

РАЗРАБОТКА ДЕАНОНИМИЗИРОВАННОЙ КРИПТОВАЛЮТЫ

Кривуля Марина Алексеевна

кандидат экономических наук, доцент кафедры экономики и финансов

Колесник Ольга Леонидовна

старший преподаватель кафедры информатики

Копченко Вадим Константинович

студент факультета естественных наук и математики

ФГБОУ ВО «Северо-Восточный государственный университет», г.Магадан

Аннотация. В статье рассматриваются принципы работы и возможности применения криптовалют, преимущества и недостатки технологической базы. Предлагается элемент дополнения технологической структуры криптовалюты для внедрения данного инструмента как платежного средства.

Ключевые слова: криптовалюта, биткоин, блокчейн, анонимность, децентрализация, распределенность.

Появившаяся в 2008 году криптовалюта Bitcoin на базе технологии blockchain стала первой попыткой исправить ощутимые недостатки современной банковской системы [2, с. 13]. Речь, в частности, идет о неудобствах при международных переводах, где продолжительность операции может составить несколько дней, что усложняет взаиморасчеты между компаниями, о высоких комиссиях банка за посреднические услуги, об ограничениях финансовых операций в политических целях. Bitcoin позволяют избавиться от этих недостатков.

Тем не менее, существует ряд недостатков технологии Bitcoin [1, с. 280]. Наиболее выраженный – сложность внедрения в существующие платежные системы, что ограничивает оборот валюты в рамки сети Интернет. С целью исправления данного недостатка создаются новые типы криптовалют (ethereum, NEM) [2, с. 105], которые как исправляют существующие недостатки, так и приносят новые возможности (например, повышенную защищенность). Однако, рынок криптовалют в еще большей степени ограничивает его анонимность. Для перевода средств не требуется удостоверять личность, достаточно знать адрес кошелька получателя, что для многих стран стало поводом ограничения оборота подобного рода финансов. Однако, при подробном рассмотрении технологии становится очевидно, что и этот недостаток можно исправить.

Blockchain– нереляционная база данных, которая хранит цепочки блоков (структур, в которых хранится информация о переводах средств), идентифицируемых уникальным

идентификатором (хэшем), который генерируется исходя из характеристик блока, что исключает возможность фальсификации данных о транзакциях [5]. Каждый вновь добавленный в базу блок хранит ссылку на предыдущий, обеспечивая тем самым согласованность данных.

Такая структура данных не уникальна. Ее можно легко воссоздать во многих нереляционных системах управления базами данных (СУБД), поддерживающих динамическую структуру [6]. Примером такой СУБД может служить ApacheCassandra – свободная децентрализованная надежная и быстрая система хранения данных с поддержкой согласованности данных, масштабирования и возможностью репликации на множество узлов, что обеспечивает ей отсутствие единой точки отказа (то есть, при выходе из строя какого-либо узла, целостность данных не будет нарушена, так как база горизонтально копируется на множество указанных администратором машин) [1, с. 44]. Список ее характеристик полностью идентичен характеристикам Blockchain, но последний, как упоминалось ранее, не хранит информацию о лице, совершившем перевод или получение средств. Это можно исправить, создав для Cassandra структуру данных, обязательным полем которой станет информация о пользователе сети (структура записи представлена на рисунке 1).



Рис.1. Структура записи

Реализовать запись в Cassandra данных такого уровня можно через формат Json [7]. Этот формат понятен человеку, а также легко может быть получен из пользовательских структур данных во многих объектно-ориентированных языках программирования, исходными данными для сериализации служит структура данных transaction, написанная на языке программирования C# (код структуры приведен на рисунке 2).

```

public class transaction
{
    public string UserInfo { get; set ;}
    public string FullName { get; set; }
    public uint Passport { get; set; }
    public uint Direction { get; set; }
    public float Rate { get; set; }
}

```

Рис. 2. Код C# для сериализации

Сохранить строку JSON можно в виде простой строки, (предполагая, что в качестве названия блока выступает хеш предыдущего). Однако, невозможно создавать запросы на основе содержимого JSON: это непрозрачные данные, которые обрабатываются на стороне клиента (клиентская программа для работы с криптовалютным счетом называется кошельком), что многократно увеличивает надежность хранилища.

Обобщая вышеизложенное, можно составить диаграмму IDEF0, иллюстрирующую процессы создания транзакции и добавления ее в блок. Пользователь определяет получателя средств, сумму перевода, полученные данные формируют хеш, формат которого зависит от выбранного криптографического протокола и схемы его размещения в базе данных. Далее, зашифрованная информация о транзакции подписывается электронной цифровой подписью и попадает, непосредственно, в базу данных.

Алгоритм получения электронной цифровой подписи весьма просто реализуется на языке C#, подписывать следует не сами данные, а хеш, что также позитивно сказывается на защищенности хранилища транзакций.

На основе вышеизложенного очевидно, что создание криптовалюты на основе баз данных, отличных от Blockchain, вполне возможно. ApacheCassandraлучше всего подходит для этих целей, так как имеет схожие характеристики и возможность создания динамических структур хранимых данных.

Список литературы:

1. Джефф Карпентер, Эбен Хьюитт - Cassandra. Полное руководство. М.: ДМК пресс, 2017. – 400 с.
2. Мелани Свон - Блокчейн.Схема новой экономики. - М.: Олимп-Бизнес, 2017. – 240 с.
3. Почему Биткойн имеет ценность: немного о сетевом эффекте // BitNovosti URL: <https://bitnovosti.com/2015/01/27/why-bitcoin-have-value/> (дата обращения: 11.04.2018).
4. Погружение в СУБД ApacheCassandra // IBM developerWorks URL: <https://www.ibm.com/developerworks/ru/library/os-apachecassandra/index.html> (дата обращения: 10.02.2018).

5. Что такое Blockchain (блокчейн)? Технология, платформа, транзакции. // Майнинг криптовалюты URL: <https://mining-cryptocurrency.ru/blockchain/> (дата обращения: 15.04.2018).
6. Blockchain: Any experiences with NoSQL? Any suggestions for alternatives? // ResearchGate URL: https://www.researchgate.net/post/Blockchain_Any_experiences_with_NoSQL_Any_suggestions_for_alternatives (дата обращения: 10.02.2018).
7. Efficient way to store a JSON string in a Cassandra column? // Stack Overflow URL: <https://stackoverflow.com/questions/36342531/efficient-way-to-store-a-json-string-in-a-cassandra-column> (дата обращения: 17.04.2018).