конференция РусКрипто

компания Актив

Обзор подходов к созданию низкоресурсных блокчейн-решений для применения в устройствах интернета вещей

Сергей Панасенко,
компания «Актив»
panasenko@guardant.ru

Структура данных блокчейна

Блоки формируются узлами (nodes): узел формирует блок после получения права на его формирование в результате выполнения протокола консенсуса.

Обычно также применяется электронная подпись:
на уровне блоков и/или
на уровне транзакций.

Классификация блокчейнов по степени доверия к узлам :

- приватный
- консорциумный
- публичный

Интернет вещей и блокчейн

Полезные свойства блокчейна для применения в Интернете вещей (IoT):

- механизмы поддержания целостности, аутентичности и привязки ко времени встроены в основу блокчейна и обеспечены криптографическими алгоритмами
- прозрачность данных (в том числе, легкость определения и подтверждения источника данных)
- децентрализация
- невозможность удаления данных, внесенных ранее в блокчейн

Эволюция IoT *:

* Рисунок из D.Stefanescu et al. A Systematic Literature Review of Lightweight Blockchain for IoT. 2022.

Низкоресурсный блокчейн

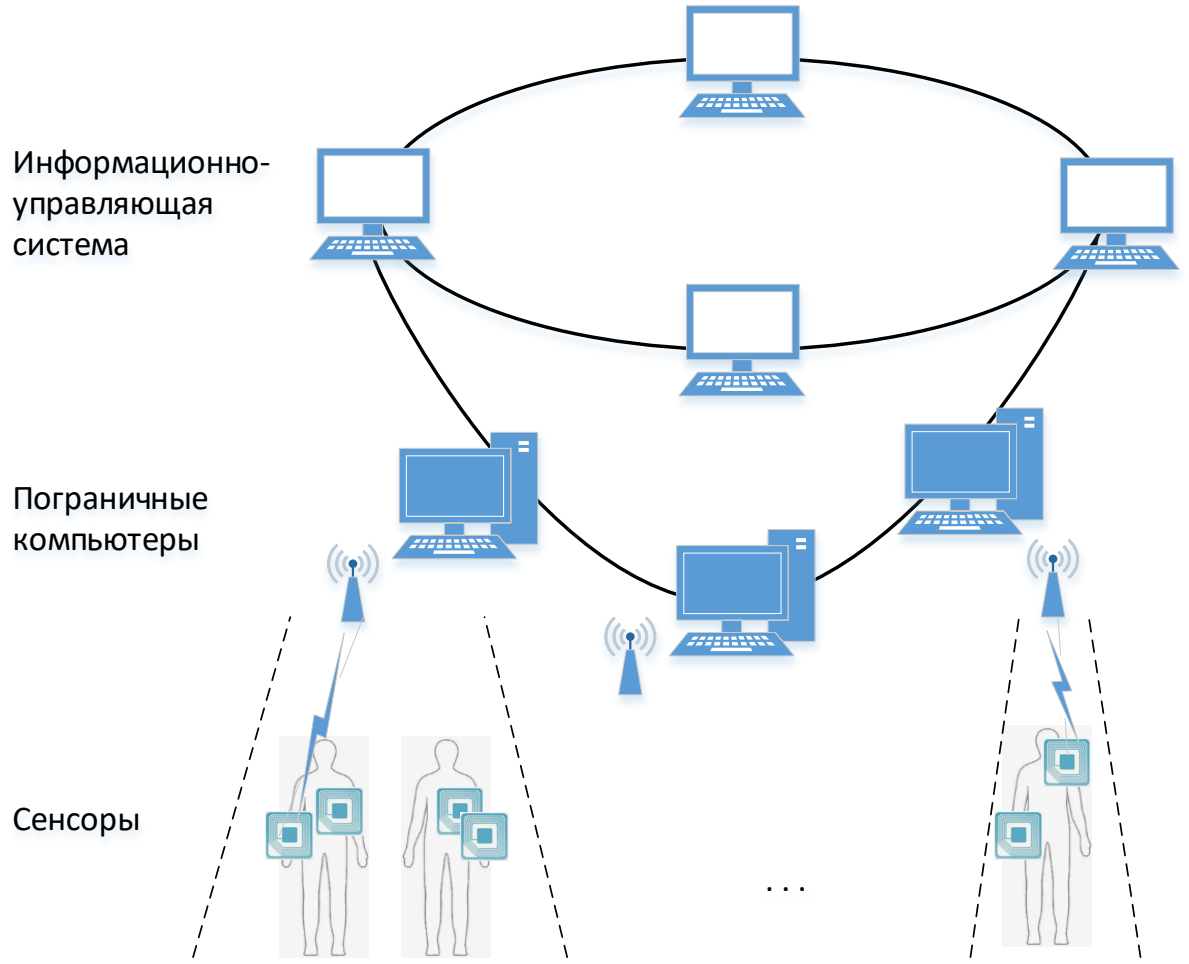
Основные проблемы применения блокчейна в IoT:

1 Высокая ресурсоемкость ряда применяемых в блокчейне механизмов, тогда как IoT-устройства (по крайней мере, расположенные на нижних уровнях IoT) обычно ограничены в ресурсах.

Решение: использование низкоресурсных блокчейнов (Lightweight blockchains, LWB).

2 Каждый сценарий использования блокчейна в IoT выдвигает собственные специфичные требования. *

3 Высокая степень гетерогенности в IoT. *



* A.Panarello et al. Blockchain and IoT Integration: A Systematic Survey. 2018.

Основные направления минимизации ресурсоемкости блокчейна

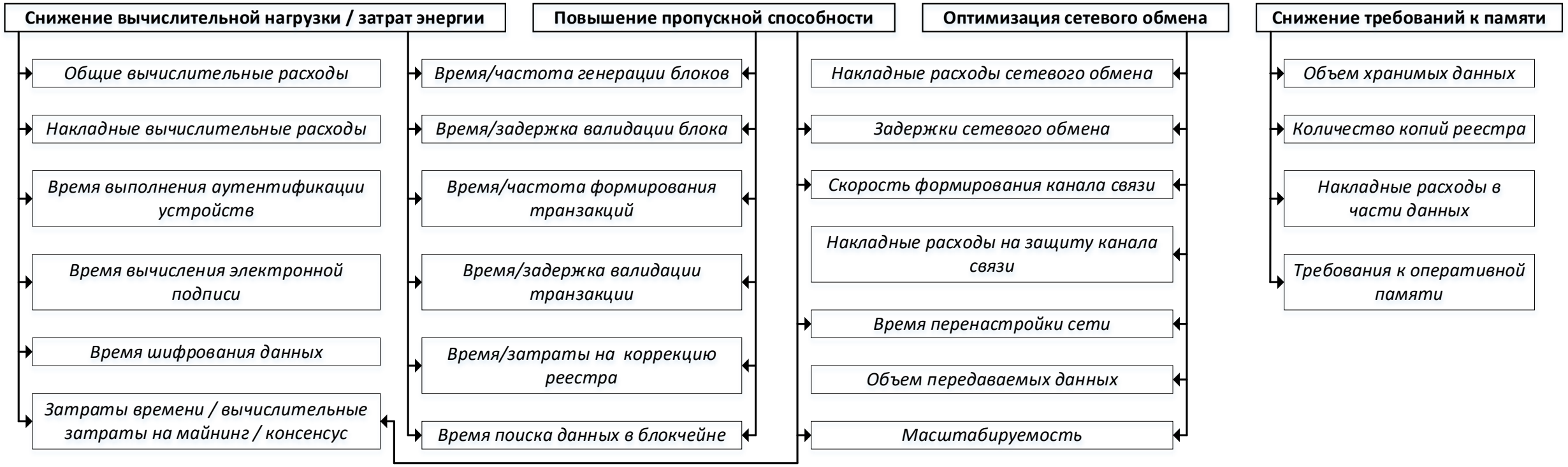
1. Проектирование системы с применением архитектурных решений, нацеленных на комплексное снижение общей ресурсоемкости блокчейна.
2. Использование низкоресурсных криптографических алгоритмов и/или снижение ресурсоемкости используемых криптографических алгоритмов.
3. Применение механизмов консенсуса с низкой ресурсоемкостью.
4. Минимизация требований к памяти, необходимой для хранения данных блокчейна.
5. Перенос ресурсоемких операций на верхние уровни IoT-систем.

Данные подходы часто комбинируются.

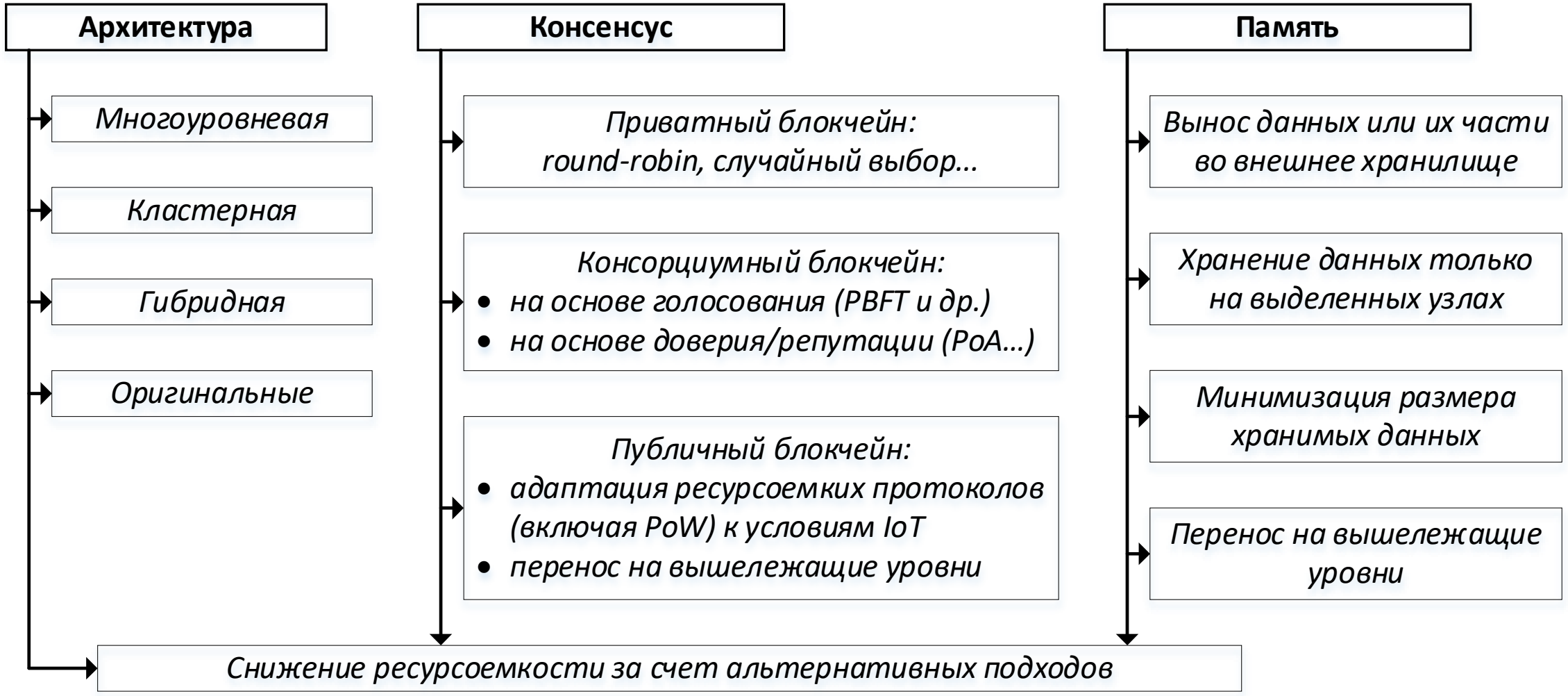
Достигаемые цели:

- снижение вычислительной нагрузки
- снижение сетевых задержек и накладных расходов
- снижение требований к памяти
- повышение пропускной способности
- снижение затрат энергии

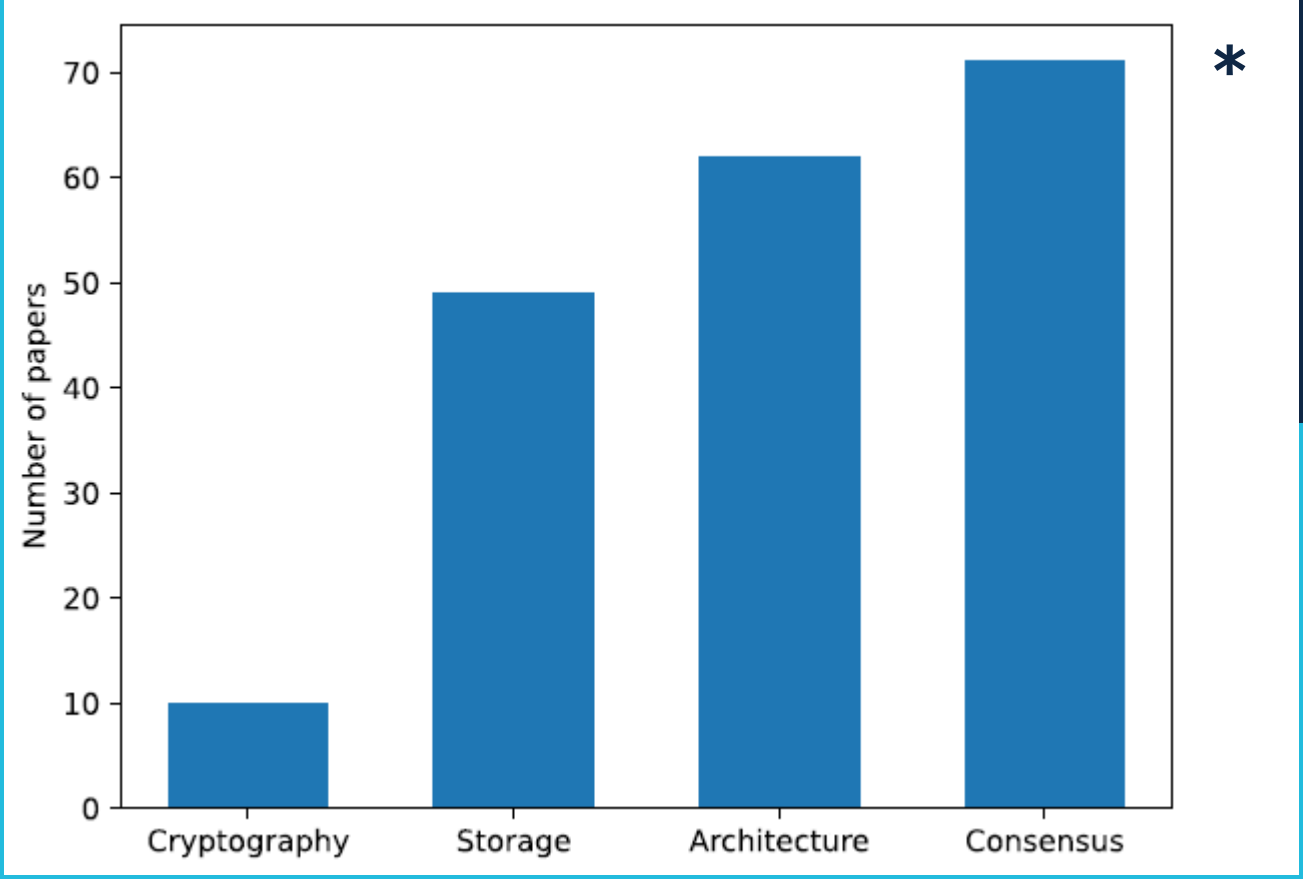
Метрики ресурсоемкости



«Некриптографические» подходы к снижению ресурсоемкости



Соотношение направлений снижения ресурсоемкости в известных работах



*

В большинстве случаев используется комплексный подход, включая варианты применения всех четырех направлений. *

* Рисунок из D.Stefanescu et al. A Systematic Literature Review of Lightweight Blockchain for IoT. 2022.

Пример гибридной архитектуры *

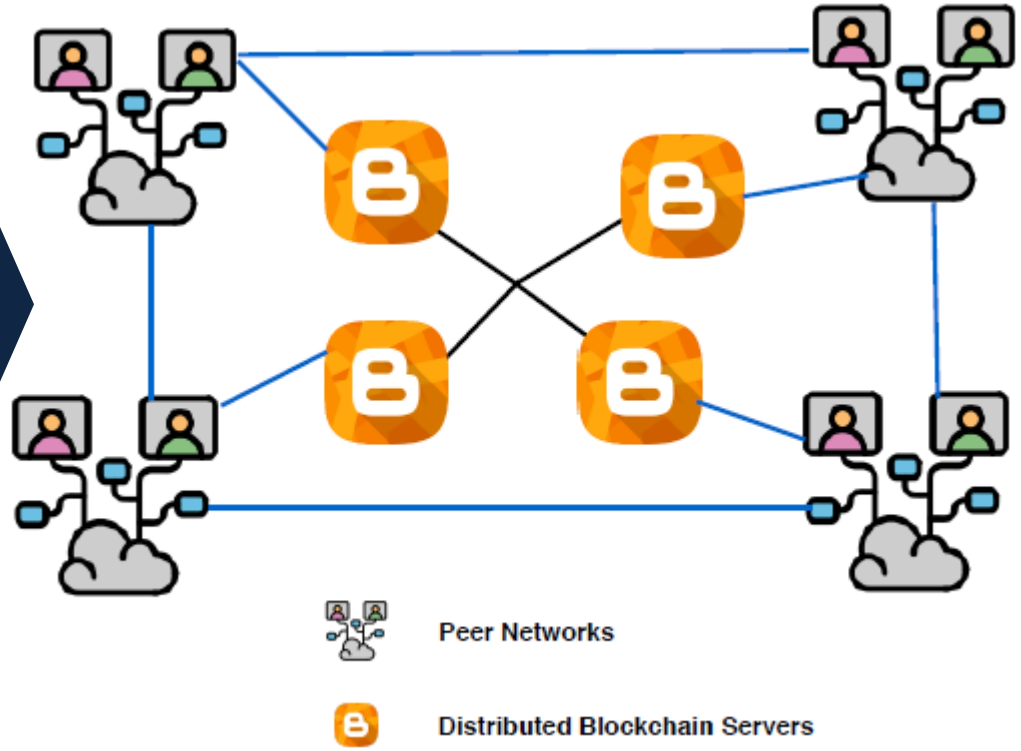
Основы подхода:

1. Двухуровневая кластерная структура консорциумного блокчейна с множественными вариантами доступа к блокчейну и с серверами-посредниками.
2. Консенсус (PBFT) используется только на уровне кластеров, раздельно для каждого кластера.

Основные результаты:

1. Высокая пропускная способность (скорость формирования и верификации транзакций и блоков).
2. Возможности масштабирования.

Изначально было предложено не для IoT-систем.

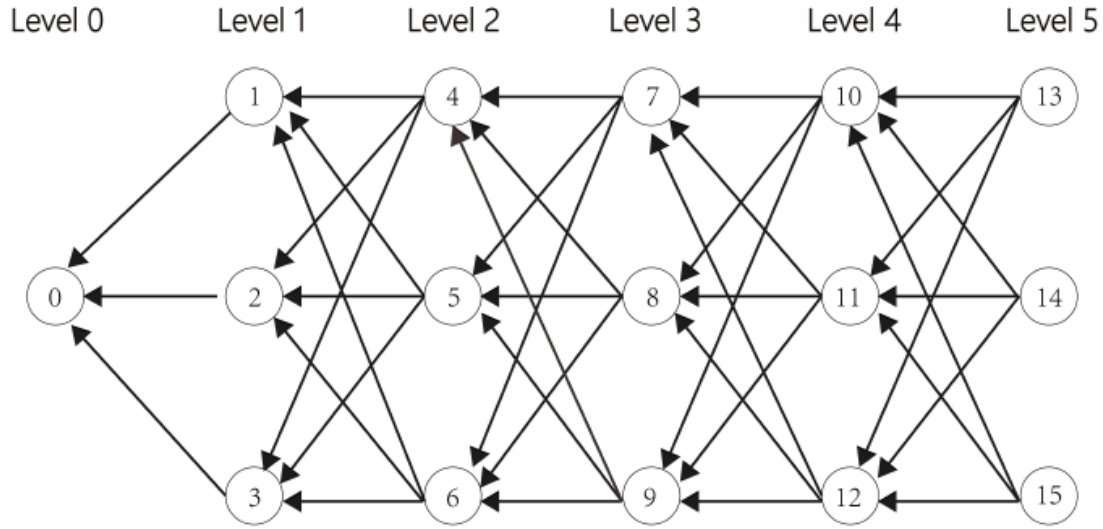


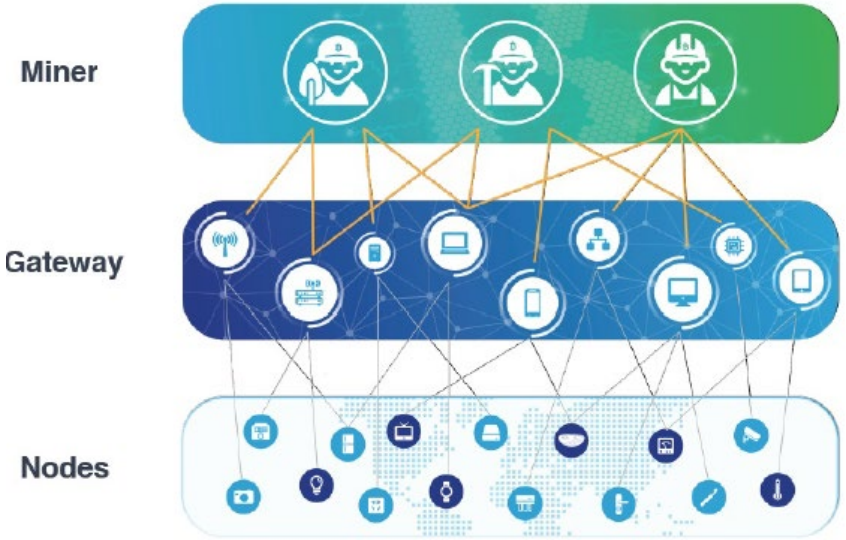
* A.Dwivedi et al. Tracing the Source of Fake News using a Scalable Blockchain Distributed Network. 2021.

Пример оригинальной архитектуры *

Основы подхода:

1 Структура на основе компактного направленного ациклического графа (CoDAG) — для публичных блокчейнов с PoW-консенсусом в IIoT-системах.





2 Разделение устройств по ролям в зависимости от ресурсов: майнер, шлюз, пассивный узел.

Основной результат:

Увеличенная пропускная способность при адекватном уровне безопасности.

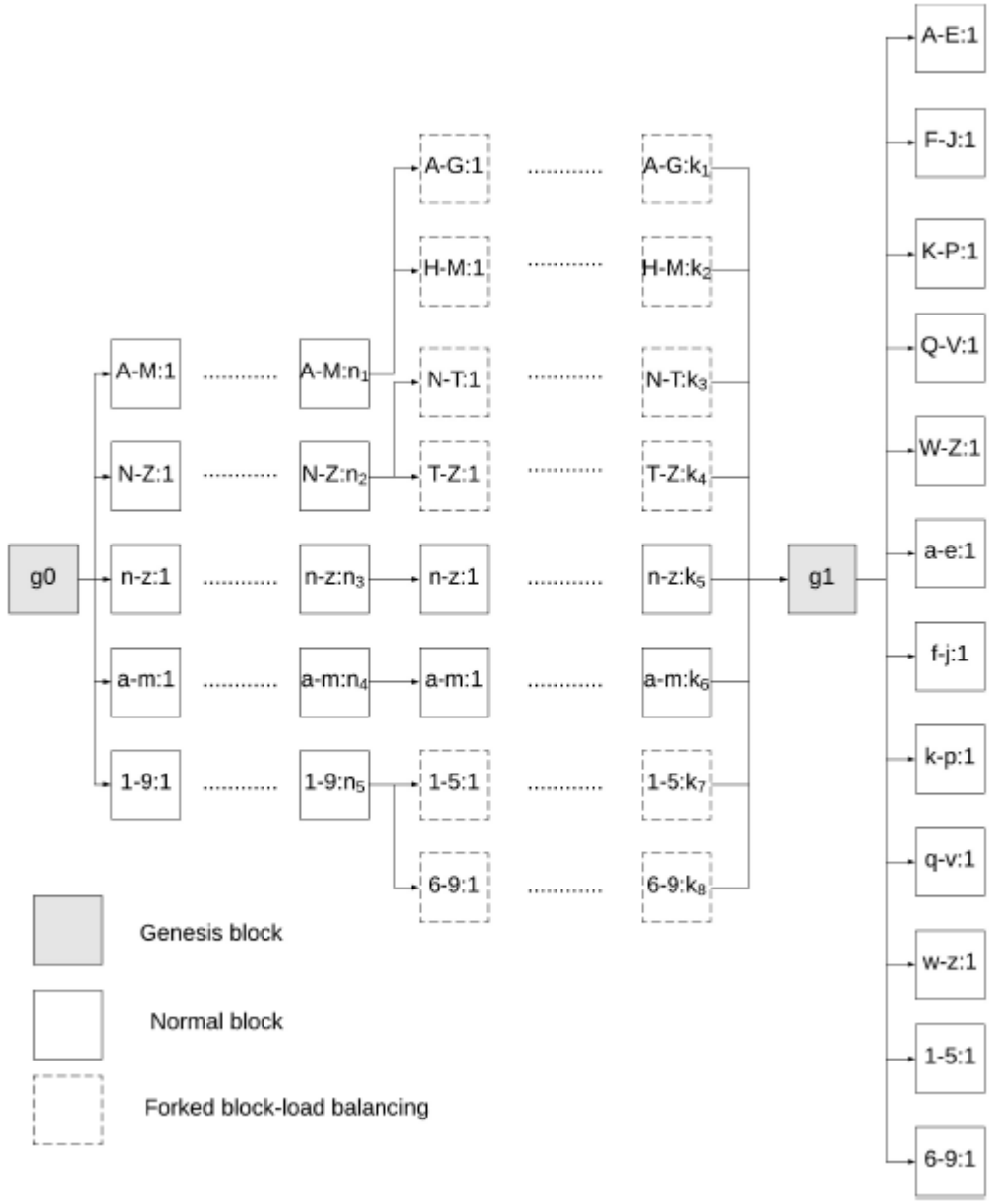
* L.Cui et al. An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things. 2020.

Пример протокола консенсуса *

Основы подхода:

1. Транзакции назначаются валидирующим узлам в зависимости от значения старшего байта хеш-кода транзакции, который сопоставляется с метрикой открытого ключа (Key Weight Metric – KWM) узла; после валидации транзакция (или несколько) сразу публикуется этим же узлом в новом блоке.
2. Периодически выполняется перегенерация ключей и обновление KWM.
3. Между обновлениями ключей каждый узел ведет свою цепочку блоков.

Основные результаты: минимальные затраты ресурсов на консенсус, увеличенная пропускная способность, минимальные задержки.



* A.Dorri, R.Jurdak. Tree-Chain: A Fast Lightweight Consensus Algorithm for IoT Applications. 2020.

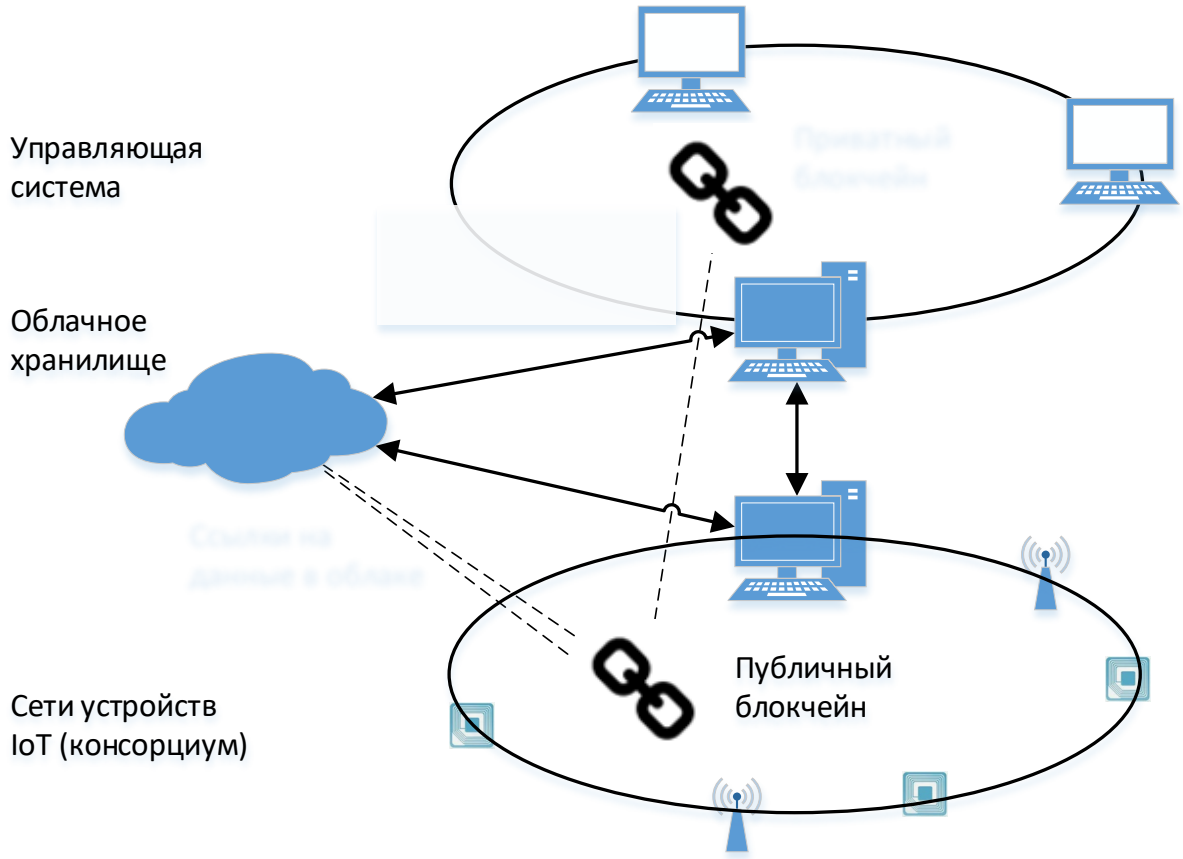
Пример переноса данных блокчейна в облако *

Основы подхода:

1 Данные IoT-системы хранятся в облаке.

2 Публичный блокчейн содержит только ссылки на хранящиеся в облаке данные и их хеш-коды.

3 Приватный (с шифрованием и ограниченным доступом) блокчейн содержит сопоставление реальных пользователей и их идентификаторов в публичном блокчейне, ведется на верхнем уровне.



Основные результаты:

- мин. затраты на хранение данных на уровне устройств с ограниченными ресурсами
- защищенное хранение критичных данных
- перенос ресурсоемких операций на верхние уровни IoT-системы

* K.Li et al. A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid. 2021.

Подходы к снижению ресурсоемкости в части криптографии

1. Использование низкоресурсных криптографических алгоритмов.
2. Отказ от ресурсоемких криптографических операций в пользу менее ресурсоемких.
3. Минимальная реализация криптографических алгоритмов общего назначения с оптимизацией под целевую платформу.
4. Упрощение и оптимизация операций генерации и распределения ключей.
5. Перенос криптографических операций (полностью или частично) на вышележащие уровни.

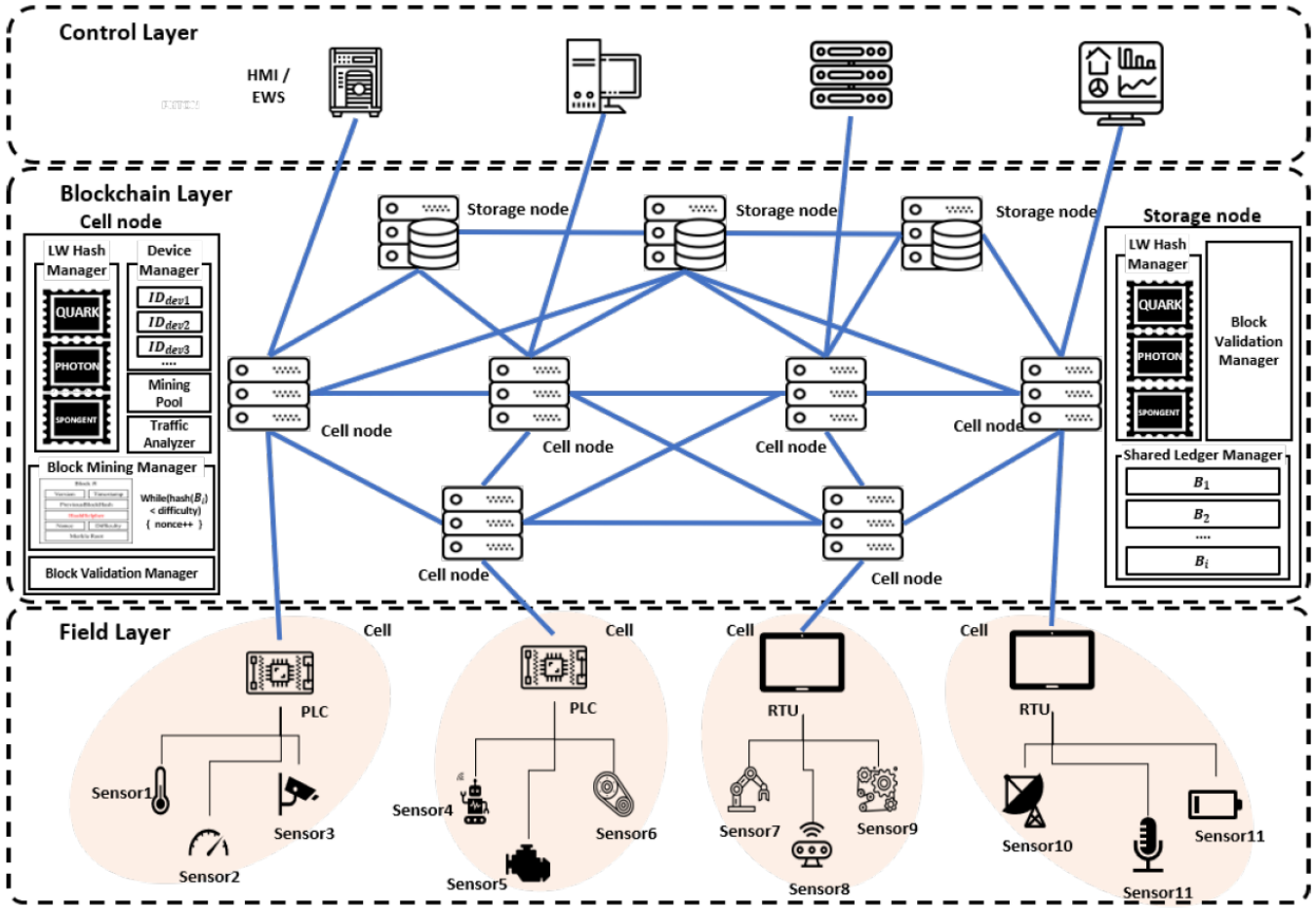
Использование низкоресурсных криптографических алгоритмов *

Основа подхода:

Применение низкоресурсных хеш-функций при хешировании данных блоков и транзакций (в т.ч. перед вычислением ЭП, применяются классические алгоритмы ЭП).

Основные результаты:

- снижение ресурсоемкости в части вычисления хеш-кодов
- снижение ресурсов IoT-устройств, требуемых на реализацию хеш-функции



* B.Seok et al. A Lightweight Hash-Based Blockchain Architecture for Industrial IoT. 2019.

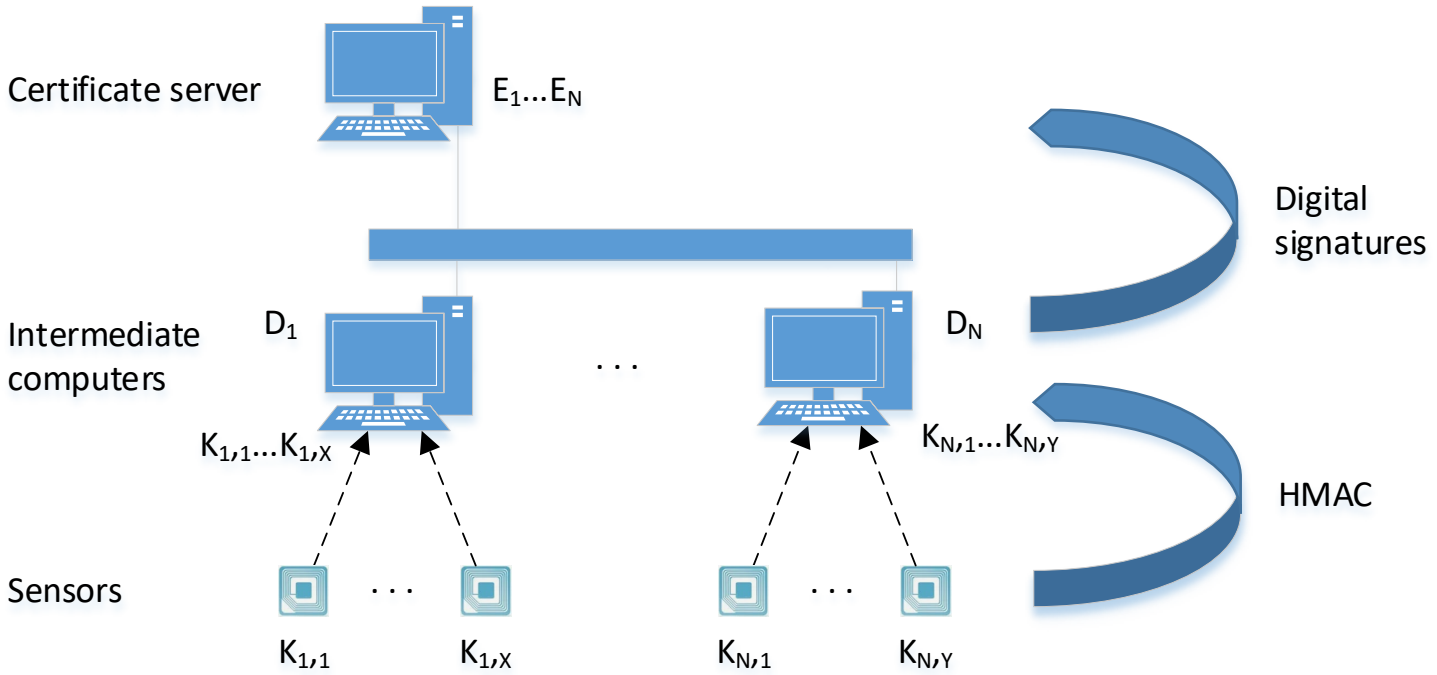
Использование менее ресурсоемких криптографических операций *

Основы подхода:

Использование HMAC вместо ЭП на уровне IoT-устройств (на уровне транзакций).

Основные результаты:

- снижение ресурсоемкости в части обеспечения целостности и аутентичности транзакций
- снижение ресурсов IoT-устройств, требуемых на реализацию криптоалгоритмов



* S.Panasenko. A Lightweight Blockchain for the Internet of Medical Things Using Hash-based Message Authentication Codes. 2023.

Минимальная реализация криптоалгоритмов с оптимизацией под целевую платформу *

Основы подхода:

- реализация только используемых вариантов / режимов работы криптоалгоритмов
- оптимизация под целевую платформу применяемых IoT-устройств с целью минимизации затрат времени на вычисления с учетом существующих вычислительных ресурсов

Используемые криптоалгоритмы:

- EC-ElGamal (шифрование на уровне транзакций)
- SHA-384 (ключевое хеширование на уровне блоков)

Основные результаты:

- снижение ресурсоемкости выполнения криптографических операций
- повышение пропускной способности

* J.Guruprakash, S.Koppu. EC-ElGamal and Genetic Algorithm-Based Enhancement for Lightweight Scalable Blockchain in IoT Domain. 2020.

Упрощение и оптимизация процедур генерации и распределения ключей *

Основы подхода:

Уход от использования классических схем ЭП и сертификатов открытых ключей за счет применения ID-based cryptography с использованием в качестве идентификаторов серийных номеров IoT-устройств.

Основные результаты:

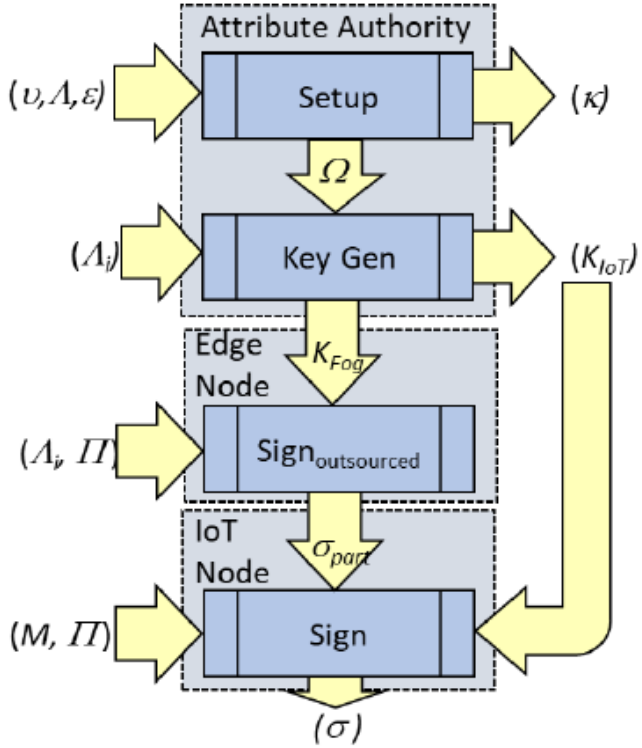
- упрощение процедур генерации и распределения ключей
- отсутствие необходимости проверки цепочек сертификатов
- уменьшение размеров ключей

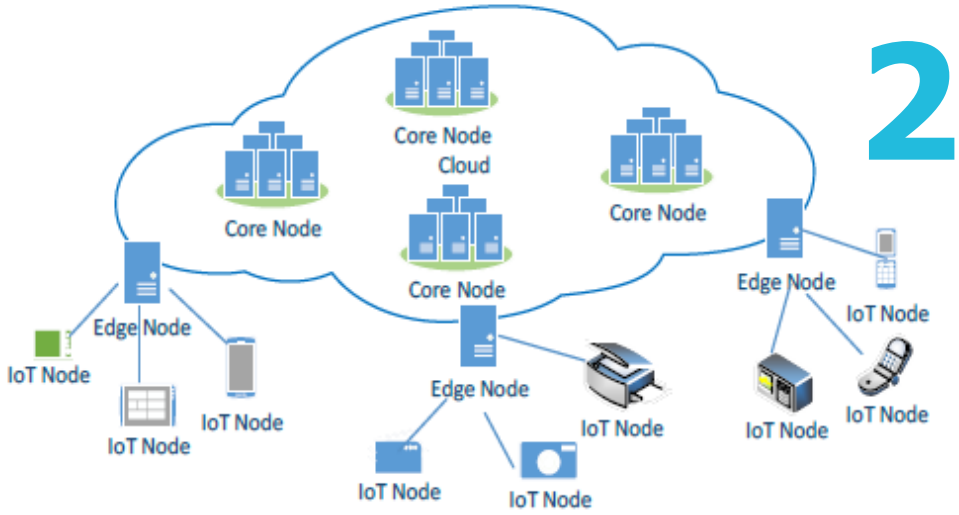
* S.Mohanty et al. An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. 2020.

Перенос ресурсоемкой части вычислений на верхние уровни *

Основы подхода:

1 Процесс вычисления аналога подписи данных (вместо ЭП используется Attribute-Based Encryption) распределен между IoT-устройством и ассоциированным с ним пограничным узлом, при этом основные вычисления выполняются пограничным узлом.





2 Проверка подписей выполняется только на верхних уровнях.

Основной результат:

- высокая пропускная способность
- минимальные затраты ресурсов IoT-устройств на подтверждение целостности и аутентичности транзакций

* M.Siddiqui et al. BlockTrack-L: A Lightweight Blockchain-based Provenance Message Tracking in IoT. 2020.

Заключение

1 Существует множество подходов по адаптации блокчейн-технологий для применения в IoT, в том числе в IoT-устройствах с незначительными ресурсами.

2 В части криптографических механизмов авторы различных подходов пытаются найти баланс между ресурсоемкостью / пропускной способностью блокчейна и качеством обеспечения криптографической защиты информации.

«'Lightweight blockchain'... is a relatively new concept that does not have a standard and universal definition yet.» *

* D.Stefanescu et al. A Systematic Literature Review of Lightweight Blockchain for IoT. 2022.

конференция РусКрипто

30 КОМПАНИЯ АКТИВ

hh

Вопросы?

Сергей Панасенко,
компания «Актив»
panasenko@guardant.ru


30
КОМПАНИЯ
АКТИВ