# Алгоритмы консенсуса

Писковский Виктор Олегович

# План

Введение

1. История вопроса
2. Определения
3. Hash функция
4. Алгоритмы консенсуса
   - Blockchain
     - Proof of work
     - Proof of Storage
     - Proof of Stake
     - Byzantine Fault Tolerance
   - HashGraph
   - DAG
     - BlockDAG
     - TxDAG

# Определения

Консенсус - процесс принятия решений группой, в котором все
члены группы соглашаются поддержать решение в интересах целого.

Hash функция - Функция свёртки, преобразующая массив входных данных в битовую строку заданной длины.

# Hash функция. Требования

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.*

*Примечание: Non-fungible Token (NFT), PCI-DSS*

# Blockchain. Proof of Work (PoW)

| 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*

# Blockchain. Proof of Storage (PoStorage)

| Название | Описание | Применение | Произв. |
|---|---|---|---|
| Proof of Capacity (PoC), Proof of Storage (PoStorage), Proof of Space (PoSpace) | Для определения права на получение блока сравнивается объём свободного места на жестком диске вместо использования вычислительных ресурсов | BurstCoint, SpaceMint, Chia | 140 TPS |
| Provable Data Possession (PDP) доказательство владения данными | Для определения приоритета (в том числе для создания блока) на узел отправляется данные, а затем периодически проверяют, хранит ли узел эти данные | Filecoin | |
| Proof-of-Retrievability (PoRet) | Тоже, что PDP, но добавляется возможность проверить, что узел в состоянии восстановить испорченные данные. | Filecoin | |
| Proof-of-Replication (PoRep) | Для определения приоритета (в том числе для создания блока) используется доказательство того, что при реплицированном хранении данных, каждая реплика хранится отдельно и независимо | Filecoin | |
| Proof of Space and Time (PoST) | В отличие от алгоритма PoC учитывает и период времени, во время которого используется дисковое пространство | Chia, Spacemesh, Filecoin | |

# Blockchain. Proof of Stake (PoS)

| 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 возворащается 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 | |

# Blockchain. Proof of Stake (PoS)

| Название | Описание | Применение |
|---|---|---|
| . Proof-of-Activity (PoA) (Доказательство активности) | Симбиоз PoW и PoS, используются оба алгоритма, при расхождении результатов вес блоков PoW больше. | Kovan, Decred |
| Proof-of-Devotion (PoD) доказательство преданности | В сети действуют система ранжирования (Nebulas ranking)узлов, учитывающая ликвидность и влияние в сети Узлы с наибольшим рангом получают право создавать блоки | Nebulas |
| Proof-of-Importance (PoI) (Доказательство важности) | Для определения узлов для создания блоков учитываются кроме наличия достаточного количества монет (PoS) также репутация, определяемая по специальным правилам, количество транзакций. | NEM |
| . Proof-of-Location (PoL) | PoS дополненная иформацией о географическом расположении мобильных узлов. Используется для исполнепния смарт-контрактов, например, подтверждения доставки товара по адресу из интернет магазина. | FOAM, Platin |
| Proof-of-Elapsed-Time (PoET) (Доказательство прошедшего времени) | Узлы генерируют случайным образом время ожидания Узел, у которого это время закончилось раньше других создает новый блок в цепочке | Intel |

# Blockchain. Proof of Stake (PoS)

| Название | Описание | Применение |
|---|---|---|
| Proof of Burn (PoB) доказательство сжигания | Для определения права на получение блока используется отпварка токенов на кошелёк, к которому ни у кого нет доступа | Slincoin |
| Proof of Credit Share (PoCS) доказательство доли кредита | После обмена информацией  которого заключается в устранении дисбаланса при обмене информацией между крупными и небольшими компаниями. Расчет баллов PoCS осуществляется после завершения членами альянса процессов обмена данными. Оценивается PoCS в зависимости от частоты транзакций. Эти параметры учитываются для проведения оплаты. Те из членов альянса, которые имеют меньший счет, будут вынуждены оплачивать более высокие комиссии. В то же время для участников с высокими счетами транзакционная комиссия будет снижаться. | |
| Proof-of-Signature (PoSign) доказательство подписи | Блоки подпсиываются всеми узлами, если узел замечен в соверщении атаки, то он исключается из сети и далее в созхдании блоков не участвует | XTRABYTES |

# Blockchain. Proof of Stake (PoS)

| Название | Описание | Применение |
|---|---|---|
| Proof-of-Brain доказательство «мозговой деятельности» | Чем более качественное содержание блока, тем больше голосов получает узел, создавший блок, тем больше монет он может получить | Steemit, Golos |
| Proof of Service | Мастер-узлы депонируют не менее определенного количества монет за право участвовать в выборе узла для создания блока. Для участия в выборе мастер узел депонируют дополнительно некоторое количество монет, которое получает обратно после образования нового блока | Remme |
| Proof of Weight (PoWeight) | Используется механизм веса пользователей сети (узлов), чем больше монет - тем больше вес | |

# Blockchain. Byzantine Fault Tolerance (BFT)

| Название | Описание | Применение | Пр-сть |
|---|---|---|---|
| Practical Byzantine Fault Tolerance (pBFT) (Реализация протокола задачи византийских генералов) | Блок принимается даже, если у одной трети узлов, создающих блок, значения недоступны или отличаются. Round-robin | Hyperledger, Chain | 700 TPS |
| Honey Badger BFT (HBBFT) Democratic BFT | В отличие от pBFT протокол асинхронный, не требует лидеров для создания блока, все узлы предлагают свои блоки, использует эффективный протокол для обмена информацией между узлами небольшими порциями. | NEO | 1 000 TPS |
| Red Belly BFT (RBBC= Red Belly BFT Consensus) | Улучшенный HBBFT, не допускает ответвлений, использует шардинг, параллельные вычисления ECDSA | | 700 тцс. - 1 мле TPS |
| Delegated Byzantine Fault Tolerance (DBFT) | Голосование по доверенности: владелец монет назначает узел, которому он доверяет. Выбранная таким образом группа узлов генерирует новые блоки | NEO, TON | |

# Blockchain. Byzantine Fault Tolerance (BFT)

| Название | Описание | Применение | Пр-сть |
|---|---|---|---|
| Simplified Byzantine Fault Tolerance (SBFT) | Определяются один генератор блоков и несколько подписчиков. Выбранный узел (генератор блоков) собирает и проверяет предложенные транзакции, периодически объединяя их в новый блок. Выбранные подписчики блоков проверяют и ратифицируют новый блок. | | |
| Scalable BFT | PBFT, дополненная иерархией узлов. Комитет занимается созданием блоков, Выбор узлов комитета подвержен специальной процедуре, обеспечивающей масштабирование системы. Если в сети узлов много больше чем узлов, входящих в комитет, то зависимость скорость регистрации транзакций от числа узлов приближено к линейной. | | 4 000 TPS |
| Federated Byzantine Agreement (FBA) (Федеративное византийское соглашение | Блок принимается, если он подписан заранее определённым количеством квалифицированных подписчиков | Stellar, Ripple | |

# HashGraph.BFT

| Название | Описание | Применение | Пр-сть |
|---|---|---|---|
| Asynchronous BFT (ABFT) | Используется подход асинхронного BFT в рамках разработанного протокола gossip protocol. | Hedera | 250 - 350 тыс. TPS |

Примечание: не устойчив к атакам Sybil

# DAG.BlockDAG

| Название | Описание | Применение | Пр-сть |
|---|---|---|---|
| SPECTRE | Каждый узел инициирует рекурсивного голосования для определения порядка доступных ему блоков | | > 1 млн TPS, практически безграничная масштабируемость |
| PHANTOM | Реализовано  полностью линейное упорядочение транзакций и блоков. Каждый узел ищет наибольший k-кластер блоков, где k-степень узла, предопределена в реестре. K-кластер считается честным, и все блоки в нем линейно упорядочены | | |
| Conflux | в качестве главной цепи используется самая длинная цепочка внутри самого тяжелого поддерева | | |

# DAG.TxDAG

| Название | Описание | Применение | Пр-сть |
|---|---|---|---|
| Tangle | Разновидность Asynchronous BFT (ABFT). Любой узел может инициировать транзакцию, но для проверки он должен проверить две предыдущие транзакции в реестре. Для достижения консенсуса используется специально асинхронный протокол. Чем длиннее ветвь проверяемой транзакции, тем больший вес оно имеет. Пользователь присоединяет хэши двух выбранных транзакций к новой транзакции и выполняет работу PoW | NXT IOTA Tangle, Holochain-DLT, RADIX (TEMPO) | > 1 млн TPS, практически безграничная масштабируемость |
| Byteball | Похож на PoS и aBFT. Выделена группа свидетелей, которые и образуют новые элементы (сообщения) в одно-ранговой сети. | Obyte | |
| Nano | Nano работает с блочно-решетчатой структурой. Каждый узел запускает локальную цепочку блоков, которая пересекается с другими. Транзакция выполняется двумя транзакциями: транзакция отправки в блокчейне отправителя и транзакция получения в блокчейне получателя. PoW Для защиты от спама используется подход PoW | Nano | |
| Avalanche | Основан на BFT без лидера FBA | | |