УДК 004 **Информационные технологии**

Чистяков М. А., *аспирант 1 курс, Высшая школа экономики и менеджмента*
ФГАОУ ВО «УрФУ имени первого Президента России Б. Н. Ельцина»
Россия, г. Екатеринбург

ИЗМЕНЕНИЕ ДАННЫХ В РАСПРЕДЕЛЁННОМ РЕЕСТРЕ ПОСРЕДСТВОМ ЗАМЕНЫ БЛОКОВ

Аннотация: Данная работа описывает эксперимент, в котором была предпринята попытка изменения данных в распределённом реестре (блокчейне) через удаление последовательности нужных блоков и последующим добавлением новых таким образом, чтобы изменения не были заметны. Эксперимент был проведён на базе Hyperledger Fabric. Эксперимент удалось совершить при 100% доступе ко всем узлам в сети. Временные штампы удалось подделать. Результаты хэш-функций не сохранились.

Ключевые слова: блокчейн, распределённый реестр, Hyperledger, виртуальные машины, Docker.

Annotation: This paper describes an experiment which goal was to perform data altering in a distributed ledger (blockchain) through removing arbitrary sequence of blocks and adding new ones with the least possible number of noticeable changes. This experiment was done using Hyperledger Fabric platform. Experiment was successfully performed only with 100% access to all peers in the network. Timestamps were successfully altered. Block hashes didn’t save.

Keywords: blockchain, distributed ledger, Hyperledger, virtual machines, Docker.

ВВЕДЕНИЕ

Одним из самых интересных открытий в сфере информационных технологий последних лет является блокчейн. Впервые он появился в сети Bitcoin и с тех пор используется в большинстве цифровых валют. Считается, что этот новый вид баз данных наделяет системы небывалыми до того возможностями, а именно – полная децентрализация всех процессов, возможность договориться между лицами, не доверяющими друг другу, без доверенной третьей стороны, и невозможность изменить информацию об уже исполненных транзакциях [1]. Но действительно ли информация неизменяема в блокчейне? Есть ли способы опровергнуть это суждение?

В данной работе был использован Hyperledger Fabric – блокчейн-система, входящая в большой зонтичный проект HyperLedger, организованный в 2015 году и имеющий на данный момент внушительный список из более чем 100 участников [2]. С помощью Hyperledger Fabric был проведён эксперимент, цель которого - выявление возможности изменения данных в блокчейне методом использования резервного копирования. Задачи, поставленные перед исследователем:

- Построение экспериментальной бизнес-сети на основе Hyperledger Fabric, состоящей из 3-5 клиентов (пиров);
- Анализ путей создания и развёртывания резервных копий различных элементов системы;
- Испытание с помощью отправки транзакций в сеть и создания резервных копий на определённых этапах.

ОПИСАНИЕ ЭКСПЕРИМЕНТА

Для выполнения поставленных задач была организована сеть из пяти виртуальных машин VMware Player с предустановленными Ubuntu 16.04, на которых была развёрнута сеть Hyperledger Fabric.

Основная особенность Hyperledger Fabric как блокчейн-системы заключается в том, что она позволяет не только добавлять данные в распределённый реестр, но и удалять их из него, однако в отличие от традиционных баз данных абсолютно все операции записываются как

транзакции и собираются в цепочку. Таким образом сохраняется полная история изменения реестра, в которой видно, какой именно участник добавил или удалил, например, актив. При этом исходя из определения блокчейна ни одну отдельно взятую транзакцию невозможно изменить. Задача исследователя заключается в том, чтобы найти решение, позволяющее стереть произвольную цепочку блоков в блокчейне и заполнить его изменёнными блоками, желательно с аналогичными временными штампами (Timestamps), таким образом формально изменив данные в блокчейне.

Поиск решения планировалось начать с создания резервной копии определённой части системы на определённой транзакции. Было найдено два предполагаемых способа сделать это:

1. Сделать резервную копию базы данных CouchDB;
2. Сделать образы всех работающих Docker-контейнеров с помощью docker commit.

Для работы с временными штампами было предложено просто изменять системное время перед выполнением транзакций.

В ходе проведения эксперимента было решено создать трёх участников сети и три актива, принадлежащих им, которые позволяют менять своё значение на любое желаемое. Задача – попробовать отменить создание одного участника и одного актива и создать их снова с возможностью выставить свой временной штамп.

РЕЗУЛЬТАТЫ

В ходе создания резервных копий было выявлено, что оба метода подходят для сохранения состояния блокчейна на любом этапе.

С результатами эксперимента можно ознакомиться в следующей таблице:

Общее кол-во узлов в сети	Успех изменения распределённого реестра при восстановлении резервной копии				Успех влияния на Timestamp	Сохранились ли хэши блоков?
	на 1 узле	на 2 узлах	на 3 узлах	на 5 узлах		
1	Да	-	-	-	Да	Нет
2	Нет	Да	-	-	Да	Нет
3	Нет	Нет	Да	-	Да	Нет
5	Нет	Нет	Нет	Да	Да	Нет

Интересным результатом эксперимента является то, что откатить блокчейн путём варианта атаки 51% не удалось. При этом если имеется контроль над всеми пирами и есть возможность создавать и восстанавливать резервные копии их данных, проблем с откатом блокчейна не возникает. В результате эксперимента удалось таким образом откатить блокчейн до состояния, в котором последний участник и актив ещё не были созданы. С подменой временного штампа путём изменения системного времени также не возникло проблем, однако стоит учитывать, что присутствие временного штампа не определяет порядок транзакций в блокчейне. Другими словами, Hyperledger Fabric допускает ситуацию, когда более поздняя транзакция в блокчейне обладает более ранним временным штампом – таким образом остаётся возможность раскрыть обман при вводе данных в блокчейн.

Другая возможность раскрыть обман скрывается в том, что результаты хэш-функций даже после одного изменённого блока будут совершенно другими. В данном случае всё зависит от предусмотрительности пользователей системы, а также от программного обеспечения, которое разрабатывается под эту платформу (она должна давать возможность просматривать хэши блоков в реестре для того, чтобы пользователи могли заметить их изменение).

Таким образом, данный эксперимент показал, что изменять данные в блокчейне действительно возможно, однако для этого необходимо соблюдать достаточно обширный ряд условий, при которых данный способ будет работать, при этом полностью скрыть факт изменения данных в реестре не представляется возможным.

Библиографический список:

1. Чистяков М., «Hyperledger Fabric: особенности, сферы применения», Аллея Науки, No. 2 (18), 776-780 (2018).

2. Хултквист Х. Что такое Hyperledger? Как Linux Foundation создает открытую платформу вокруг блокчейн проектов Intel и IBM // Голос. Beta [Электронный ресурс]. 21.06.2017. URL: https://golos.io/ru--

blokcheijn/@hultqvist/chto-takoe-hyperledger-kak-linux-foundation-sozdaet-otkrytuyu-platformu-vokrug-blokchein-proektov-intel-i-ibm.