**Шилов Илья Михайлович Методы и алгоритмы построения устойчивых распределенных реестров с использованием многомерного блокчейна**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Шилов Илья Михайлович

Оглавление

Реферат

Synopsis

Введение

Глава 1. Анализ предметной области. Постановка цели и задач исследования

1.1. Устойчивые распределенные реестры

1.1.1. Понятие устойчивого распределенного реестра и методы построения подобных систем

1.1.2. Блокчейн

1.2. Устойчивые распределенные реестры и информационная безопасность

1.3. Приложения на основе устойчивых распределенных реестров

1.3.1. Bitcoin и производные

1.3.2. Ethereum: программируемый блокчейн

1.3.3. Cardano: доказанный PoS

1.3.4. Криптография с нулевым разглашением

1.3.5. Ripple: биржа на распределенном реестре

1.3.6. Hyperledger Fabric: распределенные реестры в промышленности

1.3.7. Corda R3: «блокчейн» для банковской сферы

1.3.8. BigChainDB: база данных на распределенном реестре

1.4. Проблемы устойчивых распределенных реестров

1.4.1. Проблемы криптовалют

1.4.2. Проблемы межсистемного взаимодействия

1.4.3. Проблемы децентрализованных приложений

1.4.4. Конфиденциальность информации в реестре

1.4.5. Формализация проблем с точки зрения информационной безопасности

1.5. Фреймворк универсальной композиции

1.6. Выводы

Глава 2. Многомерный блокчейн

2.1. Многомерный блокчейн и внешние транзакции

2.1.1. Сайдчейны как основа для многомерного блокчейна

2.1.2. Понятие многомерного блокчейна

2.1.3. Адресация в многомерном блокчейне

2.1.4. Внешние транзакции в многомерном блокчейне

2.2. Оценка безопасности устойчивых распределенных реестров в пределах многомерного блокчейна

2.2.1. Подход Nakamoto

2.2.2. Подход GHOST

2.2.3. Безопасность PoW решений. Подход IOHK

2.2.4. Безопасность PoS решений

2.2.5. Византийская безопасность

2.3. Оценка безопасности многомерного блокчейна

2.3.1. Модели многомерного блокчейна и связанных технологий

2.3.2. Вспомогательные утверждения

2.3.3. Утверждения о безопасности многомерного блокчейна

2.4. Оценка безопасности масштабирования с использованием многомерного блокчейна

2.5. Выводы

Глава 3. Протокол поиска и верификации блоков и транзакций

3.1. Понятие протокола поиска и верификации и подходы к его построению

3.2. Анализ безопасности методов построения протокола поиска и верификации блоков и транзакций

3.2.1. Централизованный подход

3.2.2. Подход, основанный на подмножествах

3.3. Стойкий протокол поиска и верификации блоков и транзакций

3.3.1. Свойства общего префикса и качества (чистоты) цепочки

3.3.2. Алгоритм работы протокола поиска и верификации

3.3.3. Доказательство безопасности протокола

3.3.4. Анализ протокола поиска и верификации блоков и транзакций

3.4. Выводы

Глава 4. Оценка многомерного блокчейна

4.1. Многомерный блокчейн и альтернативные решения

4.1.1. Многомерный блокчейн и свойства информационной безопасности

4.1.2. Сопоставление многомерного блокчейна с одномерным блокчейном

4.2. Экспериментальная проверка функционирования многомерного блокчейна

4.2.1. Описание программной модели

4.2.2. Экспериментальная проверка выполнения внешних транзакций

4.2.3. Экспериментальная проверка масштабирования

4.3. Алгоритм масштабирования блокчейна на основе многомерного блокчейна

4.4. Сферы применения многомерного блокчейна

4.4.1. Экономика на многомерном блокчейне

4.4.2. Многомерный блокчейн как система управления базами данных

4.4.3. Криптоэкономика на традиционных криптовалютах

4.4.4. Бизнес-инфраструктура на многомерном блокчейне

4.4.5. DNS на многомерном блокчейне

4.4.6. Система управления версиями на многомерном блокчейне

4.4. Выводы

Заключение

Список сокращений и условных обозначений

Словарь терминов

Список литературы

Список рисунков

Приложение А. Свойства информационной безопасности и устойчивые распределенные реестры

Приложение Б. GUC-модели устойчивого распределенного реестра

Приложение В. Многомерный блокчейн и системы управления базами данных

Приложение Г. Многомерный блокчейн и системы электронного документооборота

Приложение Д. Апробация результатов работы

Д.1. Свидетельство о государственной регистрации программы для ЭВМ

Д.2. Акт о внедрении результатов диссертационной работы в АО «Азимут»

Д.3. Лицензионный договор на использование программного обеспечения

Приложение Е. Основные публикации по теме диссертации

Е.1. Многомерный блокчейн и его преимущества

Е.2. Модель устойчивого распределенного реестра для анализа безопасности многомерного блокчейна

Е.3. Безопасность протокола поиска и верификации в многомерном блокчейне

Е.4. Multidimensional blockchain security analysis