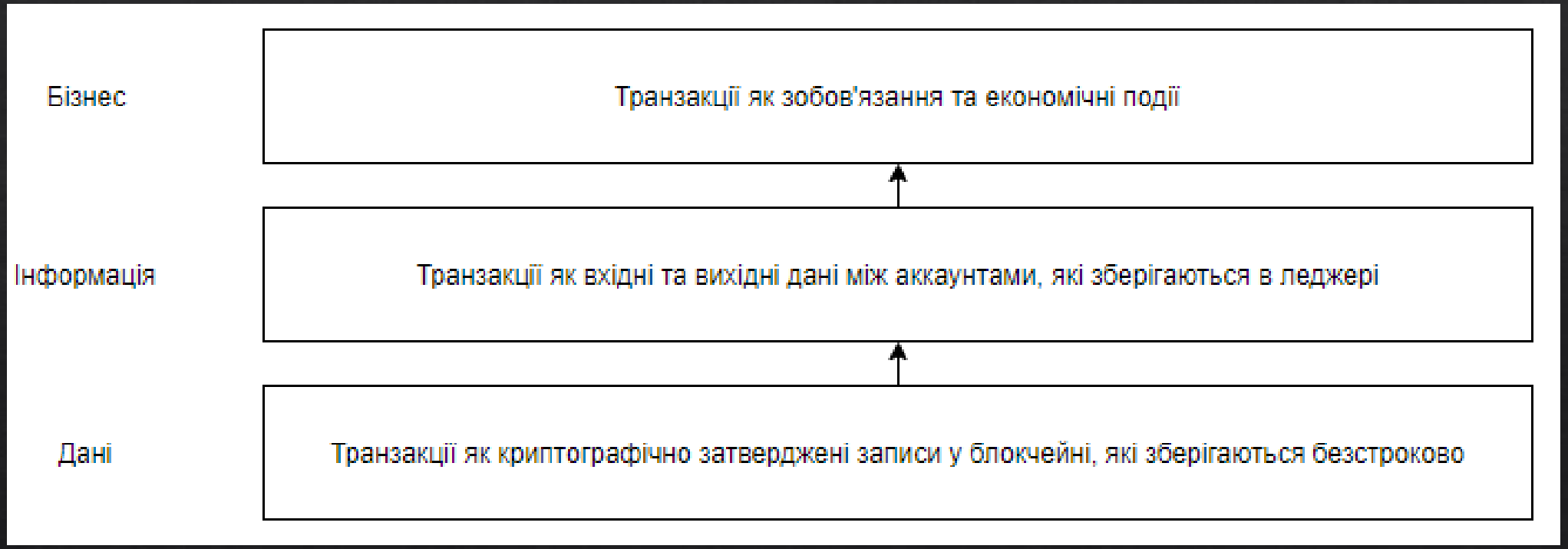
Одним із ефективних рішень цих проблем є стандартизація блокчейн-технологій та впровадження єдиної формальної моделі. У виконаній дипломній роботі було проведено дослідження можливості створення такої моделі за допомогою онтології.

Що потрібно для створення онтології?

- Команда розробки
  - Експерти з предметної області
  - Інженер онтології
  - Інженери програмного забезпечення
- Методика по створенню онтологій
- Інструментарій

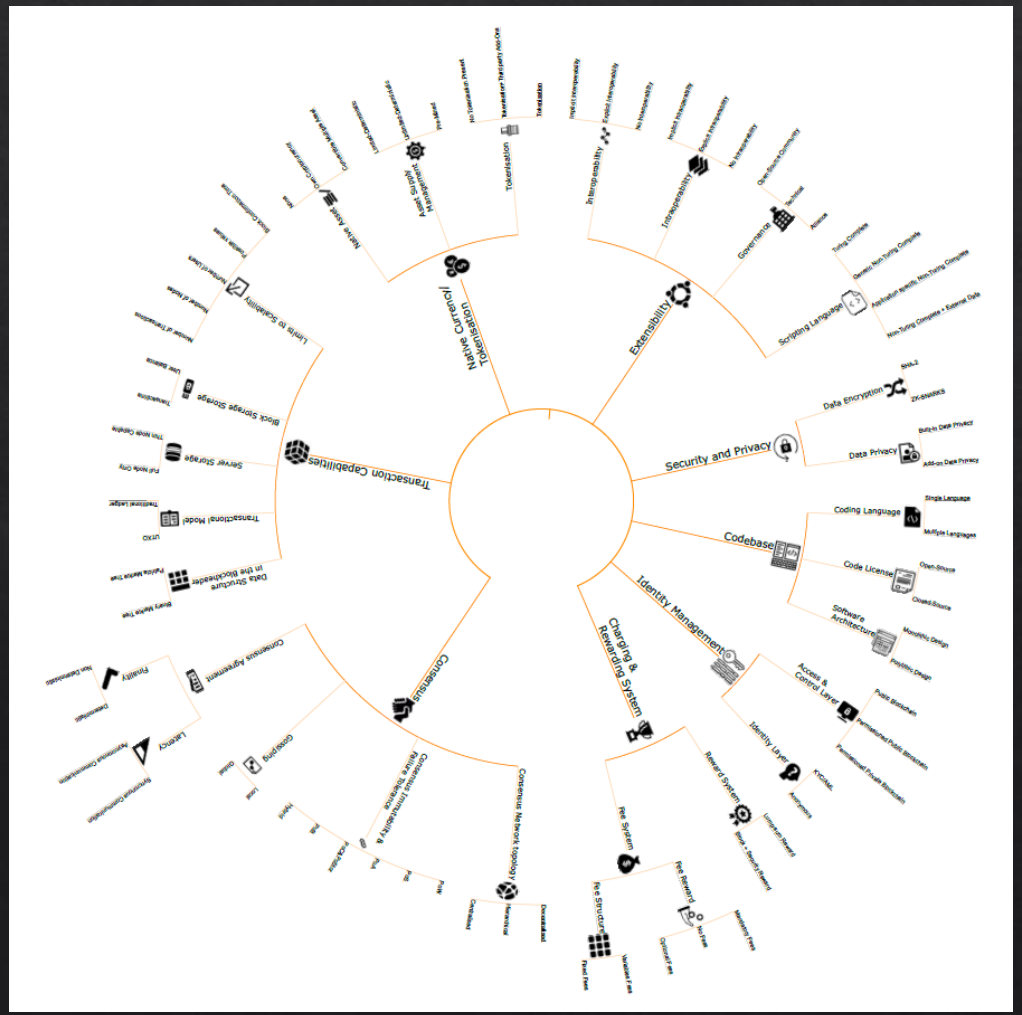
Аналіз існуючих робіт по концептуалізації блокчейн-технологій

- Towards a blockchain ontology by Joost de Kruijff, Hans Weigand.



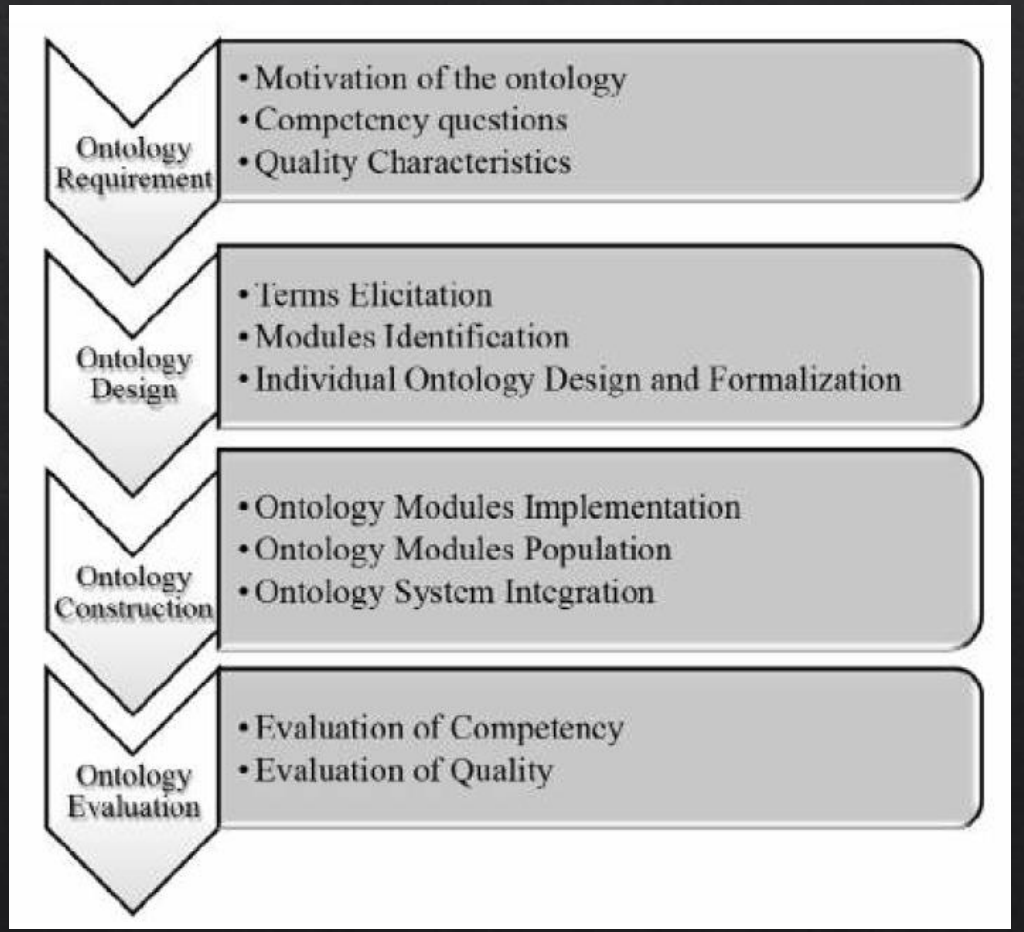
Аналіз існуючих робіт по концептуалізації блокчейн-технологій

- A Taxonomy of Blockchain Technologies: Principles of Identification and Classification by Paolo Tasca та Claudio J. Tessone. Налічує 8 основних компонентів, 34 підкомпоненти і 78 варіацій схем.



Вибір методики

Методика	Проектування, централізоване на користувачі	Модульно-орієнтована	Предметно-орієнтована	Придатна до розширення та ітеративна	Якісно-орієнтована	Оцінка на основі компетентності
Lenat, Guha (1989)	Ні	Так	Ні	Так	Ні	Ні
Grüninger, Fox (1995)	Так	Ні	Так	Ні	Так	Так
Uschold, King (1995), Uschold, Grüninger (1996)	Так	Так	Так	Ні	Так	Так
Bernaras et.al (1996)	Ні	Так	Так	Ні	Так	Ні
METHONTOLOGY	Так	Так	Так	Так	Так	Так
CommonKADS	Ні	Так	Так	Так	Ні	Ні
Noy, McGuinness (2001)	Так	Ні	Так	Так	Ні	Ні
NEON	Так	Так	Так	Так	Ні	Так
Maricela Bravo, Luis Fernando Hoyos Reyes, José A. Reyes Ortiz (2019)	Так	Так	Так	Так	Так	Так



Вибір середовища розробки

Рекомендації W3C

Критерії для вибору

- актуальна та якісно побудована документація до програми
- вільне використання повного функціоналу
- наявність покрокових інструкцій використання, прикладів та пояснень
- баланс між простотою використання та широким функціоналом.
- велика спільнота користувачів та поширеність використання
- актуальність продукту
- відкритий код

Створення онтології

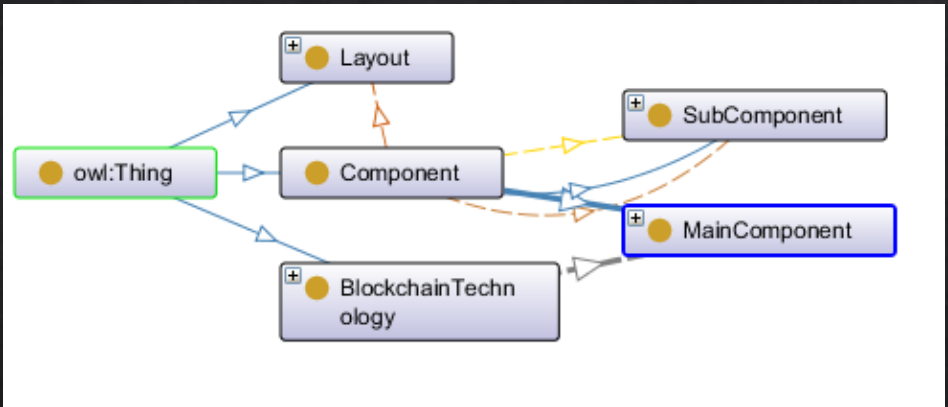
Ontology requirements specification

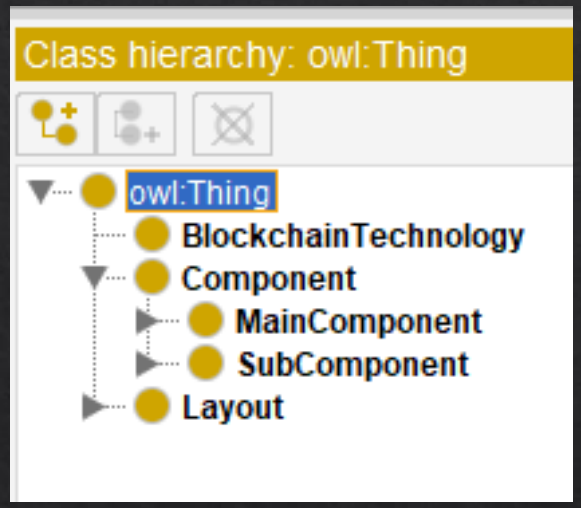
- Мотивація
- Сценарії використання
  - Прикладний
  - Освітньо-науковий
- Користувачі
- Список питань компетентності
  1) Які компоненти блокчейн-технології можна назвати основними?
  2) Які існують найпоширеніші алгоритми консенсусу?
  3) Які блокчейн-технології працюють за алгоритмом консенсусу Proof-of-work?
  4) Яким чином обмежена масштабованість у Bitcoin?
  5) У яких блокчейн-технологій скриптова мова повна за Тьюрингом?

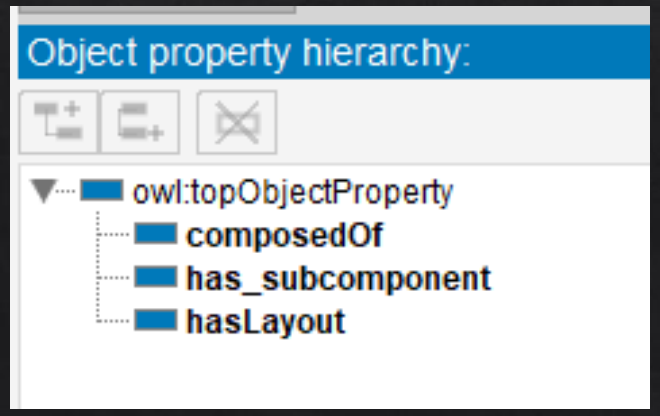
Створення онтології

Розробка онтології

- Набір концептів





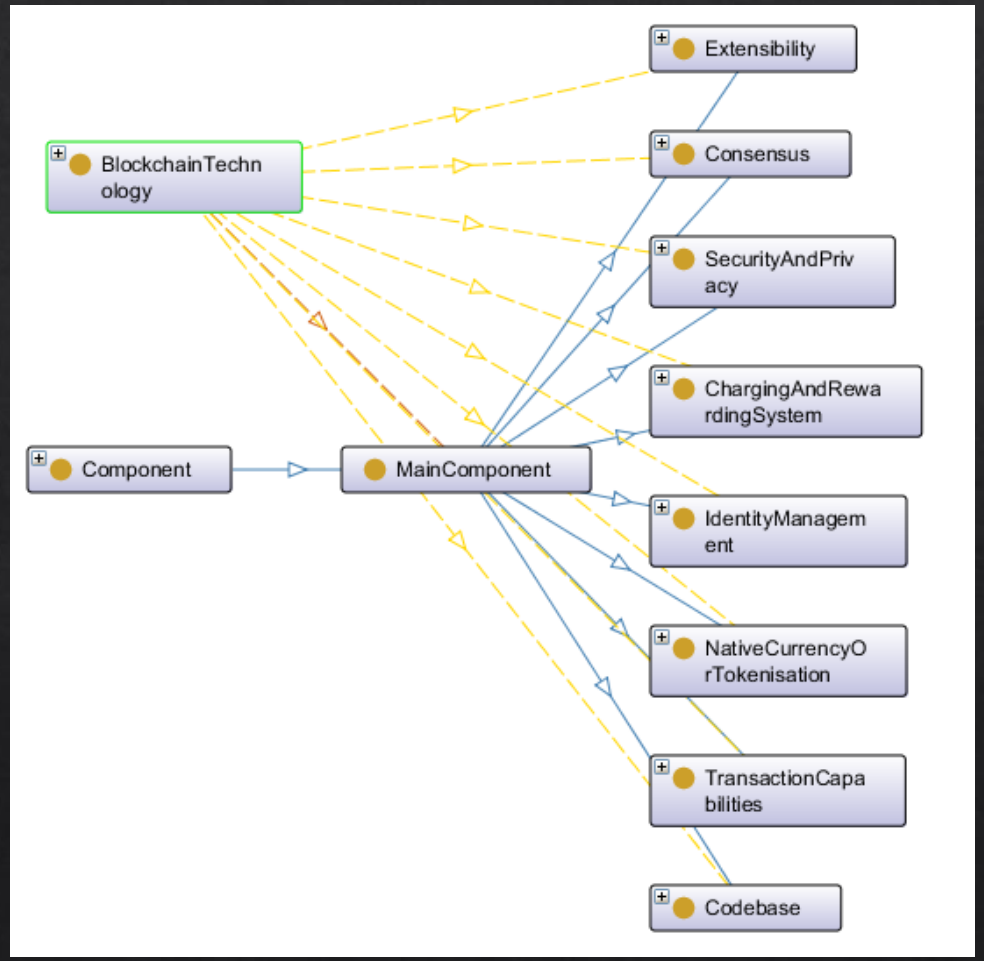


Створення онтології

Розробка онтології

Основні компоненти блокчейн-технології

- Консенсус
- Розширюваність
- Безпека та конфіденційність
- Система винагород та комісій
- Управління обліковими даними
- Нативна валюта/токенізація
- Кодова база
- Транзакційні можливості

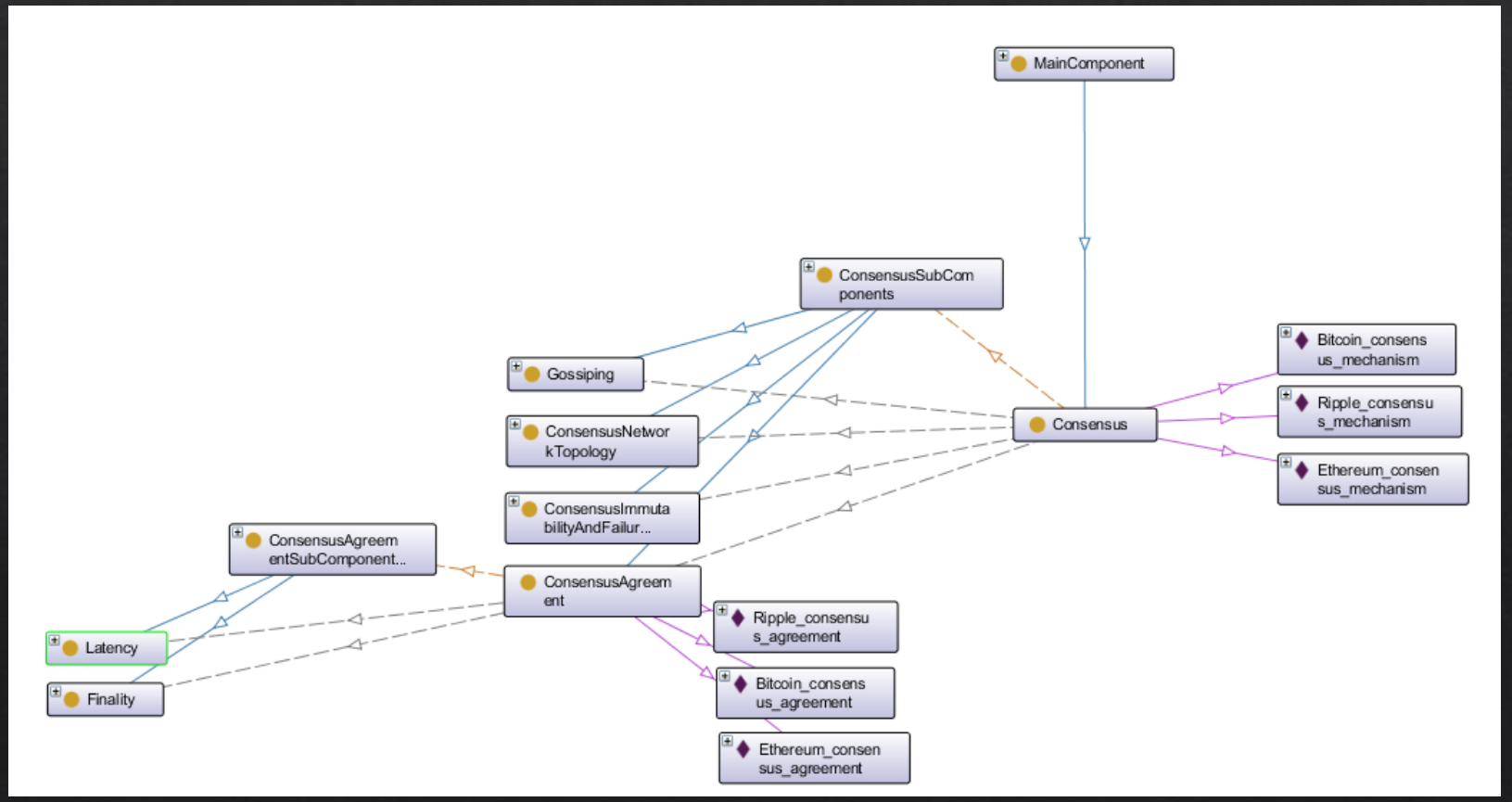


Створення онтології

Розробка онтології

Детальна будова основного компоненту «Консенсус»

- Госсипінг (розповсюдження інформації між вузлами)
- Топологія мережі
- Незмінність та відмовостійкість
- Досягнення консенсусу
  - Затримки в передачі
  - Остаточність



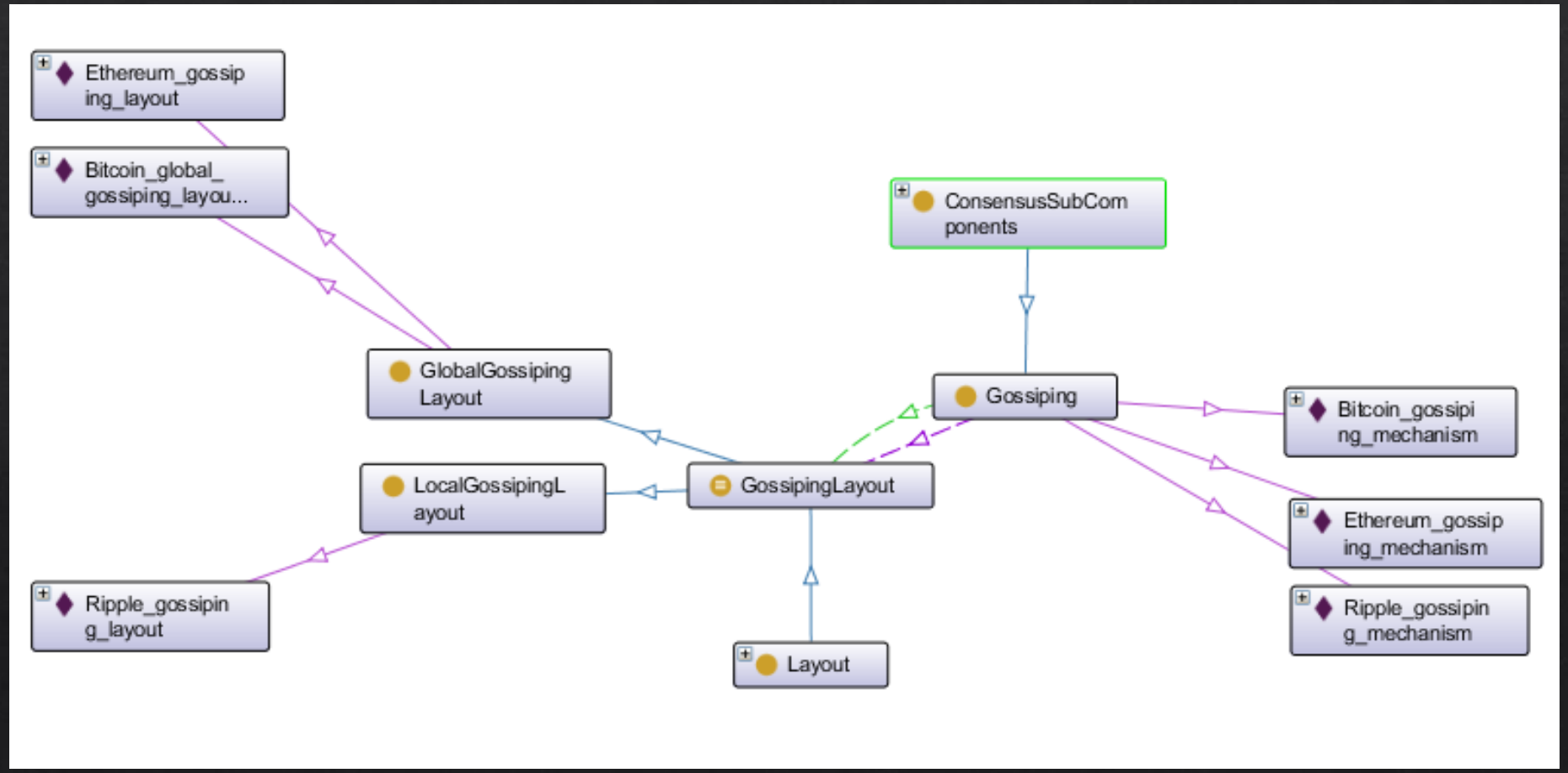
Створення онтології

Розробка онтології

Детальний розгляд підкомпоненту «Госсипінг»

Госсипінг може мати 2 можливі схеми:

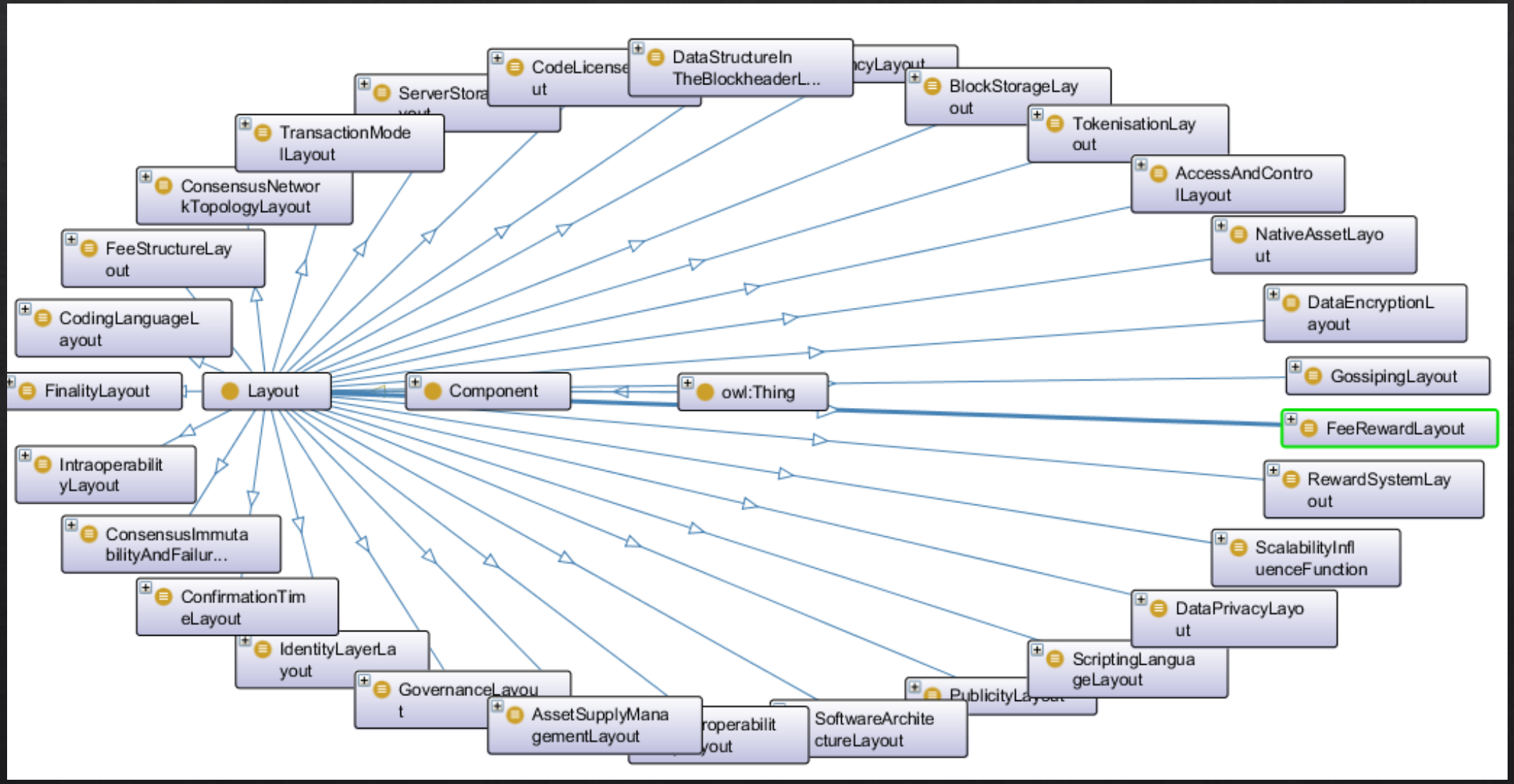
- Глобальний
- Локальний



Створення онтології

Розробка онтології

Повний набір схем компонентів



Створення онтології

Будова онтології

Метрики створеної онтології

Ontology metrics:

Metrics

Axiom	1536
Logical axiom count	776
Declaration axioms count	380
Class count	165
Object property count	4
Data property count	1
Individual count	211
Annotation Property count	2

Class axioms

SubClassOf	249
EquivalentClasses	30
DisjointClasses	63
GCI count	0
Hidden GCI Count	30

Створення онтології

Будова онтології

Популяція онтології

Bitcoin

- Публічний децентралізований Proof-of-Work
- Псевдоанонімність*
- UTXO*
- Підтримує «тонкі» вузли*

Ethereum

- Публічний децентралізований Proof-of-Work (1.x)*
- Псевдоанонімність*
- Традиційний леджер*
- Тільки повні вузли*
- Розумні контракти на Тьюринг-повній скриптовій мові*

Ripple (XRP)

- Публічний ієрархічний Ripple Consensus Algorithm*
- KYC та AML*
- Традиційний леджер*
- Конвертація валюти*

**Посилання на джерела вказані у звіті*

Оцінювання онтології

Які обмеження масштабованості є в технології Bitcoin?

Active ontology × | Entities × | Class matrix × | Individuals by class × | OWLViz × | DL Query × | OntoGraf × | SPARQL Query ×

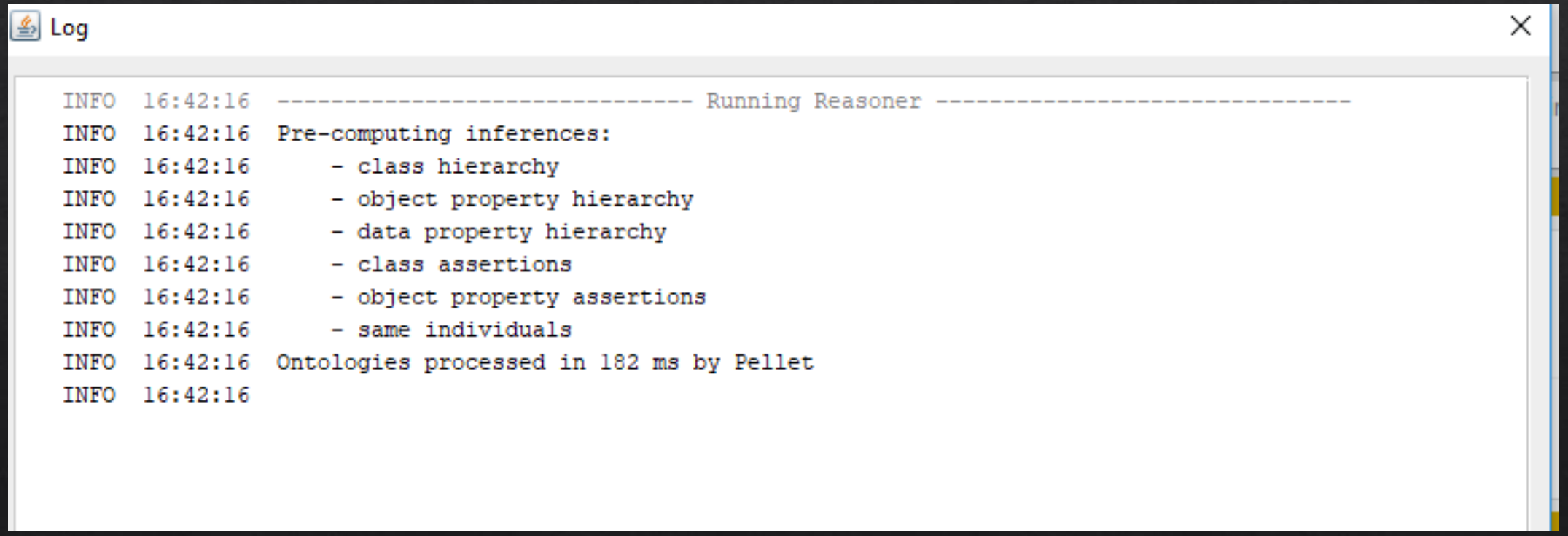
SPARQL query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX : <http://www.semanticweb.org/drast1c/ontologies/2020/4/Blockchain_component_ontology#>
SELECT ?individual ?sb ?layout ?class
      WHERE {
            ?individual rdfs:label ?label .
            ?individual :OWLObjectProperty_a140817a_3faf_4e99_b152_47767d3f071b ?sb .
            ?sb :OWLObjectProperty_756a60a0_ebea_4337_ad8e_569e1a0569dd ?layout .
            ?layout a ?class
            filter(?label= "Scalability_limits_in_Bitcoin"@en && ?class != owl:NamedIndividual)
}
```

individual	sb	layout	class
Scalability_limits_in_Bitcoin	Bitcoin_confirmation_time_limit	Bitcoin_confirmation_time_layout	StochasticConfirmationTimeLayout
Scalability_limits_in_Bitcoin	Bitcoin_number_of_transactions_limit	Number_of_transactions_in_Bitcoin	AtMostLinear
Scalability_limits_in_Bitcoin	Bitcoin_number_of_users_limit	Number_of_users_in_Bitcoin	Indifferent

Оцінювання онтології

Перевірка узгодженості за допомогою рушія семантичного міркування (reasoner) Pellet.



Висновки

- Блокчейн-технологія – надзвичайно комплексна система, концептуалізація якої вимагає значної обізнаності в предметі та суттєво ускладнюється варіативністю існуючих рішень
- Незважаючи на загальне падіння інтересу IT-спільноти до технологій семантичного веб, OWL-онтології залишаються стандартами де-факто для формалізованого опису знань предметної області. Потреба в онтології блокчейн-технологій існує, а зацікавленість ISO зайвий раз це підтверджує
- Запропонована онтологія містить чималу кількість концептів, однак її можна назвати MVP – minimum viable product. Потенціал розширення системи складно переоцінити. В залежності від особливостей призначення, онтологія може знайти використання як в прикладних так і в освітньо-наукових цілях

Дякую за увагу!