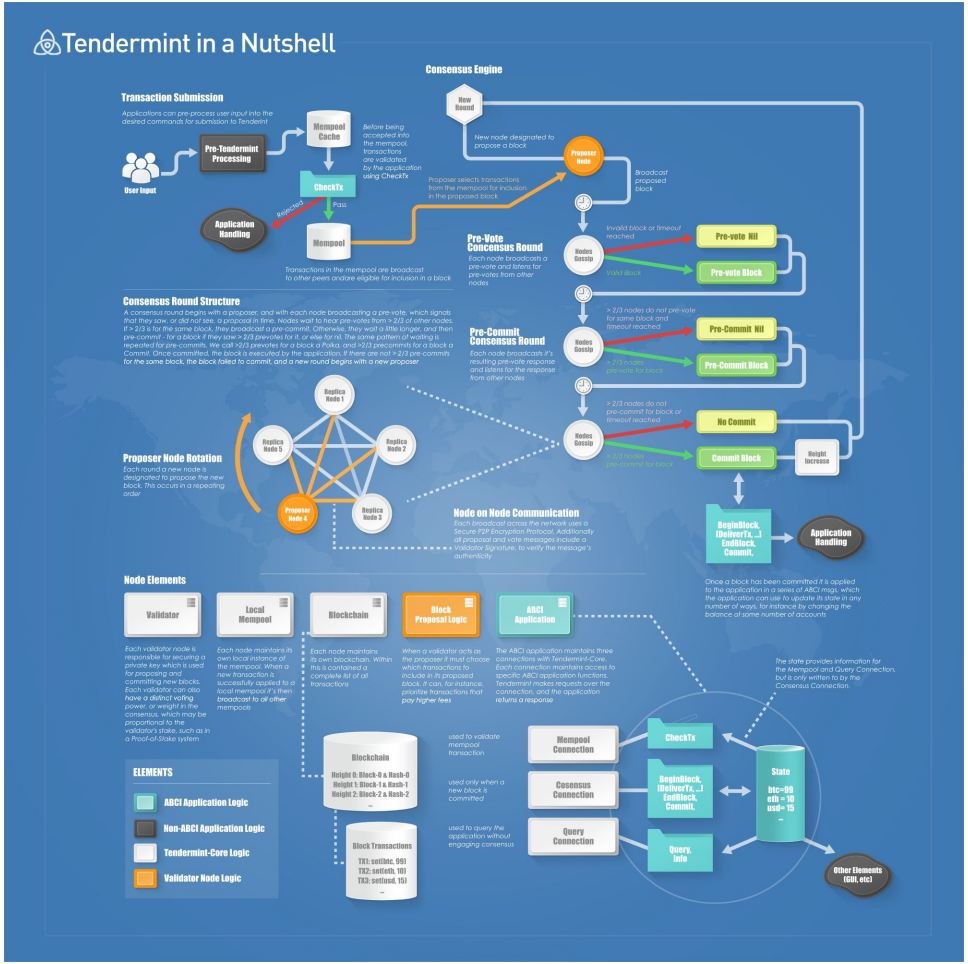
Микро-фреймворк Tendermint

А также протокол ABCI, и перспективы его использования для создания Распределённого Реестра Данных РЖД

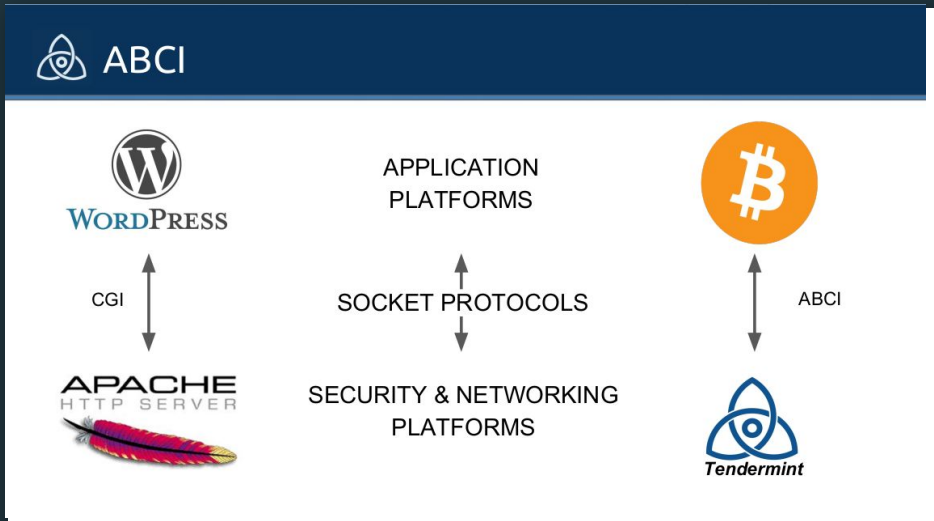
Блокчейн – это просто! :-)

- Распределённая СУБД с репликацией vs **Blockchain**
- База данных “ключ-значение” (напр. LevelDB)
- Hash-функции
- Криптография Эллиптических Кривых ECDSA
- Граф транзакций
- Состояние (напр., балансы)



Tendermint – это:

- Комплект программ на языке Go
- Алгоритм консенсуса à la PBFT и P2P протокол Gossip, выделенные в отдельную сущность: Tendermint node
- ABCI протокол для взаимодействия с Машиной Состояний
- ~10 заготовок на 8 ЯП для Машины Состояний
- Cosmos SDK для создания своих интер-операбельных блокчейнов, объединённых в Cosmos Network
- BigchainDB, Hyperledger Burrow и другие используют в качестве Consensus Engine



dApp	Децентрализованное приложение, без серверной инфраструктуры, паролей пользователей и т.п.
Токен	Fungible: долговая расписка на 1 руб. 50 коп., киловатт электроэнергии. Non-fungible: крипто-котик с ДНК в u256.
Sidechain	AEUR и Ignis по отношению к Ardor (child chains). RSK по отношению к BTC (side). Two-way peg: federated vs. pure.
EVM	Похожа на JVM, только проще и с детерминированностью (float арифметика не зависит от реализации, и т.п.)
State	UTXO db в случае BTC. Accounts в случае ETH и NXT. Все родившиеся котята в случае dApp Crypto Kitties.

ABCI – это как API, только для Блокчейна

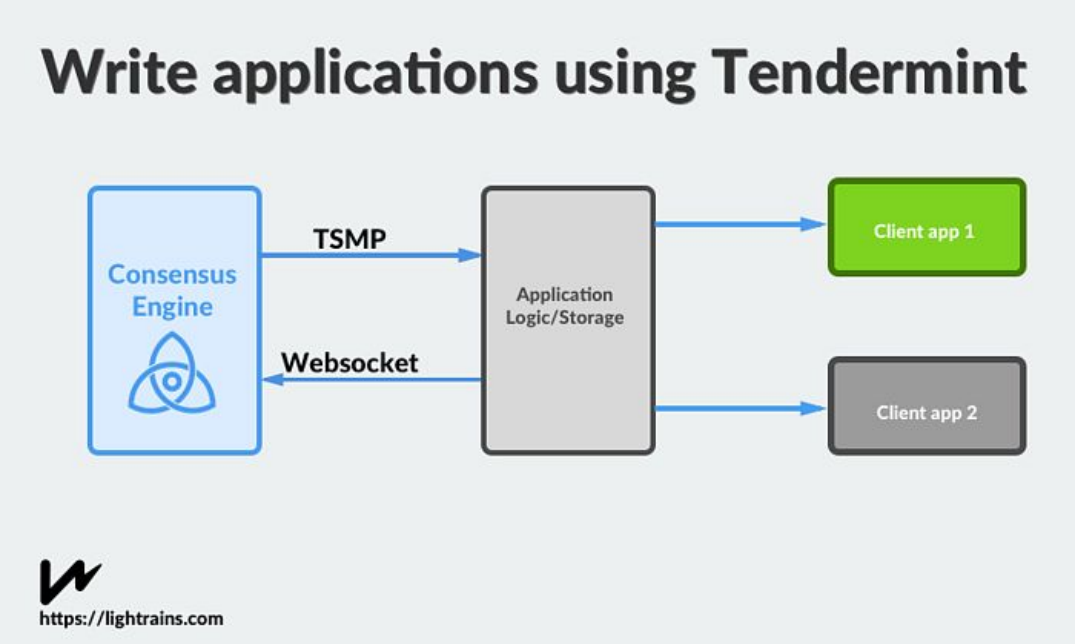
- ★ Basecoin (Cosmos SDK) реализует платформу с accounts and balances, пригодную для выпуска токенов и создания dApps, разнесённых на отдельные sidechains
- ★ Ethermint реализует Ethereum Virtual Machine, но с Tendermint в качестве консенсуса
- ★ ОЦРВ ABCI-prototype реализует World State на sqlite3, State Machine на Plain Java без фреймворков и ORM, простейший cmdline клиент на Python
- ★ ОЦРВ ABCI-backend реализует сервер на основе микро-фреймворка Dropwizard (lightweight аналог Spring), код которого имеет общую часть с ABCI-prototype
- ★ 2500 SLOC на Java и Python, 75% от общего числа .py+.java строк в проекте

Очень простая схема ABCI приложения

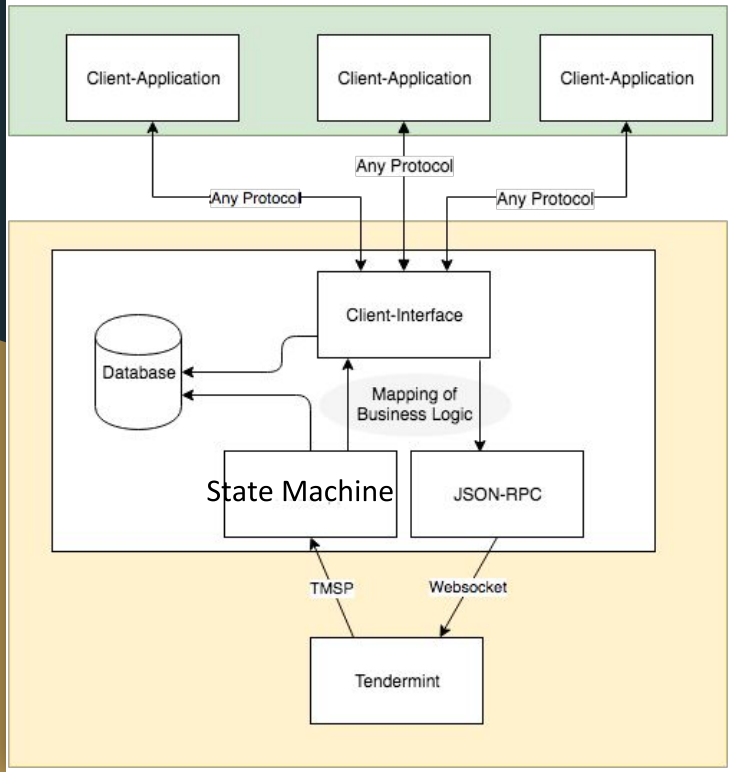
Если приложение написано не на Go, используется gRPC либо Socket

Структуры данных описаны при помощи protobuf (Protocol Buffers), поэтому основная часть заготовки генерируется автоматически

Можно переиспользовать практически любой код, написанный до наступления эры Блокчейн, встроив его в ABCI



Слегка более детальная схема ABCI приложения с его окружением



Благодаря тому, что State Machine программируется “как обычно” (нужно лишь реализовать правильно её взаимодействие с Tendermint Node), кривая освоения технологии – пологая

Кроме ABCI, Tendermint не диктует разработчику приложения ничего, поэтому каждая организация, разрабатывающая ПО, имеет простор выбирать из своих наилучших практик

4 Поколения Блокчейн-систем

Век “умельцев”: каждый велосипед не похож на другой, как до XIX в.

Индустриальный век незадолго до запуска первого конвейера...

I. II. III. IV.

bitcoin

litecoin

namecoin

ETHEREUM

NXT GENERATION OF CRYPTOCURRENCY

Byteball

ardor

RSK SMART CONTRACTS OVER BITCOIN

decred

bitshares blockchain foundat

nem

STEEM

Лотерейные консенсусы: Proof of Work, Proof of Stake с алгоритмом “слепого стрелка”

Гибридные и голосовательные консенсусы: PoW+PoS, dPoS, PBFT и его варианты

Pluggable консенсусы и P2P, сборка из стандартизованных деталей, как у велосипеда XXI в.