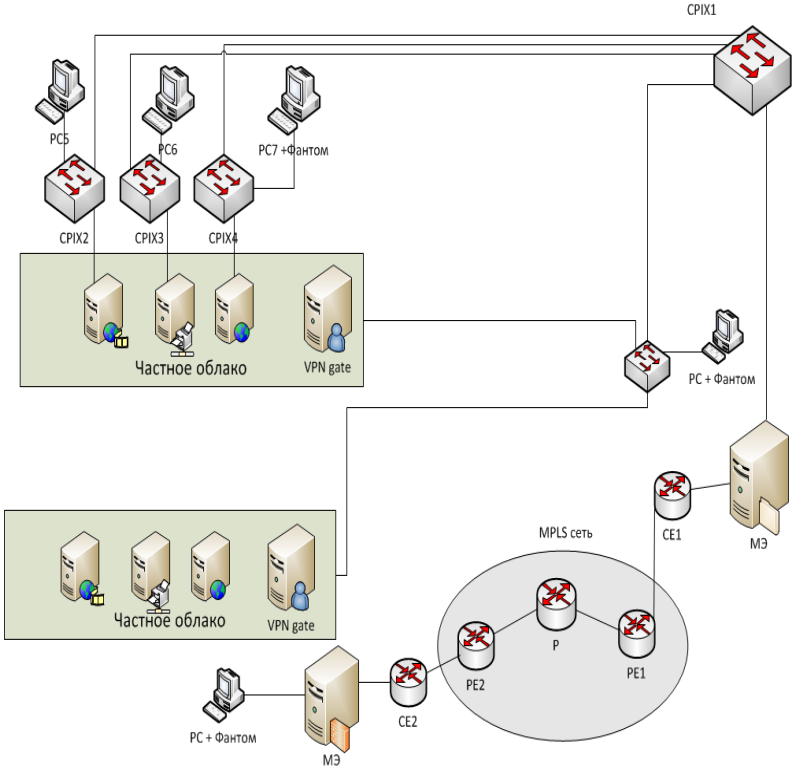
Работа с распределенным реестром в СПОД. Прогнозирование временных характеристик прикладных сетевых сервисов
21 марта 2023

Писковский Виктор Олегович

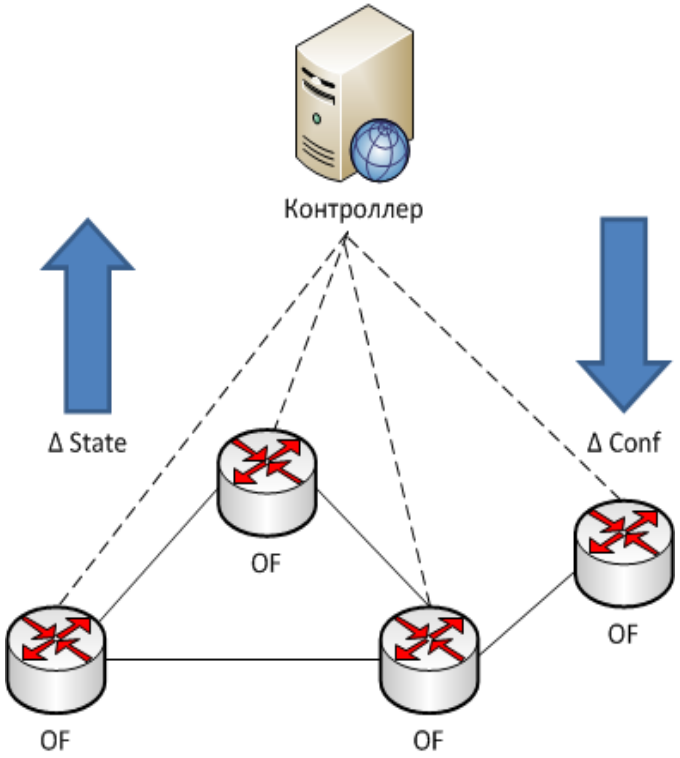
Традиционная сеть,ПКС и распределенный реестр

Традиционная сеть и ПКС

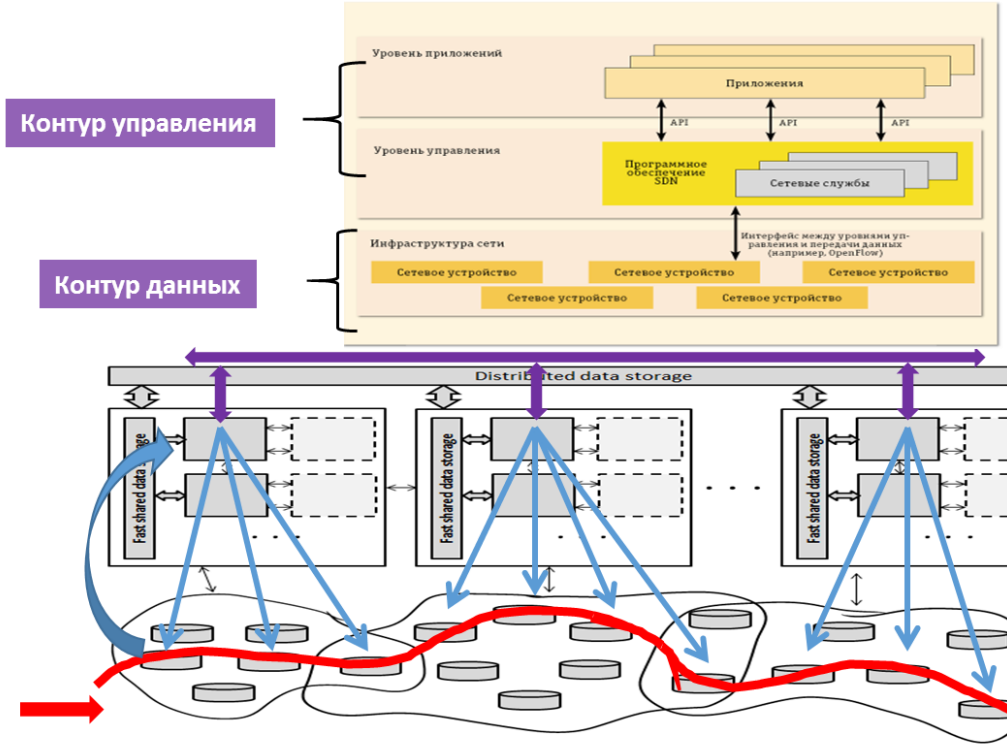
Традиционная сеть

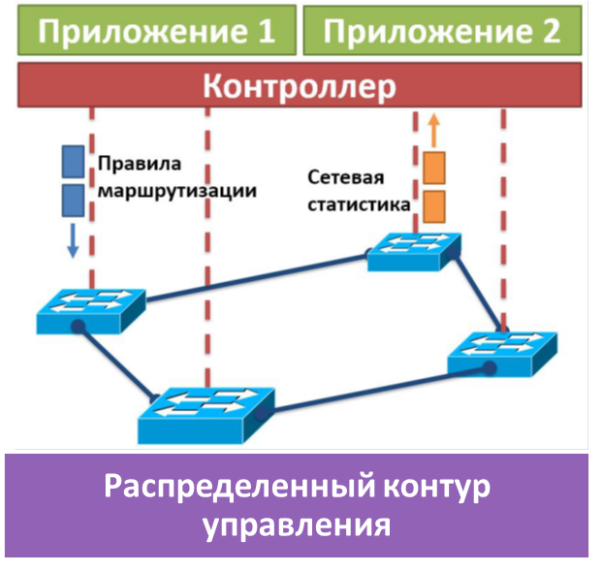


Программно-конфигурируемая сеть



Архитектура ПКС сети





- Надежность и отказоустойчивость (резервирование внутри кластера и между кластерами)
- Балансировка нагрузки (активизация новых узлов контроллера в зависимости от нагрузки)
- Согласованное управление и видение всей сети
- Работа с распределенными сетевыми приложениями
- Безопасность и противодействие внешним нагрузкам

Внесение изменений в продукционную ИТ-инфраструктуру предприятия

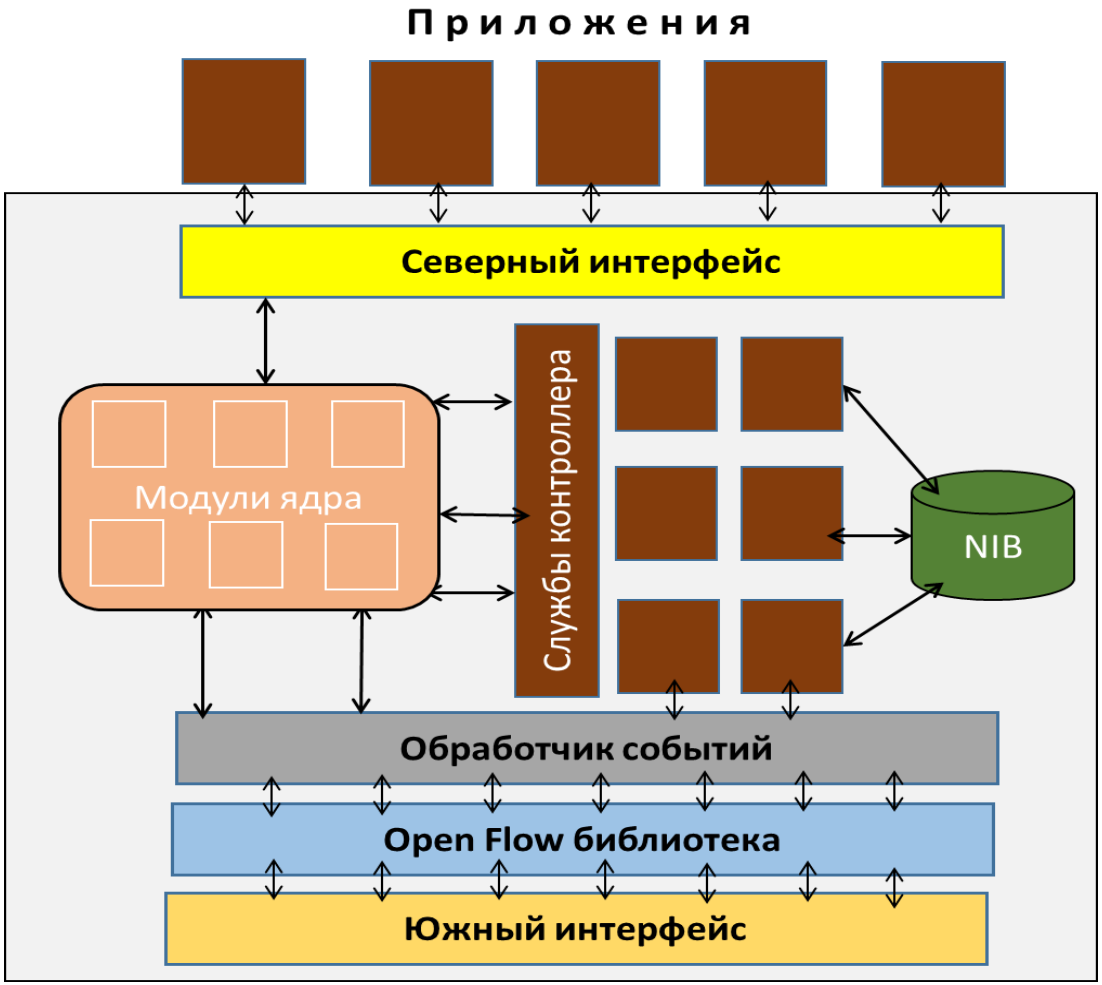
Традиционная сеть

- Длительное документальное согласование схем коммутации
- «Ручная» конфигурация сети, потоков, сетевых устройств на основе документально согласованных схем

Программно-конфигурируемая сеть

- Наличие предварительно разработанных и отлаженных приложений управления сетью передачи данных
- Автоматизированная конфигурация сети контроллером на основе пользовательских запросов при помощи указанных приложений управления сетью в соответствии с принятыми политиками безопасности
- Применение методов машинного обучения при управлении конфигурацией сети

Постановка задачи



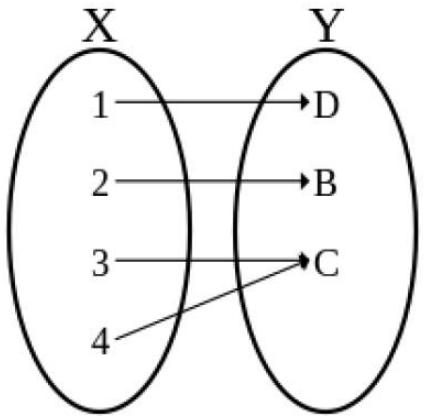
NIB: Redis -> DLT (TenderMint)

Требования к системе

- Децентрализация хранения и учета
- Невозможность локального контроля
- Корректность и устойчивость
- Производительность
- Простой аудит

Hash функция

1. *Сюръективность*
2. *Простота и высокая скорость прямого вычисления функции*
3. *NP-сложность нахождения прообраза по значению функции*
4. *Лавинный критерий («Strict Avalanche Criterion»)*
5. *Стойкость к коллизиям*
6. *Псевдослучайность*

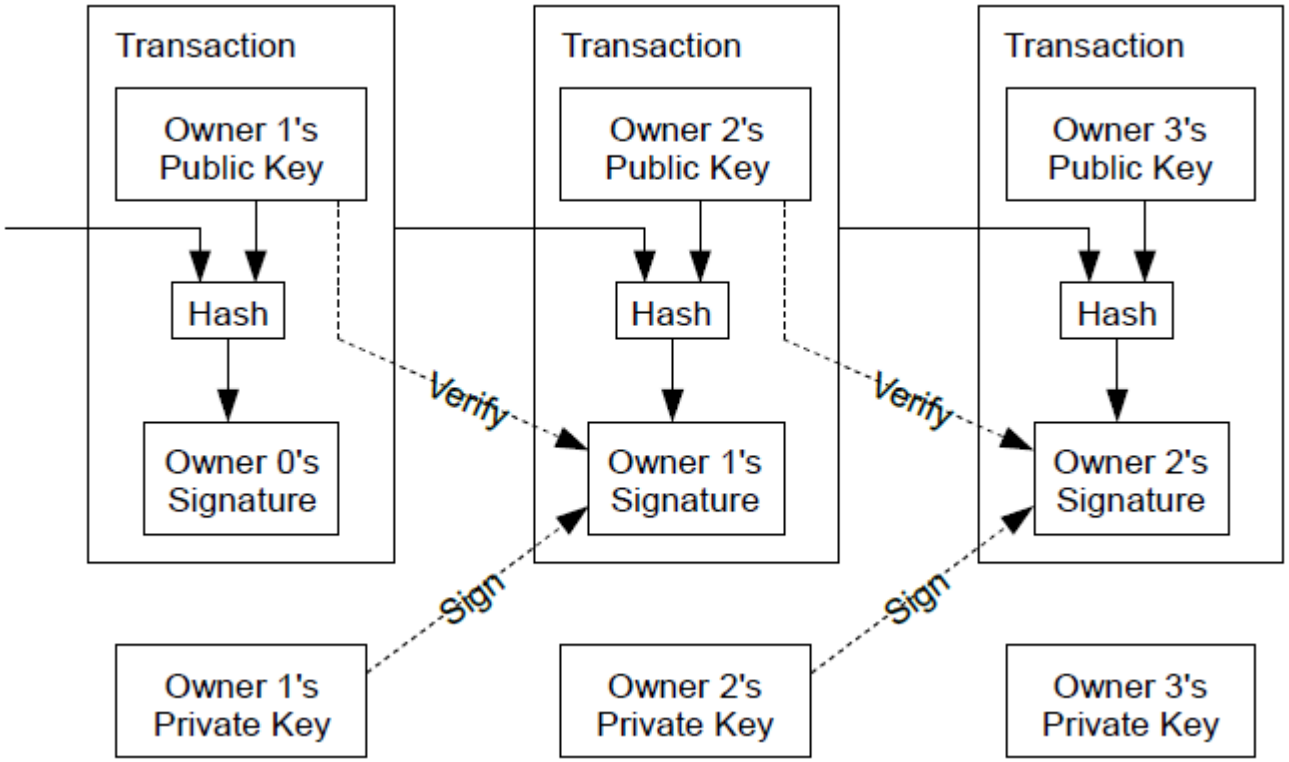


Сюръективная функция

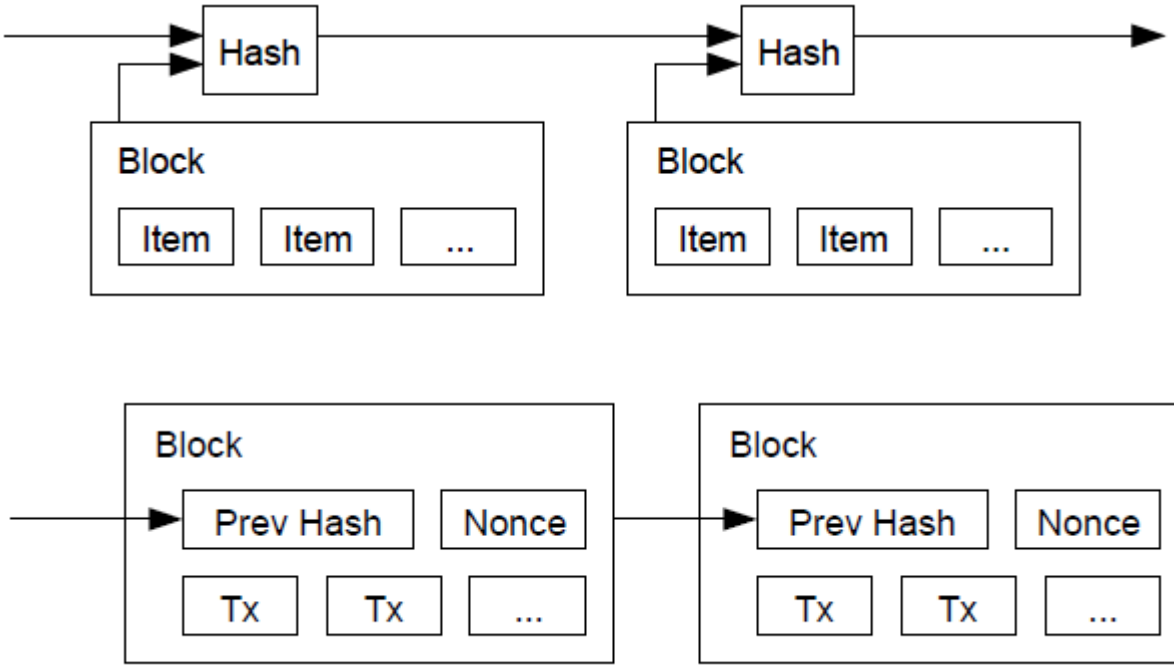
История вопроса

Bitcoin: A Peer-to-Peer Electronic Cash System

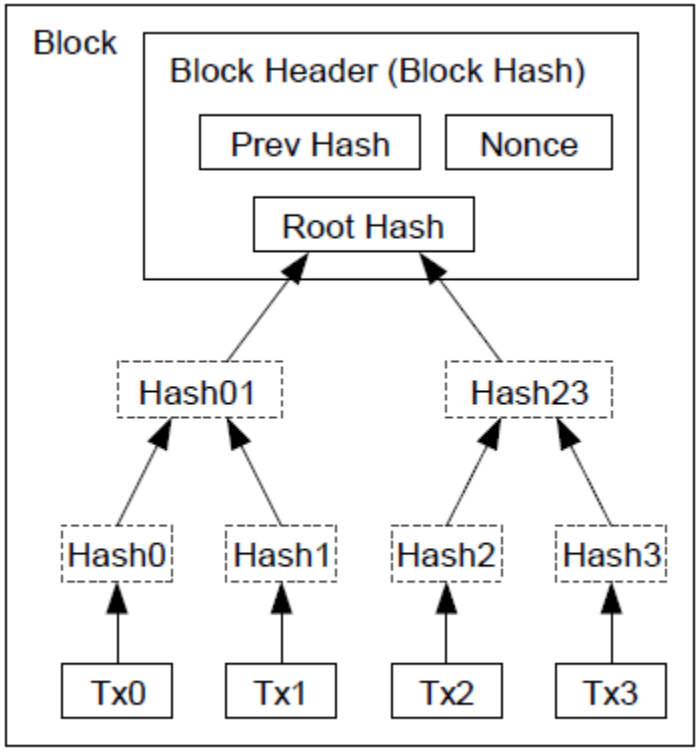
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



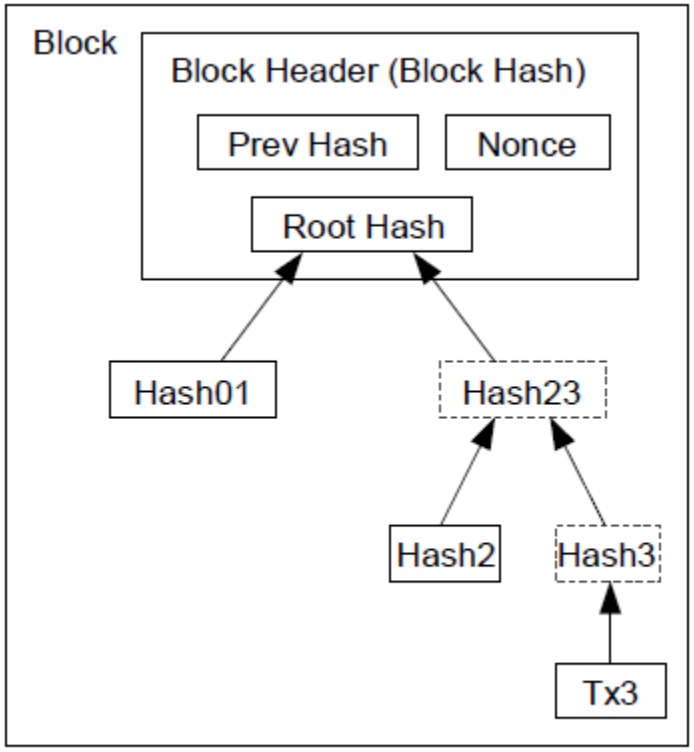
История вопроса



История вопроса

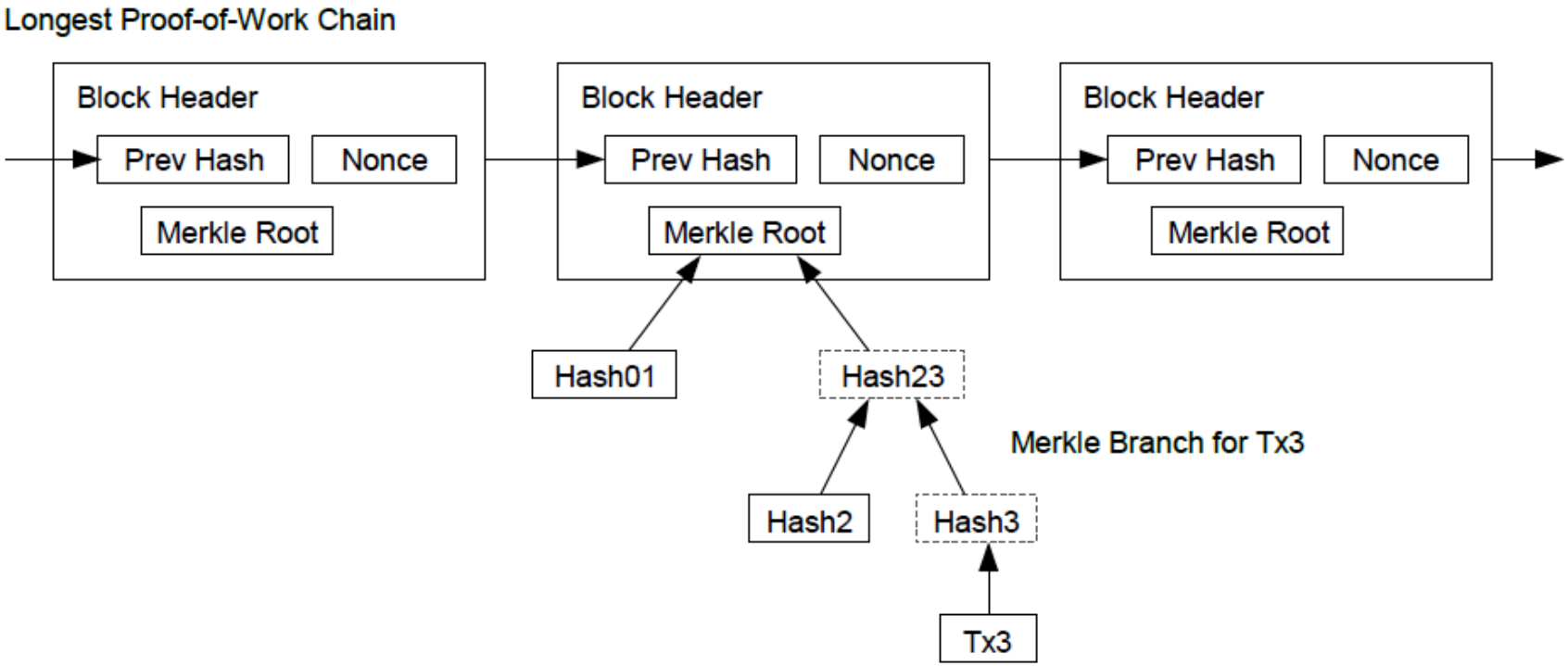


Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

История вопроса

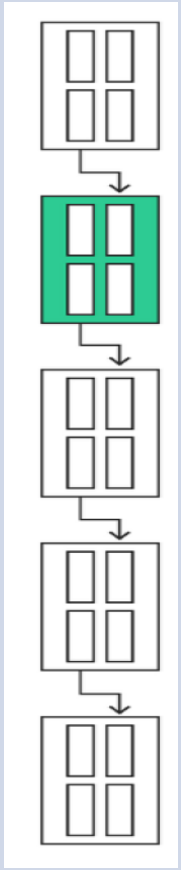
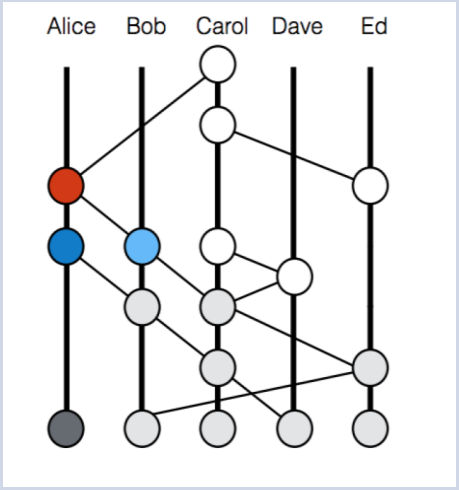
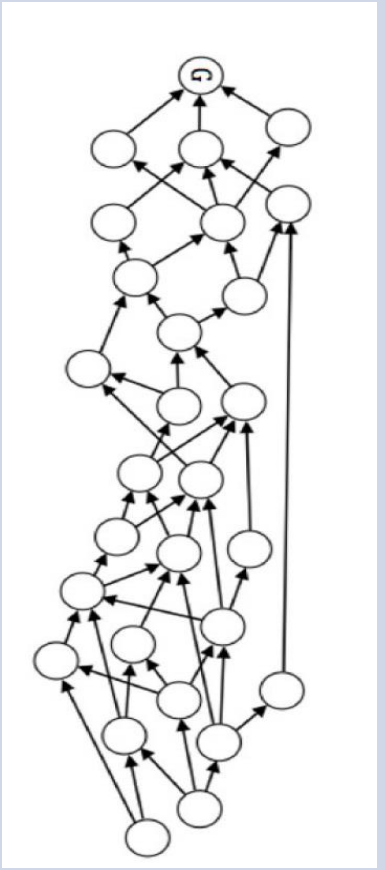


Распределенные реестры

№	Модель DLT	Протокол достижения консенсуса	Производительность (TPS)	Примечание
1	BlockChain	Proof of Work (PoW)	10	Регулируется соглашением
2		Proof of Storage (PoSt)	100-200	
3		Proof of Stake (PoS)	100-200	
4		Byzantine Fault Tolerance (BFT)	1 тыс	Отдельные решения до 1 млн
5	HashGraph	Asynchronous BFT (ABFT)	250 - 350 тыс.	SWIFT-VISA (50 тыс. TPS)
6	DAG	BlockDAG/TxDAG	> 1 млн	
7	Holochain	Proof-of-Service	неограничена	Ceptr, LLC Определение распределенных систем

https://holochain.org
https://hbarprice.com/hashgraph-vs-holochain/
https://ceptr.org

Распределенные реестры

Blockchain	Hashgraph	DAG
		

https://cryptor.net/kriptovalyuty/different-types-of-dlts

Консенсус

Название	Описание	Применение	Произв.
Доказательство работы (Nakamoto consensus)	Необходимо обеспечить наличие большого количества вычислительных ресурсов с соответствующим энергопотреблением для выполнения требований получению блока, регулируется требованием к значению hash-функции. Цель использования таких требований, существенно замедляющих появление новых блоков – синхронизация новых блоков между узлами одноранговой сети	BitCoin, Ehtereum, Litecoin	10 TPS

Примечание:
Прототип – Hashcache, защита от спама

Консенсус

Название	Описание	Применение	Произв.
Proof-of-Stake (PoS — Доказательство доли, владения) Proof of Stake Time (PoST)	Учитывается количество монет, депонируемых за возможность создавать блоки, как гарантия "честности" узла. После создания блока депозит возвращается владельцу	Peercoin, Tezos, PayCoin, Blackcoin, Nxt, Clobal.	150 TPS
Delegated Proof-of-Stake (DPoS) (Делегированное доказательство доли)	Узлы с большим количеством токенов выбирают узлы для проверки транзакций и создания блока для цепи. Каждый из выборанных узлов по круг (RoundRobin) собирают и подписывают блоки.	EOS, BitShares, Lisk, Ark, Steem	
Proof of Authority (POA)	Авторизованные узлы создают блоки для цепи. Каждый из авторизованных узлов может образовывать блоки.		
Ouroboros PoS	Узлы с большим количеством токенов (выборщики) назначают лидеров на несколько раундов создания блоков, блоки создаются лидером по одному в определенный для этого лидера период времени.	Ada	
Leased Proof of Stake (LPoS)	Тоже, что DPoS, но можно брать монеты в лизинг и тем самым пользоваться привилегией выбирать узлы для проверки	Waves	

Cosmos

- Cosmos SDK - платформа с открытым исходным кодом, 200 проектов
- Консенсус:
  - BFT (Byzantine Fault Tolerance – задача византийских генералов)
  - PoS (Proof of Stake - подтверждение наличия доли),
  - PoA (Proof of Authority - подтверждением полномочий)
  - протокол «слухов» (gossip)
- Cosmos Hub основана в 2019 г., капитализация $8 млрд

The design, architecture and performance of the Tendermint Blockchain Network

Daniel Cason
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland

Enrique Fynn
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland

Nenad Milosevic
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland

Zarko Milosevic
Informal Systems
Toronto, Canada

Ethan Buchman
Informal Systems
Toronto, Canada

Fernando Pedone
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland

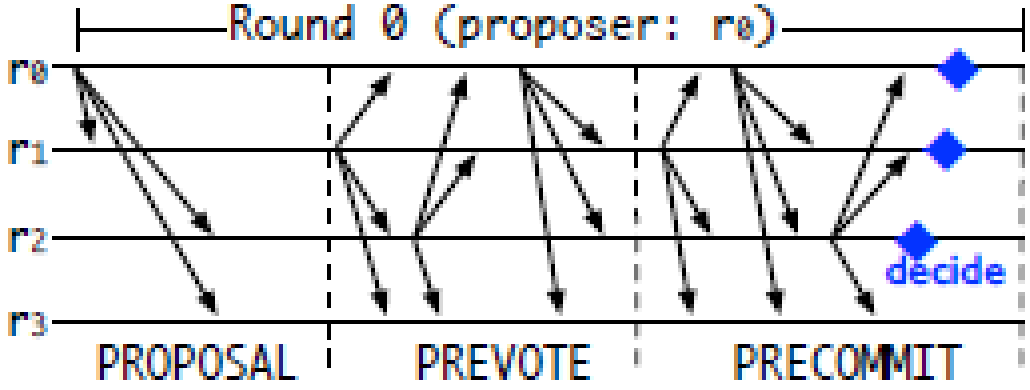
Особенности Cosmos SDK

Поддержка работы многочисленных распределённых приложений в недоверенном окружении на основе технологии распределенного реестра (PP)

Цели:

- Гибкость
- Масштабируемость
- Отказоустойчивость работы в недоверенном окружении (BFT)
- Независимость от языка программирования
- Простые клиентские места не требуют ресурсы для размещения и обработки всей цепочки блоков, RPC

Tendermint. Протокол слухов



Протокол достижения консенсуса (протокол слухов/сплетен – gossip)

Эксперименты

- Все клиенты – на одном сервере
- Клиенты создавали транзакции по 1 Кб равномерно в цикле, то есть клиент подавал транзакцию на заданный валидатор, ждал её включения в блок и подавал новую на тот же валидатор
- Версии ПО: Tendermint version 0.33.8 and Go version 1.15.
- mempool объёмом до 1Гб для 5000 транзакций в блоках по 20 Мб
- Интервалы в работе протокола слухов 100 мс, скорости до 5000 Кб/с

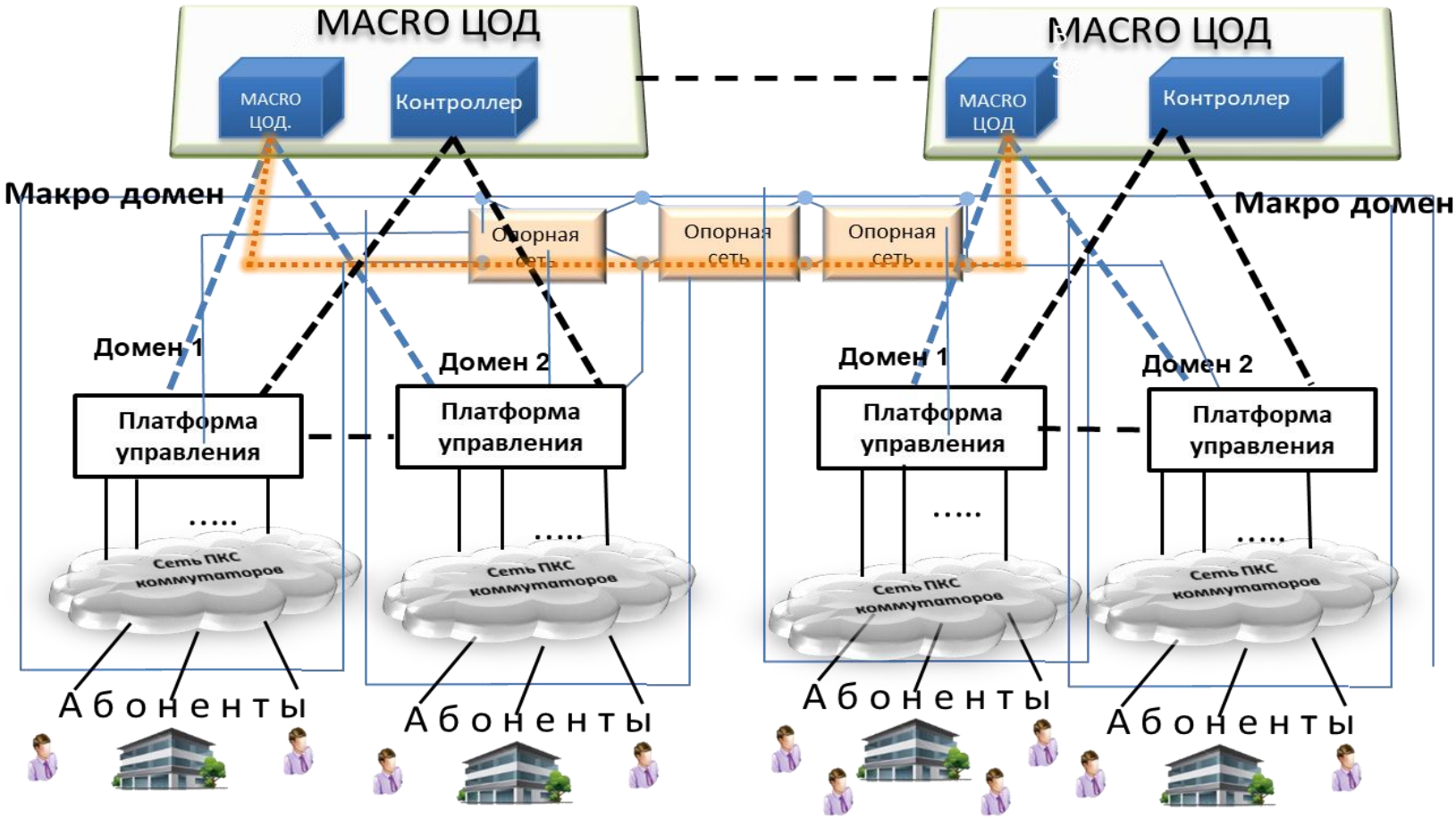
Результаты

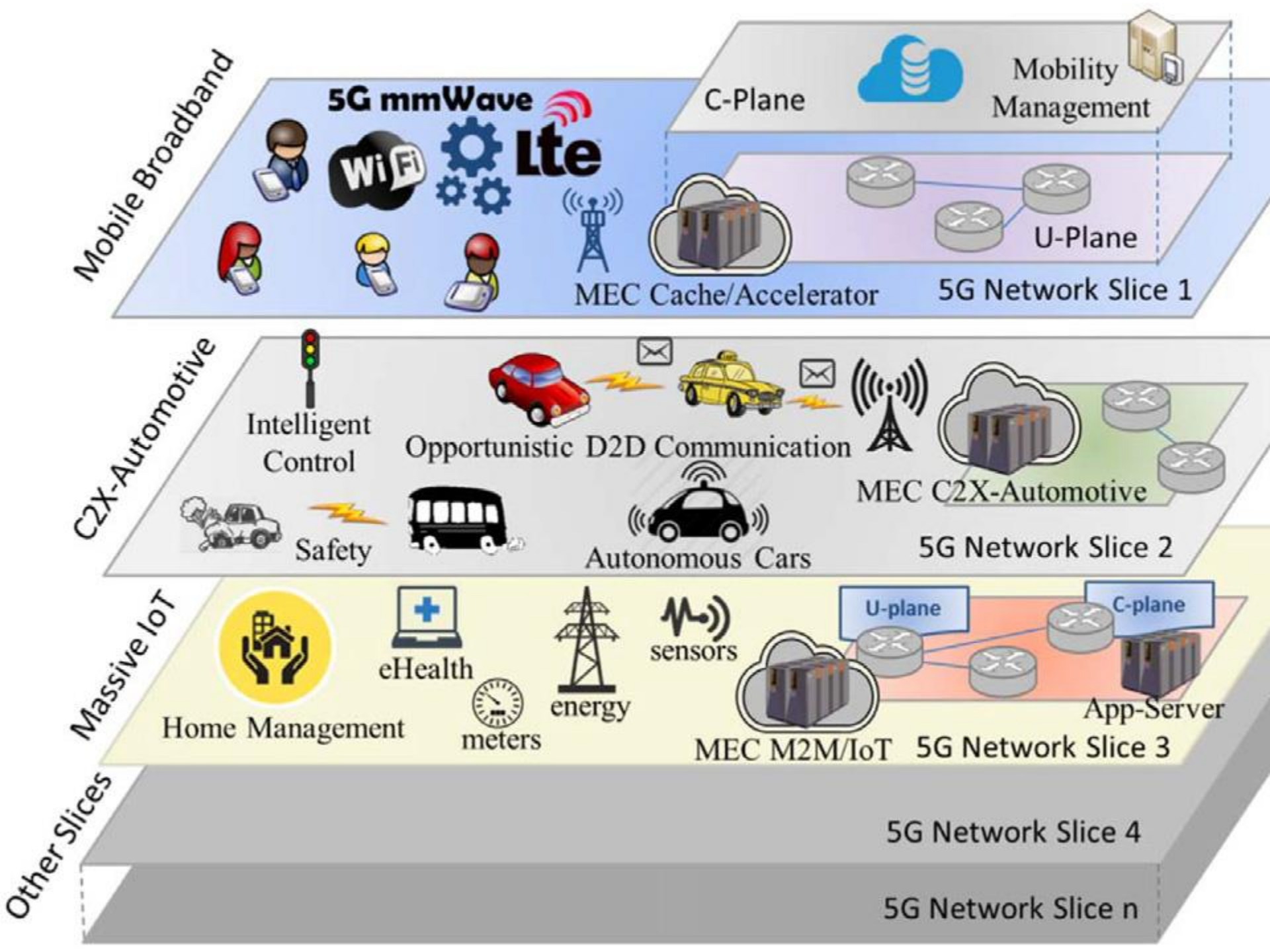
- Оптимальная нагрузка для 128 валидаторов: по 12 клиентов на валидатор (1536 клиентов)
- Регистрация блока в среднем за 2.53 с (96%: 2.3 с – 2.7 с)
- Регистрация транзакции: 40% - от 2 с до 3 с, 40% - 4.5 с, или порядка 400 тр/с
- Отказоустойчивость при отключении 1/3 валидаторов: время создания блоков на работающих валидаторов не изменилось, поданные транзакции на отключенные валидаторы потребовали в среднем в два раза больше времени, в среднем деградация 25%

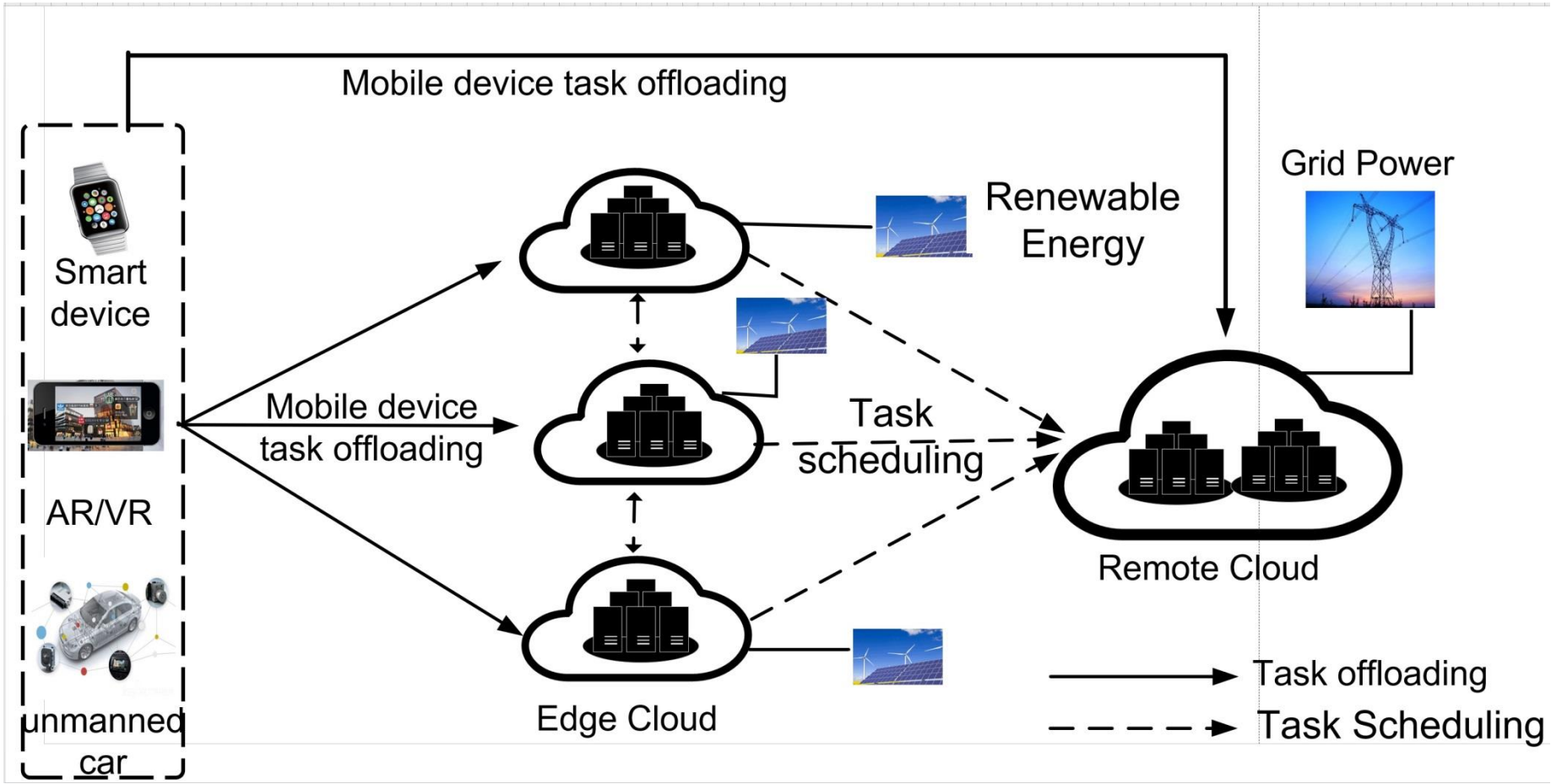
Направление работы

- Оптимизация выбора валидатора
- Интеграция с RunOS
- Испытания

Прогнозирование временных характеристик прикладных сетевых сервисов


MACRO ЦОД
MACRO ЦОД.
Контроллер
MACRO ЦОД
Контроллер
Макро домен
Макро домен
Опорная сеть
Опорная сеть
Опорная сеть
Домен 1
Домен 2
Домен 1
Домен 2
Платформа управления
Платформа управления
Платформа управления
Платформа управления
Сеть ПКС коммутаторов
Сеть ПКС коммутаторов
Сеть ПКС коммутаторов
Сеть ПКС коммутаторов
А б о н е н т ы
А б о н е н т ы
А б о н е н т ы
А б о н е н т ы


Mobile Broadband
5G mmWave
Wi Fi
Lte
C-Plane
Mobility Management
U-Plane
MEC Cache/Accelerator
5G Network Slice 1
C2X-Automotive
Intelligent Control
Opportunistic D2D Communication
MEC C2X-Automotive
Safety
Autonomous Cars
5G Network Slice 2
Massive IoT
eHealth
sensors
energy
meters
Home Management
U-plane
C-plane
App-Server
MEC M2M/IoT
5G Network Slice 3
Other Slices
5G Network Slice 4
5G Network Slice n


Mobile device task offloading
Smart device
AR/VR
unmanned car
Mobile device task offloading
Renewable Energy
Grid Power
Task scheduling
Remote Cloud
Edge Cloud
Task offloading
Task Scheduling

Цель

Прогноз времени выполнения на программ на периферийном оборудовании (Edge Cloud Computer nodes = ECC) по имеющимся зарегистрированным данным

План работы

1. Разработка математической модели
2. Применение методов машинного обучения для прогнозирования времени выполнения заданий и энергопотребления
3. Разработка математической постановки задачи оптимального распределения заданий в среде E3C2 на основе мультиагентных методов оптимизации с обучением и прогнозированием времени их выполнения и энергопотребления
4. Разработка методик оценки возобновляемых источников электроэнергии, необходимой для обеспечения бесперебойного питания cloud edge
5. Разработка методов прогнозирования времени выполнения сервиса и затрат энергии