Правительство Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

Факультет компьютерных наук
Департамент программной инженерии
Образовательная программа 09.03.04 «Программная инженерия»

ОТЧЕТ

по производственной практике
Подготовка ВКР на тему
Криптографические алгоритмы и протоколы для распределенных реестров

Выполнил студент
Группы БПИ 151
Куприянов Кирилл.

Руководитель практики от департамента ПИ:

Должность _____

ФИО _____ Оценка _____

Дата _____ Подпись _____

Оценка комиссии:
Дата _____ Оценка _____ Подпись _____

Москва, 2018г.

Содержание

1 Введение

Тема производственной практики непосредственно связана с выбранной темой ВКР “Криптографические алгоритмы и протоколы для распределённых реестров”.

Моей **целью** было проделать анализ основных и наиболее распространённых криптографических алгоритмов для распределённых реестров в мире.

Были поставлены следующие **задачи**:

- Выявить популярные распределённые реестры и выделить криптографические алгоритмы в них
- Изучить выявленные алгоритмы
- Замерить параметры алгоритмов
- Классифицировать их по:
  - Времени работы
  - Эффективности по памяти
  - Количеству операций в секунду
- Сделать обзор лучших алгоритмов по приведённым параметрам

2 Описание предметной области

Распределённый реестр — это база данных, которая распределена между несколькими сетевыми узлами (вычислительными устройствами). Каждый узел получает данные из других узлов, хранит полную копию реестра, а обновления узлов происходят независимо друг от друга. Пример распределенного реестра — платформа Corda от R3.

Блокчейн — это технология распределённого реестра, которая представляет собой набор блоков, куда записываются совершающиеся транзакции. Не все распределенные реестры используют последовательность блоков для достижения достоверного консенсуса в распределенной системе защищенным от злоупотреблений способом. Основное преимущество технологии блокчейн заключается в том, что она позволяет проводить транзакции с несколькими сторонами, что делает её децентрализованной, а также безопасносной.

Блокчейн обычно ассоциируется с криптовалютой Bitcoin, так как это было самое раннее использование блокчейна. По мере развития технологии, количество различных блокчейнов с особенностями вариантов использования резко увеличилось.

3 Блокчейны

В этом разделе будут описаны распределённые реестры, которые являются блокчейнами.

Такие технологии как Биткоин, Эфириум, и др., основаны на комбинации трёх технологий: P2P сети, криптография, и теория игр. Целью системы в целом является достижение “консенсуса” (между сторонами, которые не знают друг друга, и, возможно, не доверяют) в том, какая сделка является правилльной, без помощи централизованного лица. Чтобы достичь приватности и прозрачности, используются **криптографические алгоритмы с публичным кючом**, и **хэш-функции**, про которые речь пойдёт позже.

Существуют публичные, приватные блокчейны, и блокчейны консорциума (согласно Vitalik Buterin, создателю Эфириума). В данной работе будут рассмотрены публичные блокчейны, наиболее популярные и представляющие научный интерес.

3.1 Публичные блокчейны

- Bitcoin
- Litecoin
- Ether
- Monero
- Verge
- Dash
- Gram

3.2 Приватные блокчейны

- Внутри компаний

3.3 Блокчейны консорциума

- r3
- Hyperledger

4 Криптографические алгоритмы

Существует 2 вида криптографических систем, которые испльзуют в распределённых реестрах: **симметричные алгоритмы** и **асимметричные**.

4.1 Симметричные

Две стороны договариваются о **секретном ключе** (private key) и используют один и тот же ключ для шифрования и дешифрования. Проблема с этим подходом заключается в том, что этот метод не масштабируется. Если подразумевается общение в частном порядке с кем-то, необходимо физически встретиться и договориться о секретном ключе. В современном мире, где нам необходимо координировать свои действия со многими субъектами, такие методы были бы неосуществимы. Обработка данных в симметричных системах выполняется быстрее, чем в асимметричных, так как обычно используются ключи меньшей длины. С другой стороны, шифрование файлов и сообщений с помощью ассимметричных алгоритмов не всегда практична. Основная причина-производительность. Симметричный ключ шифрования гораздо быстрее и лучше обрабатывает шифрование больших файлов и баз данных, поэтому, по-прежнему широко используется.

Примеры симмертичных алгоритмов:

AES (Advanced Encryption Standard), **RC2** (ARC2, Ron's Code), **RC4**, **RC5**, **RC6**, **CAST** (Carlisle Adams and Stafford Tavares), **DES** (Data Encryption Standard), **Triple DES**, **ARIA** (основан на AES), **SEED** (Korean).

Позже я рассмотрю распределённые реестры, в которых используются данные технологии.

4.1.1 Асимметричные

Асимметричные системы используют **открытый ключ** для шифрования сообщения, а закрытый ключ для расшифровки. Использование асимметричных систем повышает безопасность связи. Каждая сторона создает свою собственную пару открытого и закрытого ключей. Закрытые ключи должны храниться в тайне, а открытый ключ может свободно распространяться между сторонами. В асимметричном сценарии шифрования две стороны будут распространять свои открытые ключи и разрешать всем шифровать сообщения с помощью своих открытых ключей. Благодаря математическим алгоритмам работы пар ключей, невозможно расшифровать сообщение, зашифрованное открытым ключом. Это сообщение может безопасно передаваться владельцу закрытого ключа, и только он/она сможет расшифровать сообщение с помощью закрытого ключа, связанного с открытым ключом (padlock). Этот метод работает наоборот. Любое сообщение, зашифрованное с помощью закрытого ключа, может быть расшифровано только с помощью соответствующего открытого ключа. Этот метод также называется цифровой подписью. Криптография с открытым ключом существует с 1970-х годов и с тех пор используется в компьютерной и коммуникационной безопасности.

Примеры асимметричных систем: **RSA (1024-8192)**, **DSA (1024-3072)**, **Diffie-Hellman**, **KCDSA**, **Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined, and brainpool curves**.

4.1.2 Алгоритмы хэширования

Хотя алгоритмы хэширования не являются напрямую алгоримами из обласи криптографии, именно в криптовалютах они нашли своё применение. Алгоримты хэширования помогают представить множество данных (такие как хэши предыдущих блоков, настоящий timestamp, информация о пользователе,...) в одной строке фиксированной длины.

Примеры используемых алгоритмов хэширования: **SHA-1**, **SHA-2 (224-512)**, **SSL3-MD5-MAC**, **SSL3-SHA-1-MAC**, **SM3**

5 Сравнение алгоритмов

Чтобы посмотреть глубже на конкретную криптовалюту, необходимо знать какие алгоритмы используются для:

- Хэширования
- Генерирования приватного и публичного ключа
- Цифровой подписи
- Верифицирования сигнатуры публичным ключом

5.1 Bitcoin

Хэширование: **SHA-256**
Цифровая подпись: **ECDSA**
Случайные числа: OpenSSL's **RAND_bytes**
Верификация: **ECDSA**

5.2 Litecoin

Хэширование: **Scrypt**
Цифровая подпись: **ECDSA**
Случайные числа: OpenSSL's **RAND_bytes**
Верификация: **ECDSA**

5.3 Ether

Хэширование: **KECCAK-256**; **Ethash**
Цифровая подпись: **ECDSA**
Solidity Language:

```
function random() private view returns (uint8) {
       return uint8(uint256(keccak256(block.timestamp, block.difficulty))%251);
}
```

Верификация: **ECDSA**

5.4 Monero

Хэширование: **KECCAK-256**; **CryptoNote**
Цифровая подпись: **EdDSA**
Случайные числа: **DRBG**
Верификация: **EdDSA**

5.5 Verge

Технология Stealth address
Хэширование: **Scrypt, X17, Lyra2rev2, myr-groestl, blake2s**
Цифровая подпись: **ECDH**
Случайные числа: **DRBG**
Верификация: **ECDH**

5.6 Dash

Хэширование: **X11**
Цифровая подпись: **EdDSA**
Случайные числа: **CPRNG**
Верификация: **EdDSA**

5.7 Gram

Статус криптовалюты: MVP, не стабильный
Хэширование: **UNKNOWN**
Цифровая подпись: **UNKNOWN**
Случайные числа: **UNKNOWN**
Верификация: **UNKNOWN**

6 Распределённые реестры, не являющиеся блокчейнами

Такие криптовалюты, как Byteball, IOTA не используют блокчейн. Вместо него, они имплементируют алгоритм направленных ациклических графов (DAG). Рассмотрим подробнее IOTA. В отличие от уже успевшей стать традиционной системы blockchain, IOTA использует не одну цепочку блоков, а технологию DAG – систему цепочек блоков, работающих по определенному принципу. Это, скорее, похоже на сеть цепочек блоков, каждый из которых должен подтверждать два предыдущих блока по принципу близлежащего. Если же рядом нет блоков, а ближайший находится на расстоянии двух участков, то происходит косвенное его подтверждение.

Регулирующие узлы могут отклонять одобрение конфликтующих транзакций, в случае, если информация не соответствует начальной (при отправке перевода) или имеются неоднородности в структуре очередного денежного перевода. И наоборот, чем больше одобрений от системы получает транзакция, тем меньше вероятность “двойной траты”.

7 Заключение

SHA-256 является более сложным из алгоритмов, и он используется биткойном и большинством валют. Обработка блоков данных с SHA-256 имеет тенденцию быть медленнее-время выполнения транзакций, в результате, измеряется в минутах, а не в секундах—но утверждается, что это также более тщательно и оставляет меньше места для ошибок. Его сторонники также утверждают, что это лучше для общей безопасности данных.

Scrypt-это более быстрый и простой алгоритм, по сравнению с SHA, и по мере внедрения новых цифровых валют больше из них предпочитают его SHA-256. Scrypt намного проще запускать на уже существующем процессоре и, как правило, он использует меньше энергии, чем SHA-256. Некоторые утверждают, что эта более простая система сильнее восприимчива

к проблемам безопасности, так как быстрое время выполнения транзакций может означать, что система менее тщательно изучает данные, ведь хэш не высчитывается до конца. Его сторонники указывают, однако, что это до сих пор не представляло реальную проблему.

Криптовалюта Verge использует другие алгоритмы для хэширования и цифровых подписей, но имеет значительное преимущество. Её технология скрывает в блоках IP адреса клиентов при помощи Stealth address (реализовано через Tor сеть). Благодаря этому, выбор лиц, которым важна приватность и безопасность, падает на данную валюту.

IOTA заслужила отдельное внимание за DAG (направленный ациклический граф). Такая технология не только не использует блокчейн, но ещё и может бесконечно масштабироваться и является полностью бесплатной для использования.

Каждая технология в чем-то превосходит другую, но не более чем на то количество жертв, на которые пришлось им пойти для выигрыша данного преимущества. Например, Scrypt работает гораздо быстрее, чем SHA-256, но менее безопасен по этой причине. Выбор технологии зависит от правильного расставления приоритетотв и бизнес-логики программи.

8 Приложение 1

Для вычисления параметров быстродействия была использована библиотека crypto++ (язык C++).