Блокчейн изнутри

мастер-класс Сергея Лукашкина,

Директора по управлению проектами цифровой трансформации ВТБ

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

75 минут

+15 минут Q&A

ВТБ

- **Введение**
- Bitcoin
- Консенсус
- Криптовалюты
- Смарт-контракты
- Ethereum
- Ripple
- Hyperledger Fabric
- Corda
- Примеры
- Выводы

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Нужен ли вам блокчейн?

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Нужен ли вам блокчейн?

ДА!

Правильный ответ

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Что такое?

Что?

Делать

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

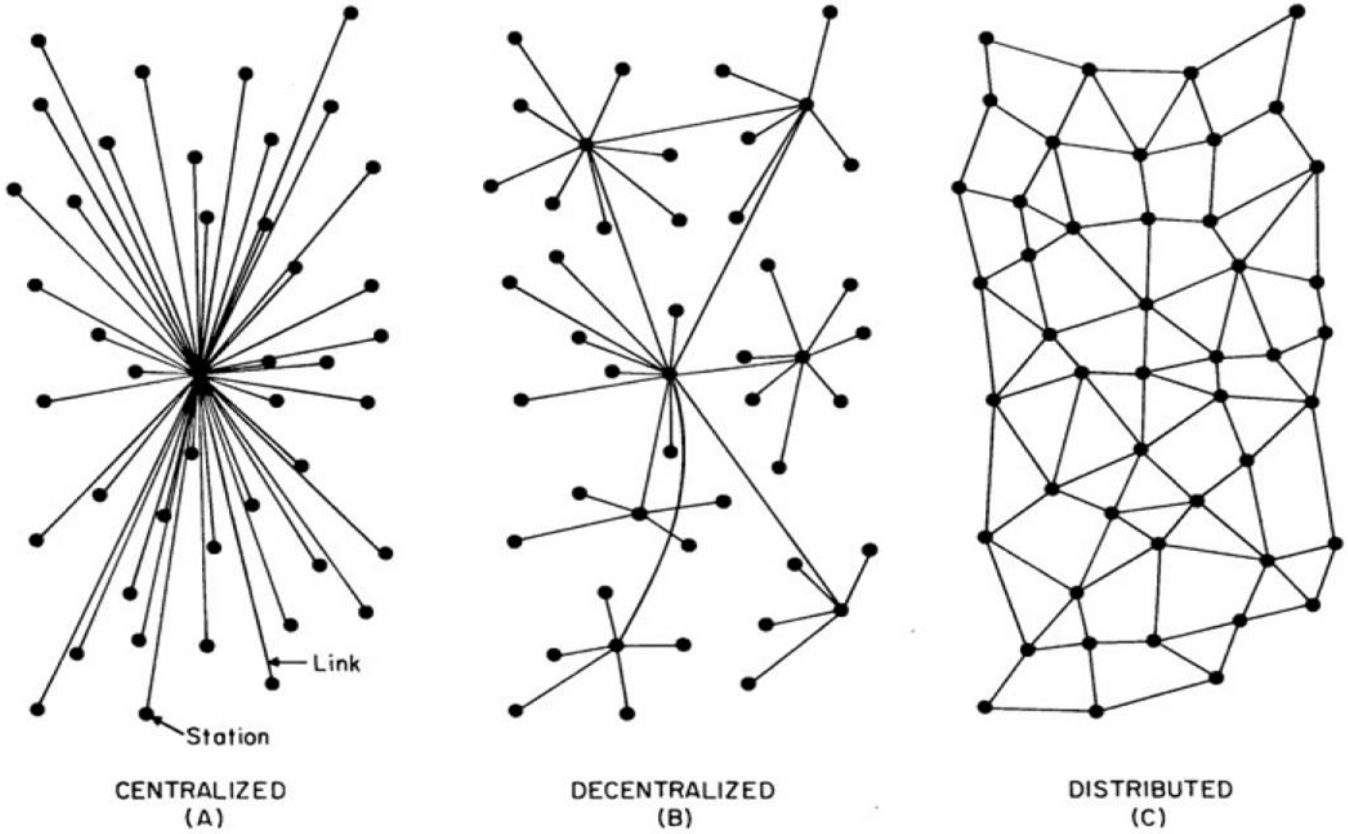
Выводы

Что такое биткоин

ВТБ

Введение
Bitcoin
Консенсус
Криптовалюты
Смарт-контракты
Ethereum
Ripple
Hyperledger Fabric
Corda
Примеры
Выводы

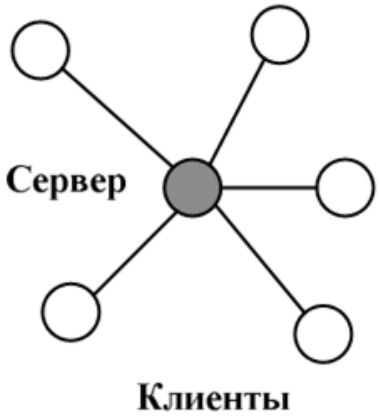
Архитектура

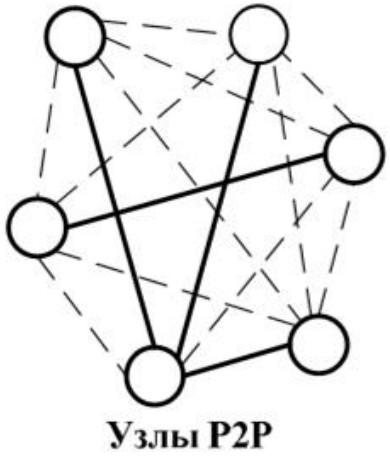


Технология одноранговых сетей

p2p-сетей от анг. peer-to-peer – равный-к-равному

Однора́нговая, децентрализо́ванная, или пи́ринговая (англ. peer-to-peer, P2P — равный к равному) сеть — это оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера.





ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

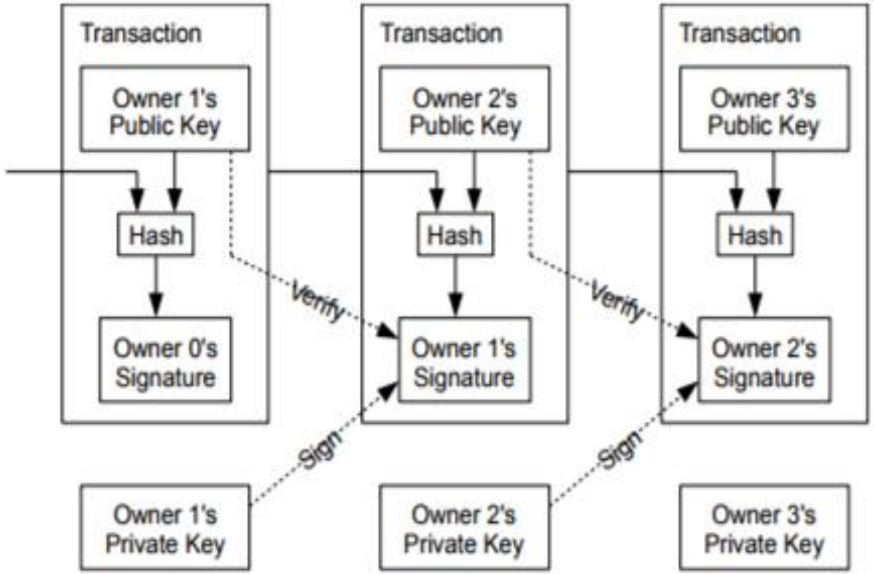
Преимущества одноранговых сетей

- высокая масштабируемость, связанная с равномерным распределением вычислительной нагрузки на всех участников сети;
- стабильность работы сети, независимость отдельных машин от выделенного сервера;
- возможность объединения ресурсов отдельных участников сети, и их предоставление другим участникам;
- распределение совокупных затрат на предоставление ресурсов между участниками сети;
- анонимность, т.е. пользователи могут избежать предоставления любой информацию о себе;
- легкость в установке и настройке;
- возможность пользователем контролировать свои собственные ресурсы;
- сравнительная дешевизна в приобретении и эксплуатации;
- отсутствие необходимости иметь отдельного человека в качестве выделенного администратора сети.

Bitcoin: A Peer-to-Peer Electronic Cash System (24 May 2009)

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



https://bitcoin.org/bitcoin.pdf

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

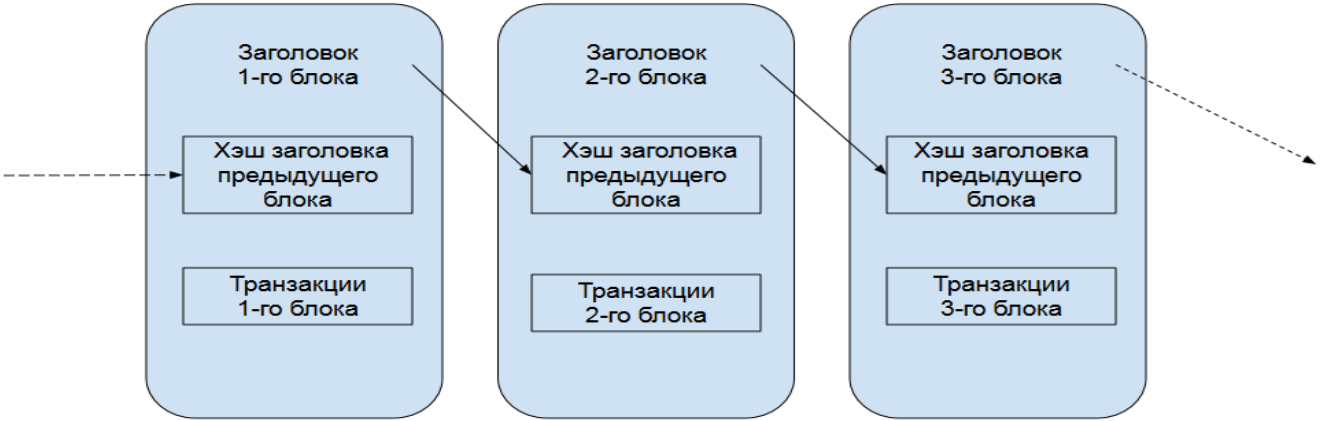
Corda

Примеры

Выводы

BlockChain - это

- структура данных
- упорядоченный обратно связанный список блоков
- ...



Упрощенная цепь блоков

Структура блока

Размер	Поле	Описание
4 байта	Размер блока	Размер блока в байтах
80 байт	Заголовок блока	Несколько полей образуют заголовок блока
1-9 байт (VarInt)	Счетчик транзакций	Количество транзакций в блоке
Переменная	Данные (транзакции)	Данные (транзакции), записанные в этом блоке

Структура заголовка блока

Размер	Поле	Описание
4 байта	Версия	Номер версии для отслеживания обновлений программного обеспечения/протоколов
32 байта	Хэш Предыдущего Блока	Ссылка на хэш предыдущего (родительского) блока в цепочке
32 байта	Корень дерева Меркле	Хэш корня дерева Меркле транзакций этого блока
4 байта	Временная метка	Приблизительное время создания этого блока (секунды от эпохи Unix*)
4 байта	Целевая сложность	Целевая сложность алгоритма доказательства работы для данного блока
4 байта	Некое случайное число (nonce)	Счетчик используется в алгоритме доказательства работы

*Определяется как количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года

Хэш

Хэширование — преобразование массива входных данных произвольной длины в выходную битовую строку фиксированной длины, выполняемое определённым алгоритмом.

Хэш-функция — функция, реализующая этот алгоритм и выполняющая преобразование. Значение, полученное в результате вычисления хэш-функции, называется **хэшем.**

SHA Secure Hash Algorithm - алгоритм стойкого хэширования

В блокчейне биткоинов используется SHA256

Результирующий 32-байтовый хэш называется *хэшем блока*, но более правильно его называть *хэшем заголовка блока*, потому что для его вычисления используется только заголовок блока.

Пример:

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f — это хэш самого первого блока Биткоин из когда-либо созданных.

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Алгоритм SHA256

Входит в семейство алгоритмов под общим названием **SHA-2** (опубликован в 2002 году – FIPS PUB 180-2, обновлен в 2008 году - FIPS PUB 180-3).

На вход подается сообщение любой длины, но меньшее, чем 2^{64} бит, а на выходе получаем 32-байтовый хэш.

Алгоритм состоит из двух этапов: предварительная обработка и вычисление хэша.

По материалам сайта http://solutionmes.wikidot.com/crypto-sha

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Свойства хэш-функции

хэш-функция должна удовлетворять двум **свойствам**:

- быстрое вычисление;
- минимальное количество «коллизий».

Кроме того, хорошая хэш-функция должна (приближенно) удовлетворять условию равномерного хэширования, т.е. все её значения должны быть равновероятны.

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Свойства хэш-функции

хэш-функция должна удовлетворять двум **свойствам**:

- быстрое вычисление;
- минимальное количество «коллизий».

Кроме того, хорошая хэш-функция должна (приближенно) удовлетворять условию равномерного хэширования, т.е. все её значения должны быть равновероятны.

Криптографические хэш-функции

Хэш-функция H считается криптографически стойкой, если она удовлетворяет трём основным требованиям:

- *необратимость*: для заданного значения хэш-функции *m* должно быть вычислительно неосуществимо найти блок данных X, для которого H(X)=m;
- стойкость к *коллизиям первого рода*: для заданного сообщения *M* должно быть вычислительно неосуществимо подобрать другое сообщение *N*, для которого H(N)=H(M);
- стойкость к *коллизиям второго рода*: должно быть вычислительно неосуществимо подобрать пару сообщений (M,M‘), имеющих одинаковый хэш.

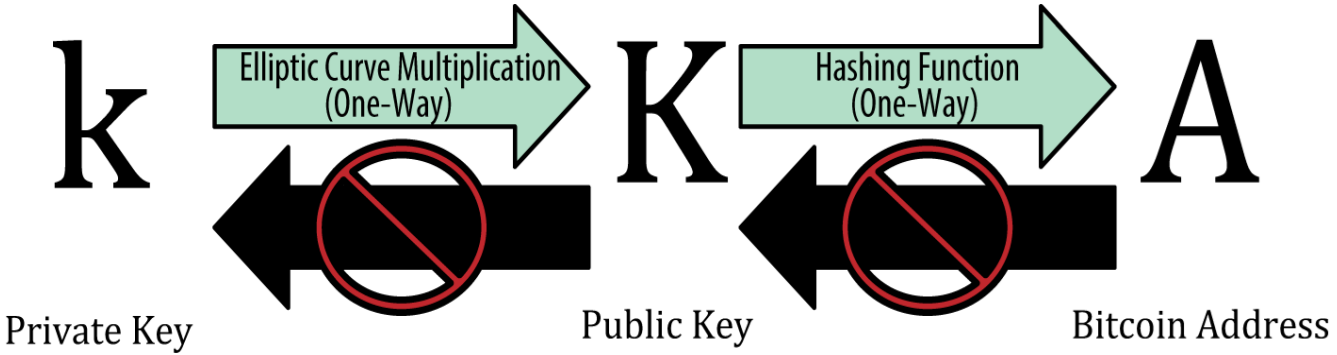
Кодировки BASE58 и BASE58CHECK

Алфавит Base64 состоит из 26 прописных букв, 26 заглавных букв, 10 цифр, и еще двух символов: "+" и "/". Формат кодирования Base58 разработан для использования в Биткойн и используется во многих других кирптовалютах. Base58—это Base64 без числа 0 (ноль), O (заглавная буква O), l (маленкая L), I (большая i), и символов "+" и "/". Таким образом алфавит Base58:

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

Криптографические хэш-функции

Криптографические хэш-функции



ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Криптографические хэш-функции

https://anders.com/blockchain/hash.html

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

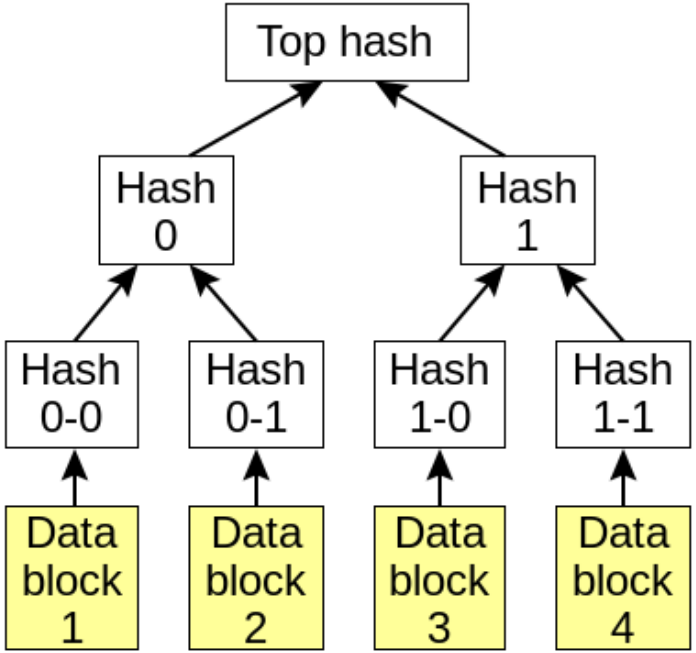
Corda

Примеры

Выводы

Дерево Merkle

Концепция была запатентована Ральфом Мерклом еще в 1979 году, а само дерево получило название дерево Меркла или хэш дерево. Используется для проверки целостности данных.

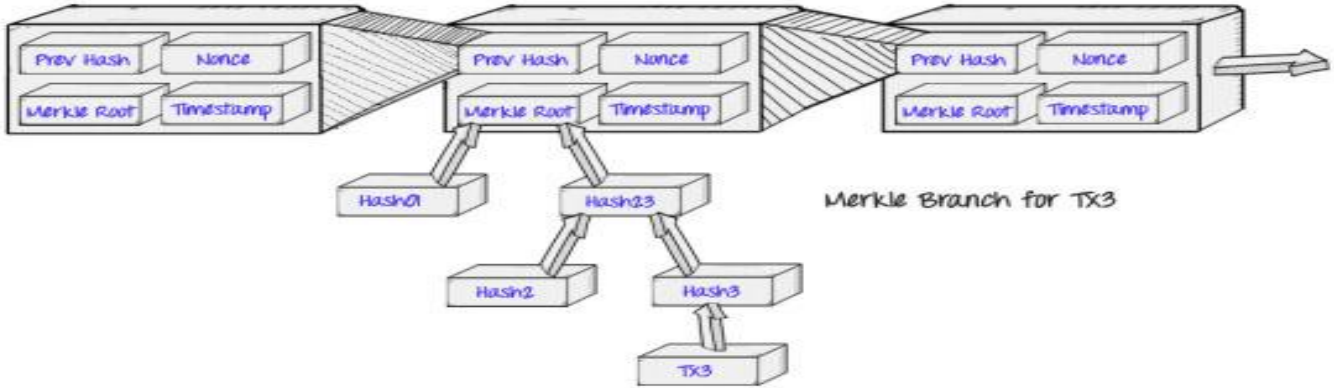


Доказательства Меркла в Биткойне

Сатоши Накамото использовал доказательства Меркла в Биткойне для сохранения сведений о транзакциях в блоках.

Эта схема используется для упрощенной верификации платежей (SPV): вместо того чтобы скачивать все транзакции и все блоки, «облегченный» клиент может скачать лишь цепочку заголовков блоков, каждый из которых содержит всего 80 байтов:

Если облегченный клиент захочет получить ту или иную транзакцию, он может запросить доказательство Меркла для соответствующей ветви, корень которой сохранен в блоке с этой транзакцией.



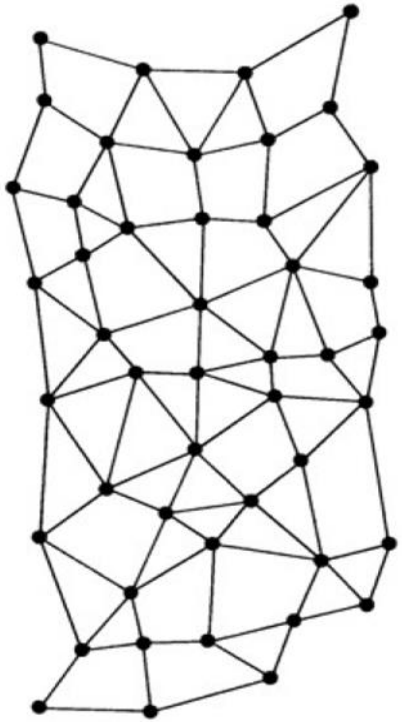
https://impgun.wordpress.com/2015/11/22/merkling-in-ethereum/

Эффективность дерева Меркле

Эффективность деревьев Меркле становится очевидной с увеличеием масштаба. В таблице показано количество данных, которые должны быть заменены на пути Меркле, для доказательства присутствия транзакции в блоке.

Количество транзакций	Приблизительный размер блока	Размер пути (в хэшах)	Размер пути (в байтах)
16 транзакций	4 килобайта	4 хэшей	128 байт
512 транзакций	128 килобайт	9 хэшей	288 байт
2048 транзакций	512 килобайт	11 хэшей	352 байт
65535 транзакций	16 мегабайт	16 хэшей	512 байт

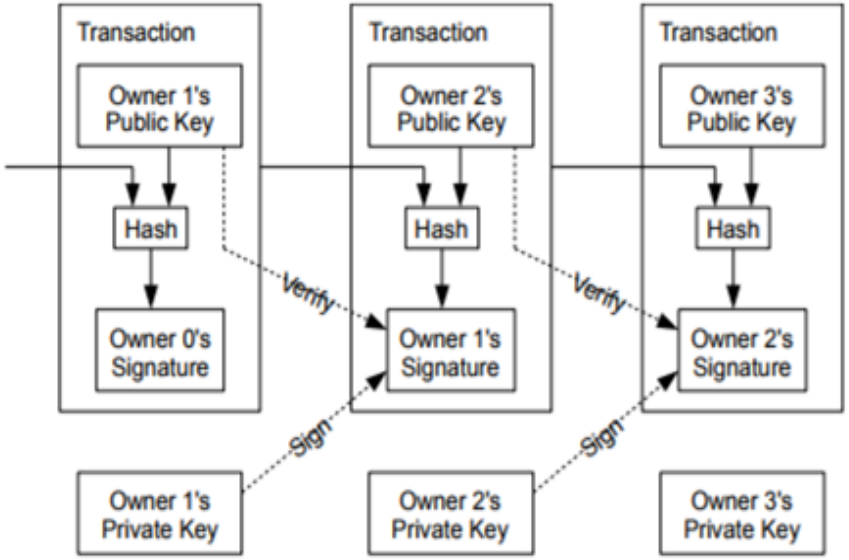
1



DISTRIBUTED
(C)

2 SHA256

3



ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Консенсус это

механизм выбора участника децентрализованной сети для совершения операции формирования нового блока, включение в его тело транзакций отправленных в децентрализованную сеть, включение нового блока в реестр и последующая дистрибуция копии базы данных всем участникам

Виды консенсуса

Proof-of-Work

Proof-of-Stake

Proof-of-Authority

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Proof-of-Work

Доказательство работы было «изобретено» задолго до биткойна еще в начале 90-х и применялось в ином контексте: для защиты от спама.

В случае доказательства работы хеш сообщения, объединенного со специальным полем (nonce), должен быть меньше определенного значения (или начинаться с определенного числа нулевых битов). Nonce не несет смысла для самого сообщения — это поле перебирается автором доказательства, пока не будет найдено подходящее значение. Название «доказательство работы» отражает тот факт, что для нахождения nonce надо совершить вычислительную работу, ожидаемое количество которой измеримо.

https://habr.com/company/bitfury/blog/327468/

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

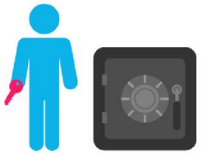
- Консенсус Накамото решает главный бич анонимных сетей — атаки Сибиллы, в которых злоумышленник создает кучу фейковых узлов, чтобы «задавить» получившимся большинством мнение честных пользователей. Чтобы обладать мнением в консенсусе Накамото, нужно обладать реальной вычислительной мощностью, которую нельзя подделать, и которая не требует никакой дополнительной аутентификации — она сама по себе привязывает узлы к реальному миру.
- Доказательство нельзя подделать и «перенести» на другие блоки. Таким образом, майнеры не могут воровать доказательства друг у друга.
- Более того, доказательства нельзя заготовить впрок — в каждый блок входит ссылка на предыдущий, поэтому начать работать над доказательством можно только после появления предыдущего блока в сети.
- Доказательства работы обеспечивают честность — награда каждого майнера пропорциональна его вычислительной мощности (хешрейту). Если у майнера есть 10% хешрейта от всей сети, то он будет в среднем создавать 10% блоков и получать 10% награды.
- Поскольку на создание доказательства тратятся реальные ресурсы (которые в случае биткойна измеряются тысячами долларов в минуту), у майнеров возникает совершенно новый стимул действовать в рамках протокола — нечестное поведение немедленно лишает их реальных денег.

https://habr.com/company/bitfury/blog/327468/

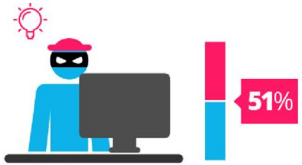
Blockgeeks

Proof-of-Work против Proof-of-Stake

Proof-of-Work требует дорогостоящих вычислений, также известных как майнинг

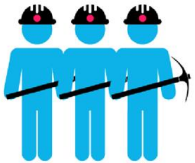


В системе Proof-of-Stake создатель нового блока выбирается системой заранее на основании его личного состояния, то есть доли в общем количестве криптовалюты.



Вознаграждение получает майнер, первым решивший математическую проблему, связанную с блоком

В системе PoS вознаграждение за блок отсутствует в принципе. Доход майнеров составляют исключительно комиссии с транзакций.



Майнеры в сети соревнуются между собой в поиске решений

Криптовалюты на базе Proof-of-Stake могут быть в тысячи раз более энергоэффективными

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Proof-of-Authority

Доказательство полномочий. Сгенерировать новый блок могут только те узлы, которые изначально имеют на это полномочия. Данный алгоритм находит своё применение в корпоративных и регулируемых монетах. О децентрализованности говорить не приходится, зато все блоки под контролем разработчика. Именно Proof-of-Authority можно ожидать в различных государственных криптовалютах.

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Поколения блокчейна

Блокчейн 1.0

bitcoin – исторически первый способ передачи данных при помощи blockchain. По этой причине он был определен в категорию блокчейн 1.0:

- создание следующих блоков путем математических вычислений (хэширование);
- майнинг как основа функционирования системы;
- блокчейн служит для транзакций криптовалюты

Поколения блокчейна

Блокчейн 2.0

децентрализованная платформа Ethereum поддерживает возможность создавать самоисполняющиеся контракты (смарт-контракты), которые будут работать по строго заданному алгоритму с четким выполнением всех условий.

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

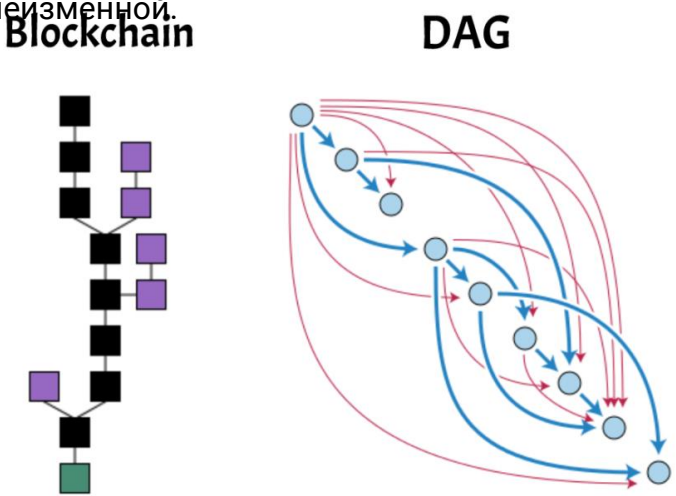
Выводы

Поколения блокчейна

Блокчейн 3.0

DAG (directed acyclic graph) – структура с топологическим деревом в основе. Блоки в этой структуре расположены не последовательно друг за другом, а могут идти от более ранних к поздним, но при этом подтверждать не одну, а несколько транзакций.

1. Система определяет родительские транзакции;
2. Затем система подписывает их хэши и включает в состав следующих переводов;
3. Формируется древовидная структура транзакций, где каждая будет считаться подтвержденной и неизменной.



ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

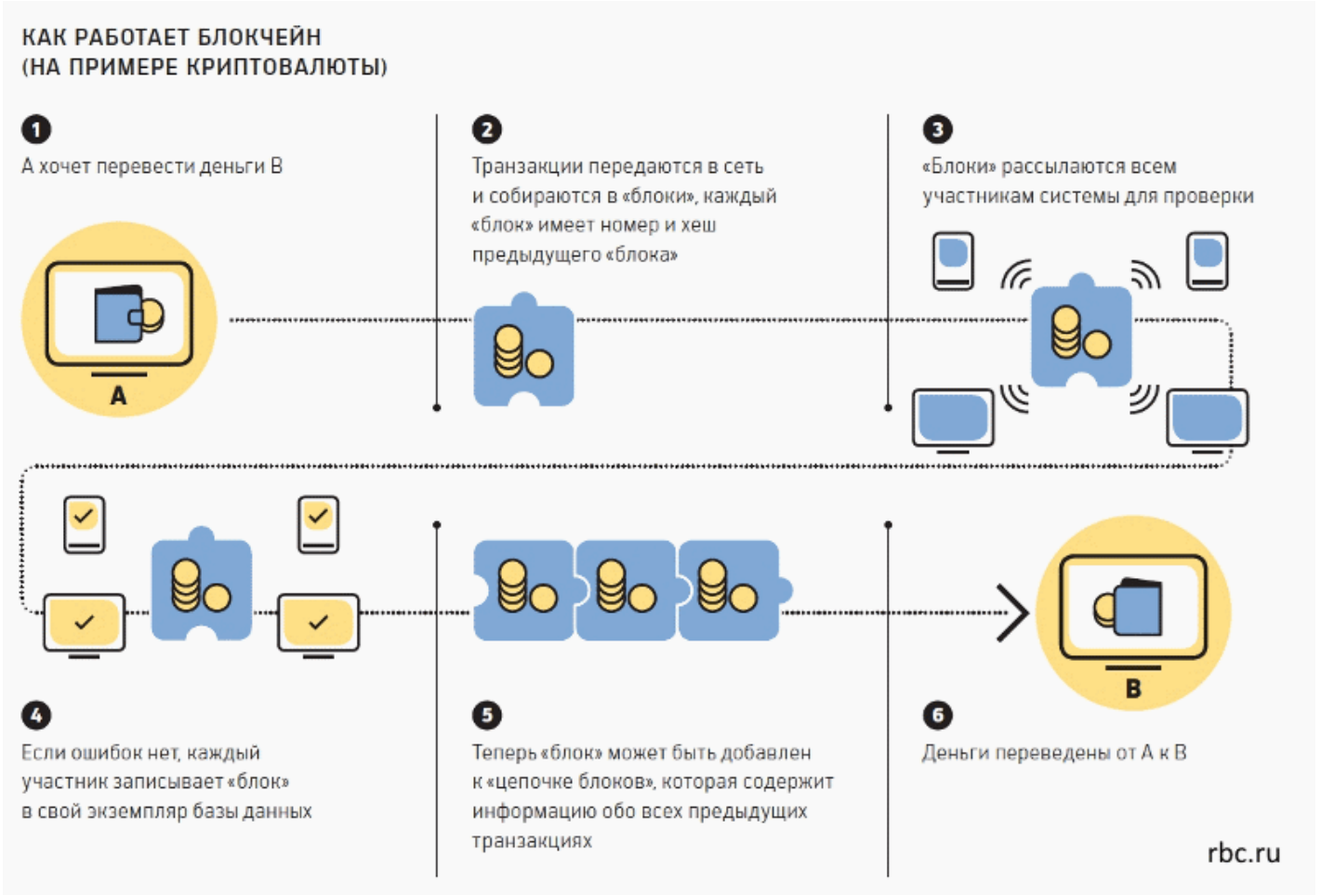
Hyperledger Fabric

Corda

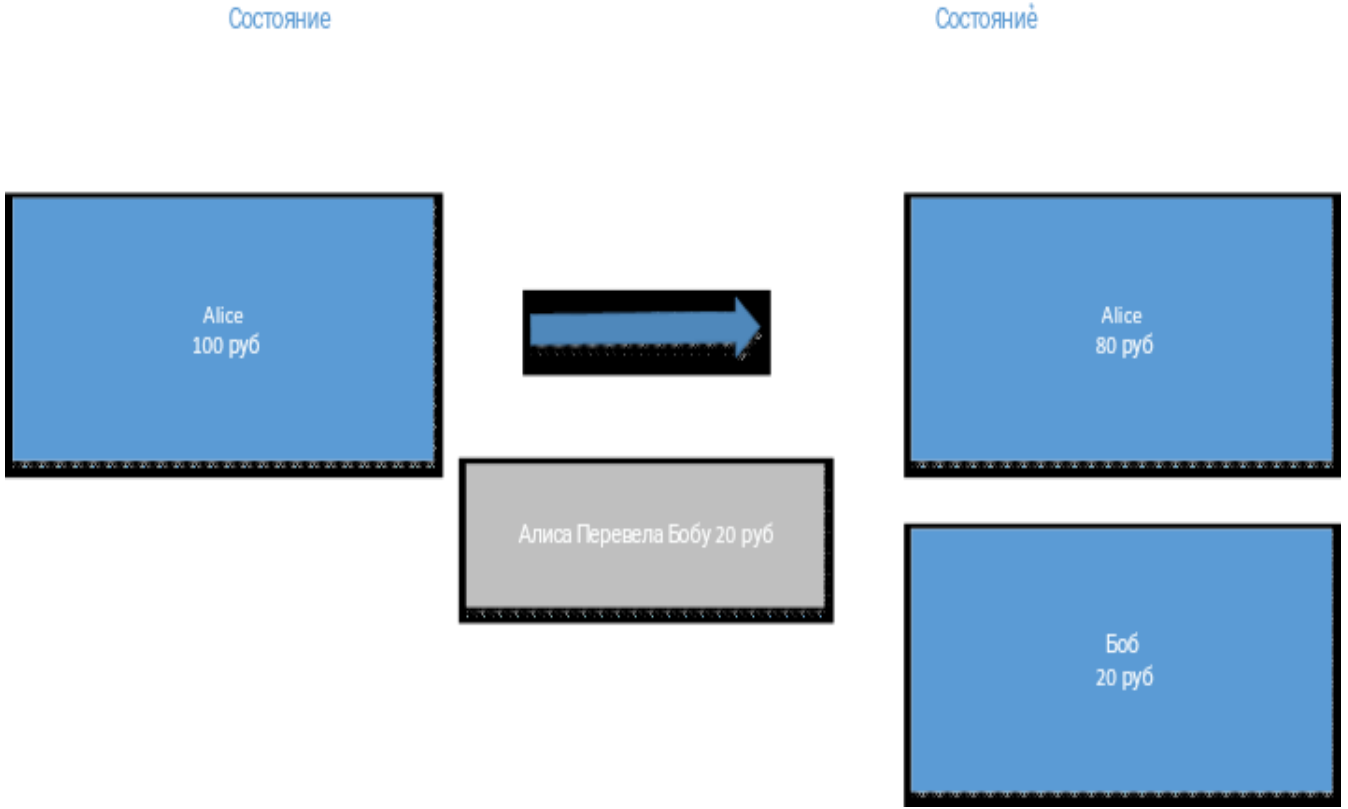
Примеры

Выводы

Криптовалюты



Транзакция


Состояние
Состояние
Alice
100 руб
Алиса Перевела Бобу 20 руб
Alice
80 руб
Боб
20 руб

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

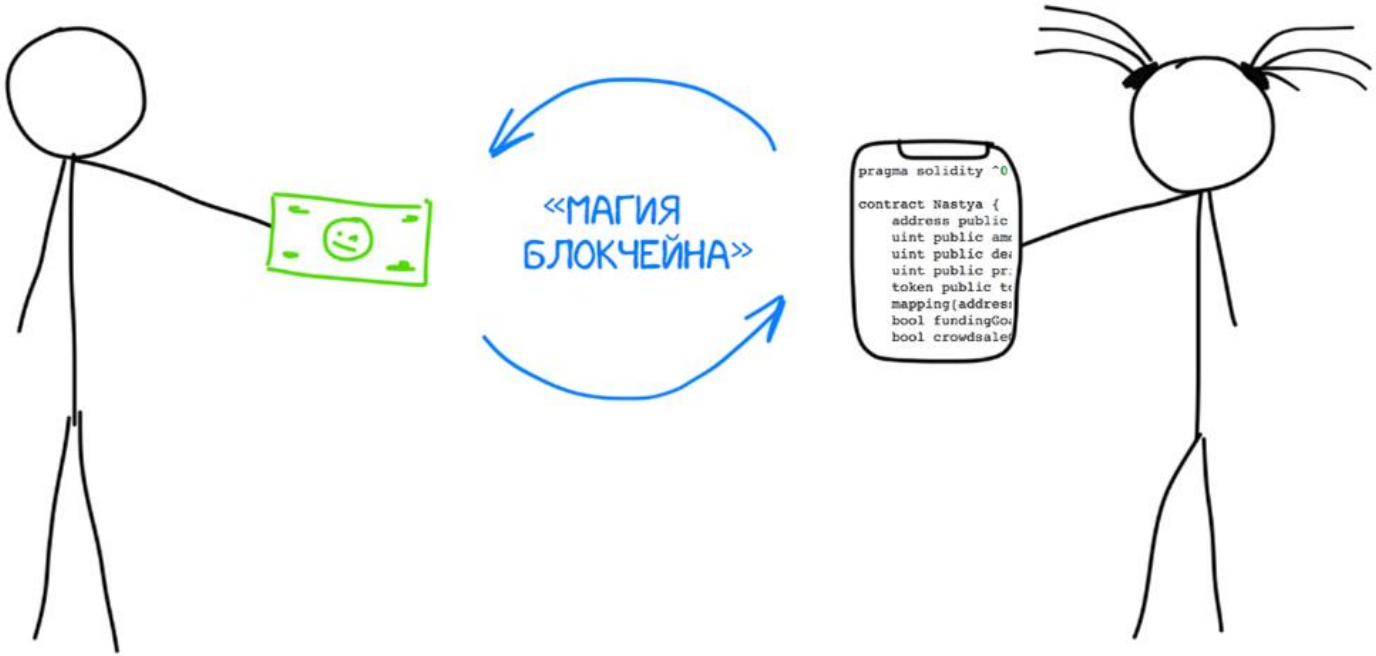
Hyperledger Fabric

Corda

Примеры

Выводы

“Умные” контракты



ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

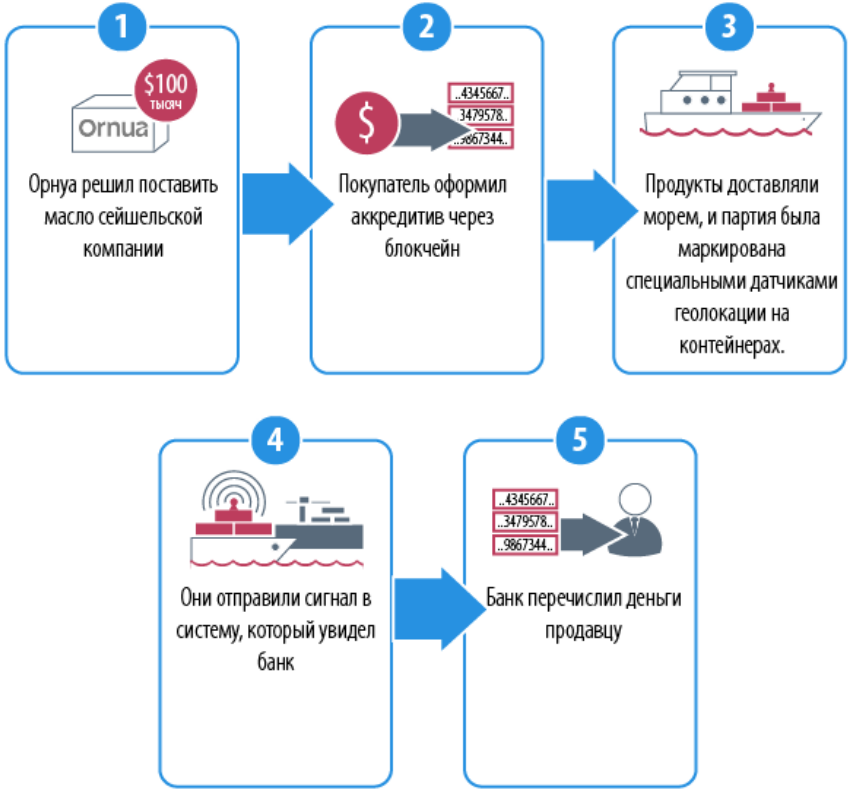
Hyperledger Fabric

Corda

Примеры

Выводы

“Умные” контракты



ПРАВО RU
www.pravo.ru

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

An Ontology for Smart Contracts

Darryl McAdams
Input Output Hong Kong
Email: darryl.mcadams@iohk.io

I. Introduction

This paper introduces a basic ontology that attempts to capture the essential features of many smart contracts, in order to aid in formal reasoning about their behavior. Section II gives a general overview of the proposed ontology, and Section III gives analyses of a number of interesting smart contracts from the literature, through the lens of this ontology. The proposals here are not intended to be the One True Ontology, but rather a useful ontology. A well-designed blockchain should be able to support arbitrary such ontologies.

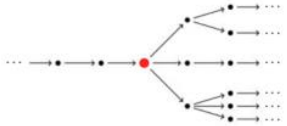


Fig. 1. Relationships between states. The present is larger and red. Arrows represent events that transition one state to another, creating a notion of time.

II. The Ontology

An ontology is a collection of concepts (or kinds, types) which are seen as the most fundamental way of viewing a problem domain, and the relationships that hold among them. In the context of particle physics, the ontology is the Standard Model of particles and the various associated fields.

In the context of smart contracts, a number of concepts arise over and over, which constitute this domain's ontology. This paper assumes that smart contracts fundamentally are stateful computations consisting of some state value which changes over time, and a fixed, unchanging transition function. Precisely what constitutes a state, and how many states there are, is entirely dependent on the smart contract, and might be as simple as a token representing a state in a finite state machine (e.g. q_3) or it might be some richer piece of symbolic data.

The ontology provides concepts for thinking about such contracts, abstracted over the details that are contract-specific or orthogonal to the macroscopic behavior, and are as follows:

Agent An Agent is a participant in a contract, whether that means a person, an organization, a piece of software, or something else. Agents take actions which affect the state of a contract.

Event An Event is a transition from one state to another. Events are brought about by Agents invoking the transition function on the most recent state.

Object An Object is something that is manipulated by a smart contract and may be transferred between Agents. Who can manipulate it and how is determined by the contract. Some Objects might have constraints on usage, such as who they can be transferred to (e.g. a "gift card" that can only be spent at certain retailers).

Time Time is the extrinsic notion of time, which passes at rates independent of the block chain. It is distinct from the internal before-after ordering that blockchains exist to creat. Time is calendar time.

Modality Modalities are higher-order phenomena that describe the relationships between states in the totality of what is logically possible. Modalities quantify over past or future states in relation to a given current state, and allow concepts of possibility, necessity, and so on. Modalities come in two main flavors:

Vertical A Vertical Modality quantifies over the alternative futures that are compatible with the given present state. Concepts like "must" and "may" are fundamentally vertical, because they describe only the existence, or not, of events of some kind. Something "must" occur if every future has that thing occurring, while it "may" occur if at least one future has it occurring.

Horizontal A Horizontal Modality, which may also be called a Temporal Modality, quantifies over sequences of states. Concepts like "eventually" and "never" are fundamentally horizontal because they describe the internal structure of alternative futures. Something "eventually" occurs if at some future, it occurs, but maybe only after many events have taken place. Something "never" occurs if there is no number of events after which it occurs.

The terminology "Vertical" and "Horizontal" come from visualization. We may imagine that a sequence of state transitions is like a time line laid out left to right, as in Figure 1. At any given state, there is a past extending to the left, and a variety of futures extending to the right. Each future is geometrically related to that state by being horizontally offset from it, but is vertically offset relative to other futures of that state. It may even be the case that a state has multiple pasts, as there may be multiple ways to have come to that state.

Some other things which are related to the ontology, but which are considered more fundamental in this paper, are notions like information, knowledge, identity, secrets, and verification. These are all related notions involving information theory and cryptographic protocols, and reasoning about them is extremely difficult. There is also a substantial literature on that subject already, which can provide a better set of tools than this paper could.

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

These apps run on a custom built **blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.**

This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk.

The project was bootstrapped via an ether presale in August 2014 by fans all around the world. It is developed by the Ethereum Foundation, a Swiss non-profit, with contributions from great minds across the globe.

On traditional server architectures, every application has to set up its own servers that run their own code in isolated silos, making sharing of data hard. If a single app is compromised or goes offline, many users and other apps are affected.

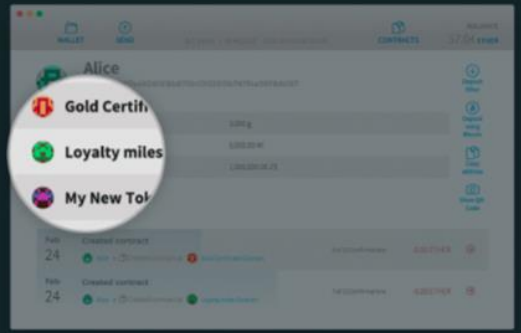
On a blockchain, anyone can set up a node that replicates the necessary data for all nodes to reach an agreement and be compensated by users and app developers. This allows user data to remain private and apps to be decentralized like the Internet was supposed to work.

Smart money, smart wallet

The **Ethereum Wallet** is a gateway to decentralized applications on the Ethereum blockchain. It allows you to hold and secure ether and other crypto-assets built on Ethereum, as well as write, deploy and use smart contracts.

DOWNLOAD
Ethereum Wallet for Linux

See all versions



Hold ether or any Ethereum-based token in safe wallets

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

7 недостатков Ethereum с точки зрения его создателя

1. Масштабируемость на дне; блокчейн по своей сути полностью полагается на критические точки, где отдельные узлы должны обрабатывать каждую отдельную транзакцию во всей сети.

2. PoW чрезвычайно дорого обходится и, кроме того, в своей основе подвержено атакам 51% “кемперов на респауне”, эффективных стратегий восстановления после которых не существует. Эгоистический майнинг становится выгодным на 25-33% хеш-мощностей, а атаки цензурирования 51% определённо выгодны.

3. Защита личных данных на дне.

4. Обычные пользователи не могут хранить большие объёмы эфира без риска их кражи или утери в случае кражи или утери приватного ключа.

5. Экономика не способствует “поддержанию чистоты в хранилищах”; недостаточные побудительные меры для очистки хранилищ и недостаточная плата за их заполнение, особенно в долгосрочной перспективе.

6. Куча различных мелких технических недостатков.
(много технических недочетов).

7. Обычным пользователям сложно понять, что контракты, с которыми они взаимодействуют, делают то, что они приказывают им делать, и не имеют случайных или вредоносных багов.

https://ttrcoin.com/7-nedostatkov-ethereum-s-tochki-zreniya-ego-sozdatelya.253/

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

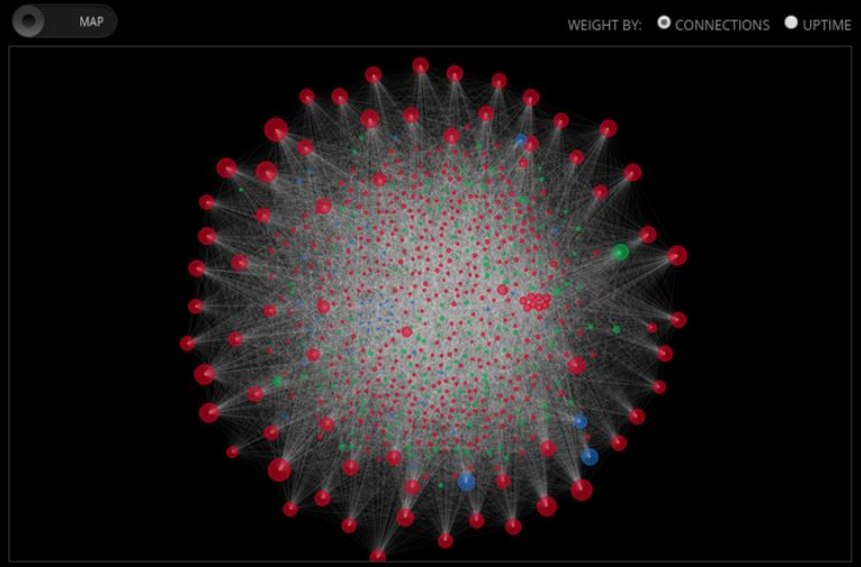
ripple

XRP CHARTS

Ripple Network Topology

Total Nodes: 676 Thu, May 24, 2018 1:16 AM

TypeError: Cannot read property 'replace' of undefined



Public Key	IP Address	Version
n9KPf6vyxVeUB14Mh6KRjjEKA2QkZFwE7bckPwmyGT8FSMkntHLs	34.229.211.180	rippled-0.90.0
n94p6BPKuQgwooq2HrkGNDLKp2whS6thp8wM35ikmMuN3S7ui1jX	52.15.66.195	rippled-0.90.0
n9LwVv4w65bw5cHm2UriGnnfj6Y1jfERXTmj3cVfVJDz2vbwEjLD	184.173.45.36	rippled-0.90.1
n9K6gh1AU85GVEVbL7gph7cYLQmp2mMsEYDhbpn6Tiiapcf6byLV	184.173.45.35	rippled-0.90.1
n94fxgvuVS9CYzx42rRdrrkj2kKnJUaSNavaqn5jgtqs49h7bZea	54.244.69.36	rippled-0.90.1
n9KzDjTURaG9sWnq3Y6H54sDPVWmKHoE6K4Gmo2Xu2GfNenjSx9m	174.37.225.45	rippled-0.90.1

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Факты о Ripple

- Ripple используется более чем 40 финансовыми организациями
- Транзакция в сети занимает 4 секунды
- Возможность отправки платежей одной валюте с получением в другой с автоматической конвертацией по наиболее выгодному курсу доступному среди контрагентов
- Поддержка переводов как в фиате так и в крипте
- Открытый API на базе которого было создано расширение для создание счет фактур
- Ripple заявляет, что может заменить SWIFT в ближайшем будущем

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Ripple 3 место по капитализации

https://coinmarketcap.com/

Cryptocurrencies ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$131,899,353,817	$7,735.42	$6,581,310,000	17,051,350 BTC	-2.77%	
2	Ethereum	$60,615,324,476	$608.41	$3,073,690,000	99,628,910 ETH	-5.20%	
3	Ripple	$24,279,556,973	$0.619535	$472,363,000	39,189,968,239 XRP *	-3.38%	
4	Bitcoin Cash	$17,875,213,641	$1,042.63	$873,836,000	17,144,350 BCH	-6.32%	
5	EOS	$9,957,651,517	$11.38	$1,628,210,000	875,259,433 EOS *	-6.63%	
6	Litecoin	$6,893,518,811	$121.64	$382,263,000	56,670,548 LTC	-4.49%	
7	Cardano	$5,507,739,449	$0.212432	$113,976,000	25,927,070,538 ADA *	-3.66%	
8	Stellar	$5,430,706,257	$0.292323	$41,613,300	18,577,759,043 XLM *	-0.89%	
9	TRON	$4,855,892,534	$0.073856	$606,639,000	65,748,111,645 TRX *	-2.37%	
10	IOTA	$4,252,820,310	$1.53	$87,891,900	2,779,530,283 MIOTA *	-5.57%	
11	NEO	$3,517,806,500	$54.12	$109,880,000	65,000,000 NEO *	-4.25%	

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Рост капитализации

https://coinmarketcap.com/

HYPERLEDGER FABRIC

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Hyperledger fabric

Предназначен для создания основы для разработки решений на блокчейне и основан на модульной архитектуре, где в случае необходимости могут быть подсоединены различные компоненты, например, алгоритм консенсуса. Умные контракты в Fabric называются chaincode. Сеть Hyperledger Fabric включает в себя «одноранговые узлы», которые выполняют блокчейн-код, данные регистров доступа, поддерживают транзакции и интерфейс приложений.

Fabric предназначена для проектов, в которых требуется технология распределенных регистров (DLT). Поддерживает chaincode в Go (Golang), Java и JavaScript (через Hyperledger Composer, или с версии 1.1) и, следовательно, потенциально более гибкий, чем язык смарт-контрактов.

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

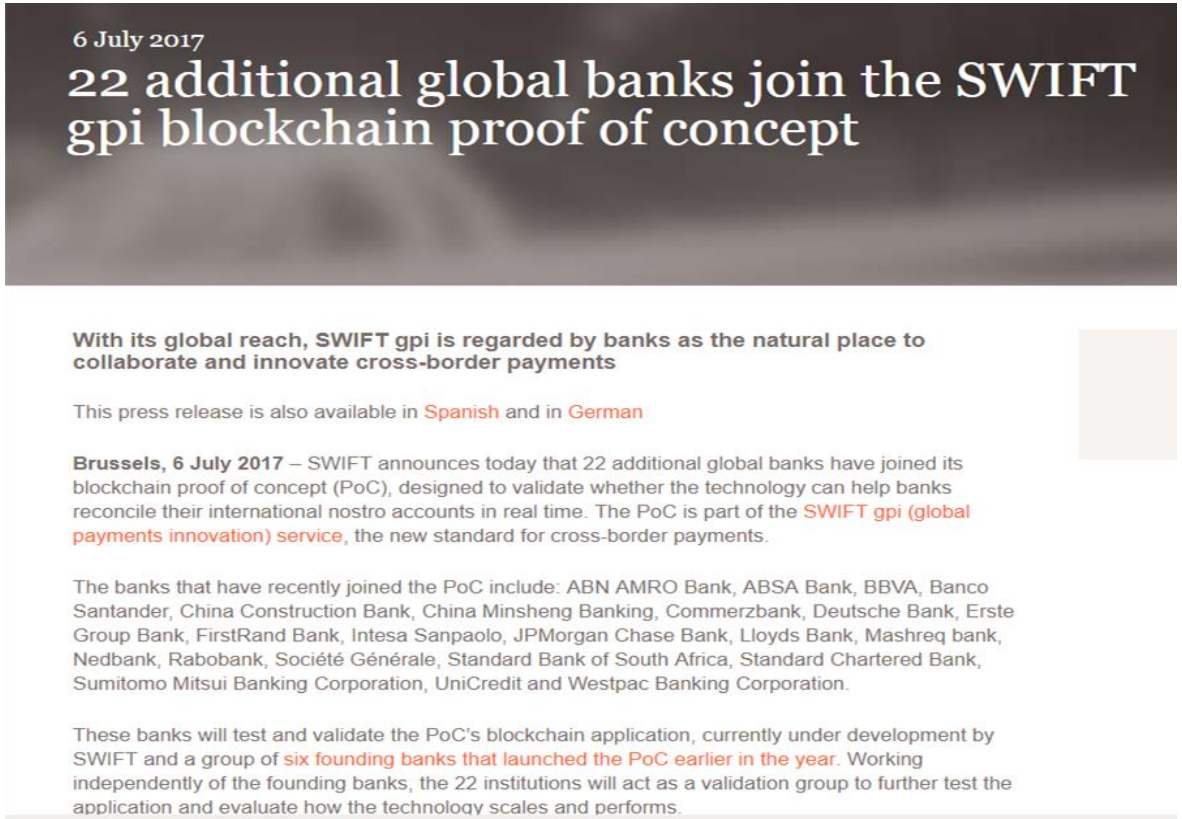
Hyperledger Fabric

Corda

Примеры

Выводы

PoC: SWIFT cgi with Hyperledger



6 July 2017

22 additional global banks join the SWIFT gpi blockchain proof of concept

With its global reach, SWIFT gpi is regarded by banks as the natural place to collaborate and innovate cross-border payments

This press release is also available in Spanish and in German

Brussels, 6 July 2017 – SWIFT announces today that 22 additional global banks have joined its blockchain proof of concept (PoC), designed to validate whether the technology can help banks reconcile their international nostro accounts in real time. The PoC is part of the SWIFT gpi (global payments innovation) service, the new standard for cross-border payments.

The banks that have recently joined the PoC include: ABN AMRO Bank, ABSA Bank, BBVA, Banco Santander, China Construction Bank, China Minsheng Banking, Commerzbank, Deutsche Bank, Erste Group Bank, FirstRand Bank, Intesa Sanpaolo, JPMorgan Chase Bank, Lloyds Bank, Mashreq bank, Nedbank, Rabobank, Société Générale, Standard Bank of South Africa, Standard Chartered Bank, Sumitomo Mitsui Banking Corporation, UniCredit and Westpac Banking Corporation.

These banks will test and validate the PoC's blockchain application, currently under development by SWIFT and a group of six founding banks that launched the PoC earlier in the year. Working independently of the founding banks, the 22 institutions will act as a validation group to further test the application and evaluate how the technology scales and performs.

https://www.coindesk.com/swift-selects-hyperledger-tech-cross-border-blockchain-test/
https://www.swift.com/news-events/press-releases/22-additional-global-banks-join-the-swift-gpi-blockchain-proof-of-concept

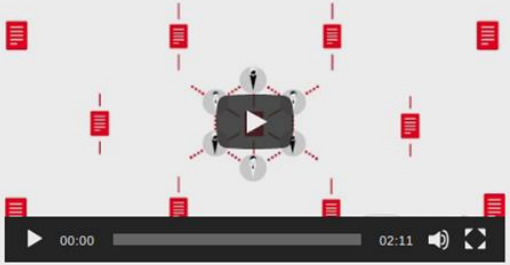
ВТБ

- Введение
- Bitcoin
- Консенсус
- Криптовалюты
- Смарт-контракты
- Ethereum
- Ripple
- Hyperledger Fabric
- **Corda**
- Примеры
- Выводы

c·rda

Discover Develop Community Blog

c·rda



Blockchain. Open for business.

Corda is an open source blockchain project, designed for business from the start. Only Corda allows you to build interoperable blockchain networks that transact in strict privacy. Corda's smart contract technology allows businesses to transact directly, with value.

Discover	Develop	News
Read the updated intro white paper	Download the DemoBench	Subscribe to the announce mailing list
Read the technical white paper	Hello, World!	Join the office hours
Read the Corda introduction	Subscribe to the dev mailing list	Check out content from CordaCon Tokyo

ВТБ

Введение
Bitcoin
Консенсус
Криптовалюты
Смарт-контракты
Ethereum
Ripple
Hyperledger Fabric
Corda
Примеры
Выводы

Corda представляет собой платформу на основе блокчейна Ethereum с ограниченным доступом, использующую JVM смарт-контракты и предназначенную для использования исключительно финансовыми учреждениями. Это децентрализованная база данных или распределенный реестр.

Ключевой особенностью Corda является то, что платформа не использует блокчейн. Вместо этого применяются специальные нотариальные ноды. Стоит обратить внимание и на то, что Corda не использует концепцию майнинга и систему Proof-of-Work.

Corda является единственной платформой, поддерживающей множество различных алгоритмов консенсуса, взаимно совместимых друг с другом и внутренними правилами сети.

https://forklog.com/obzor-platformy-corda-nody-smart-kontrakty-i-otsutstvie-blokchejna/

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Транзакции, которые совершаются в платформе Corda, не транслируются всем ее участникам. Записи доступны лишь тем участникам сети, которые обладают законным правом на их просмотр и управление. Таким образом, ноды “видят” транзакции, только если они имеют к ним отношение либо если эти транзакции взаимосвязаны с деятельностью ноды.

В данном случае нотариат представляет собой децентрализованный сервис, играющий ту же роль, что и майнеры в других блокчейн-системах. Т.е. нотариальные ноды подтверждают, что транзакция может быть принята и пропущена дальше. Также нотариат используется для создания меток времени.

https://forklog.com/obzor-platformy-corda-nody-smart-kontrakty-i-otsutstvie-blokchejna/

Corda не блокчейн, но DLT

Finance

American Option
by R3
Options trading

Project Maison
by RBS, FCA, R3
Mortgages on blockchain

Project Ubin
by R3
RTGS with LSM

Letter of Credit
by R3
Trade Finance, Letter of Credit

Wildfire
by R3
Central bank digital cash

Utility

BlockOne IQ
by Thomson Reuters
Thomson Reuters Data Oracle

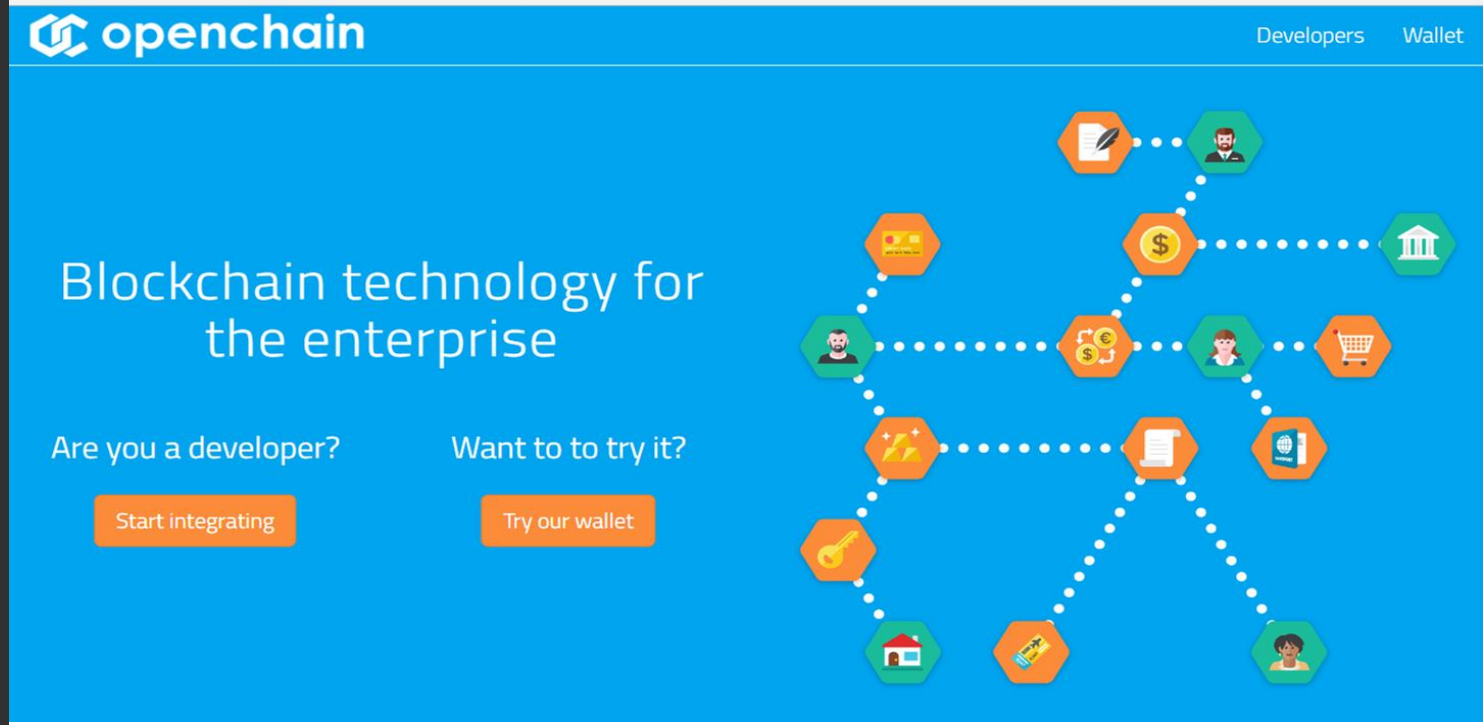
Oraclize
by Oraclize
Oracle service

File Transfer
by R3
FTP over blockchain

Yo!
by R3
Ping a Yo! to any peer

Whistle Blower
by R3
Anonymous whistleblowing

OpenChain


openchain
Developers
Wallet
Blockchain technology for the enterprise
Are you a developer?
Start integrating
Want to to try it?
Try our wallet

Сравнение платформ для построения блокчейн-сетей*

ДОМ РФ @BLOCKCHAINRF ТЕЛЕГРАМ-КАНАЛ

*На основе открытых источников

ethereum

Описание: Самый популярный проект в мире для создания публичных блокчейн-приложений. Работает глобальная сеть для создания решений, доступных во всем мире.

Целевая аудитория: создание **публичных** решений с открытыми данными.

Разработчики: Ethereum Foundation + большое открытое сообщество

Особенности: Самое большое сообщество разработчиков с высокой компетенцией по знанию платформы. Простота платформы. Смарт-контракты являются частью неизменной сети.

Модель сети: одноранговая сеть, все участники равны.

Подключение участников: любой может стать участником сети

Риски: риск получение контроля злоумышленником над всей сетью при достаточной мощности. Отсутствует контроль над списком участников. Обязательный майнинг. Ограничение на максимальную сложность логики смарт-контрактов.

Проекты:
1. Проект правительства Москвы «Активный гражданин»
2. Проект удаленной идентификации – IDChain (РосЕвроБанк, Microsoft)
3. Цифровой аккредитив (ВЭБ)
4. Проект по обмену реквизитами банков (банк «Открытие», банк «Ак Барк», Сбербанк, АФТ, ВТБ)
5. Факторинг. (М.Видео, Сбербанк)

Мастерчейн

Описание: Закрытая платформа на базе модификации протокола Ethereum, с доработками под законодательство РФ. ГОСТ шифрование.

Целевая аудитория: платформа для финансового сектора и коммерческих организаций, соответствует законодательству РФ.

Разработчики: Ассоциация ФинТех.

Особенности: ГОСТ подпись и шифрование (аттестация в 2018). Готовые и востребованные рынком ФинТех продукты по модели *As a Service*. Майнинг у ограниченных участников

Модель сети: одноранговая сеть с управляемым доступом.

Подключение участников: администратором сети.

Риски: Возможное отставание по версии, из-за необходимости получать обновлений от проекта Ethereum, в том числе, обновления безопасности. Закрытое развитие платформы. Обязательный майнинг. Ограничение на максимальную сложность логики смарт-контрактов.

Проекты:
1. Проект Электронная Закладная (децентрализованный депозитарный учет закладных) - Сбербанк, АФТ, АИЖК
2. Проект KYC (Know Your Customer) - Обмен информацией о физических лицах между участниками сети (Банк Открытие, АФТ)
3. Распределенный реестр цифровых банковских гарантий (ВТБ, АФТ)
4. Цифровой аккредитив (Альфа-Банк, АФТ)

HYPERLEDGER Fabric

Описание: Открытая платформа от мирового разработчика для организации коммерческих взаимодействий со строго регулируемым списком участников.

Целевая аудитория: коммерческий сектор. Ведение доверенных распределенных баз данных.

Разработчики: консорциум *Hyperledger*.

Особенности: Возможность настройки нескольких блокчейн - сетей, используя один клиент. Легкое обновление логики смарт-контрактов владельцем смарт-контрактов. Легкое администрирование списка участников сети через выдачу и отзыв сертификатов. Отсутствует майнинг. Гибкая балансировка нагрузки.

Модель сети: *многоролевая*: пользователи сети, администратор сети (УЦ); узлы – валидаторы операций над своей зоной ответственности (конкретные смарт-контракты, операции над конкретными сущностями в БД (акции, облигации, денежные переводы); обслуживающий сервис для снижения нагрузки на простых участников.

Подключение участников: через выдачу сертификатов удостоверяющим центром

Риски: низкая компетенция специалистов в РФ и малый размер сообщества.

Проекты:
1. Платформа по выпуску облигаций (НРД)
2. Системы дистанционного банковского обслуживания финансовых институтов (Сбербанк)

EXONUM

Описание: Открытый фреймворк, для разработки полноценных приложений с использованием распределенной БД.

Целевая аудитория: Для разработки публичных и частных сетей. С доработкой платформы под каждого заказчика.

Разработчики: компания BitFury.

Особенности: Гибкость в работе с внешними источниками данных. Позволяет создавать как публичные так и приватные решения. Контроль участников в сети через голосование. *Смарт-контракты* реализуются отдельно на каждом узле, в сети регистрируется описание смарт-контракта, условие для успешного выполнения контракта – идентичная реализация у большинства валидаторов. Отсутствует майнинг. Фиксация среза базы данных.

Модель сети: *многоролевая*: легкий клиент для удаленной работы с базой данных; полный клиент для хранения базы данных; ограниченная группа лиц, именуемые «узлы-валидаторы» для исполнения транзакций, контроля изменений в базе данных и контроля списка участников через голосование.

Подключение участников: методом голосования среди привилегированных участников сети.
Риски: Риск рассинхронизации версий клиента.

Проекты:
1. Проект ДДУ, взаимодействие Росреестр-Фонд(АИЖК)
2. Регистрация прав собственности (NAPR, Грузия)
3. Цифровой контракт (ВЭБ)
4. Третейская оговорка – прототип (Сбербанк)

corda

Описание: Платформа для обмена B2B сообщениями/уведомлениями для технической и юридической фиксации фактов в децентрализованной системе. Юридическая фиксация подкрепляется автоматическим созданием текстового договора и его подписанием юридически значимыми электронными подписями участников.

Целевая аудитория: участники финансового сектора, операции по учету активов, проведению финансовых сделок в закрытом канале.

Разработчики: консорциум R3: Консультанты: Barclays, Bank of America, HSBC, Citi, Royal bank of Canada и другие.

Особенности: Работа в формате утверждения фактов, а не в режиме базы данных. Содержание сообщений открываются только списку участников и, при необходимости, регулятору. При правильной работе формирует связи между созависимыми объектами. Высокая гибкость. Отсутствует майнинг.

Модель сети: *многоролевая*: *пользователи* сети, *пользователи*, подключаемые для выполнения разовой валидации, *оракулы* – узлы, ответственные за валидацию информации из внешней среды (курс валюты по ЦБ, мировое время и т.д.), *нотариусы* – необязательные участники сети, независимые валидаторы сети; администратор участников сети

Подключение участников: через выдачу сертификатов удостоверяющим центром

Риски: узконаправленность платформы: финансовый коммерческий сектор

Проекты: около 50 проектов
1. MarcoPolo для оптимизации торгового финансирования
2. HQLAx - биржа токенизации высоколиквидных активов

Особенности обеспечения процесса внедрения

- Необходимо разработать концепцию ролей и полномочий участников децентрализованной системы\сети
- Необходимо разработать механизм присоединения участников децентрализованной сети
- Необходимо урегулировать вопрос о владении децентрализованной сетью ее участниками
- Необходимо разработать методологию описания, трансформации бизнес процессов с учетом рисков и особенностей распределенных реестров
- Отсутствие рынка специалистов

Недостатки концепции децентрализации при продуктивной эксплуатации

- Отсутствие единой точки входа для конечного пользователя в части разрешения инцидентов. – деньги перевел в неправильное место
- Возможность выбора альтернативной цепочки записи распределенного реестра путем проведения процедуры hard fork.
- Риск невозможности достижения консенсуса среди участников децентрализованной сети после возникновения альтернативной цепочки блоков.
- Открыт вопрос о горизонтальной (растет объем информации) и вертикальной (количество узлов) масштабируемости. См. исследование
- Уязвимости используемой криптографии – коллизии - генерация существующих хэшей

Недостатки протокола распределенных реестров

- Невозможность использовать разные реализации механизма консенсуса для выбранных задач
- Отсутствие полной, постоянно поддерживаемой имплементации интерфейсов на языках высокого уровня являющихся стандартом дефакто в финансовой сфере
- Возможность организации атак различного характера
- Трудности во встраивании криптографии ГОСТ в текущую имплементацию протокола
- Низкая производительность при росте количества участников децентрализованной сети
- Отсутствие унифицированного механизма интеграции с событиями из внешнего мира
- Огромное количество успешно эксплуатируемых возможных типов атак на децентрализованную сеть

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы

Свойства блокчейна

1. Публичность (Public Verifiability)
2. Прозрачность (Transparency)
3. Конфиденциальность (Privacy)
4. Целостность (Integrity)
5. Избыточность данных (Redundancy of data)
6. Защищенность (Trust Anchor)

*- Do you need a Blockchain? - Karl Wüst, Arthur Gervaisy, Department of Computer Science ETH Zurich, Switzerland

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

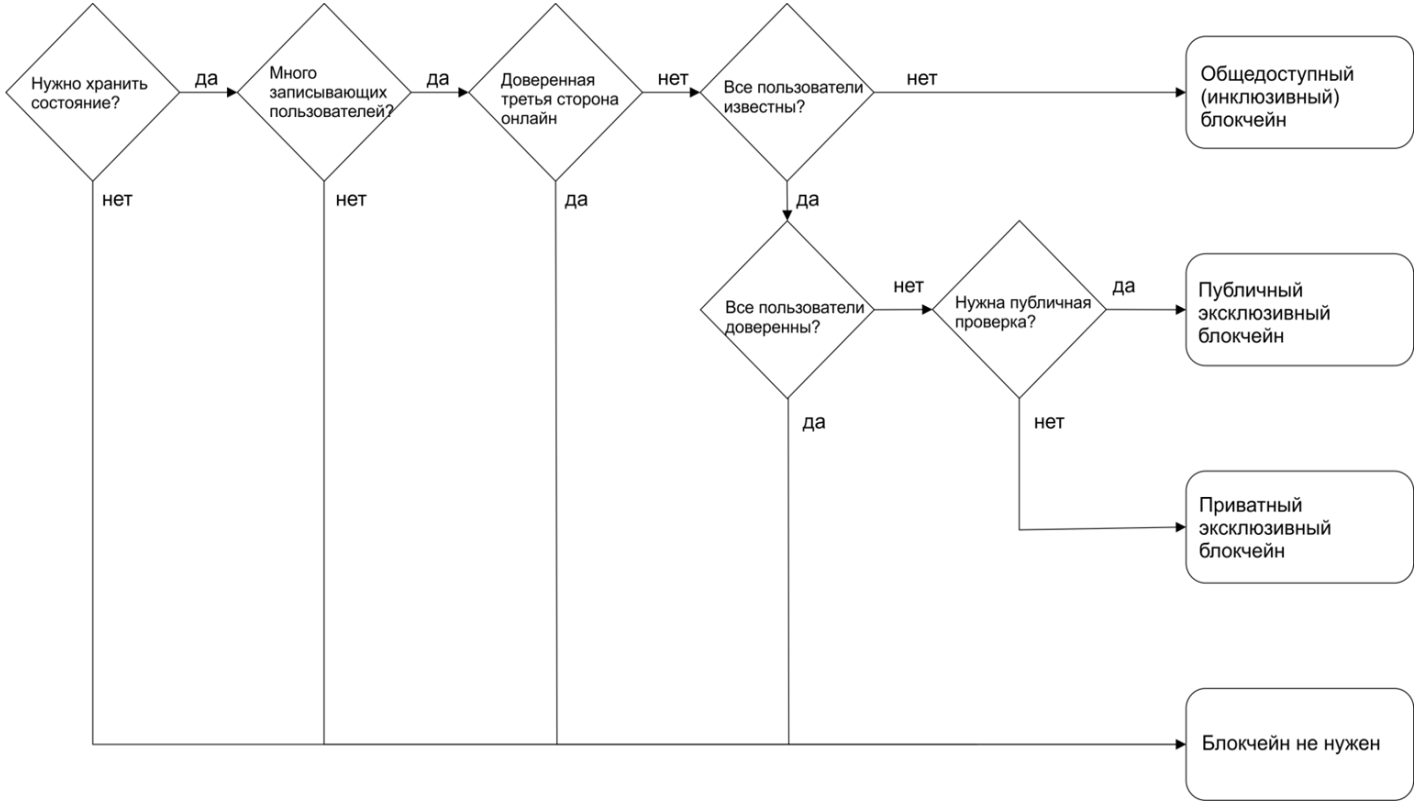
Hyperledger Fabric

Corda

Примеры

Выводы

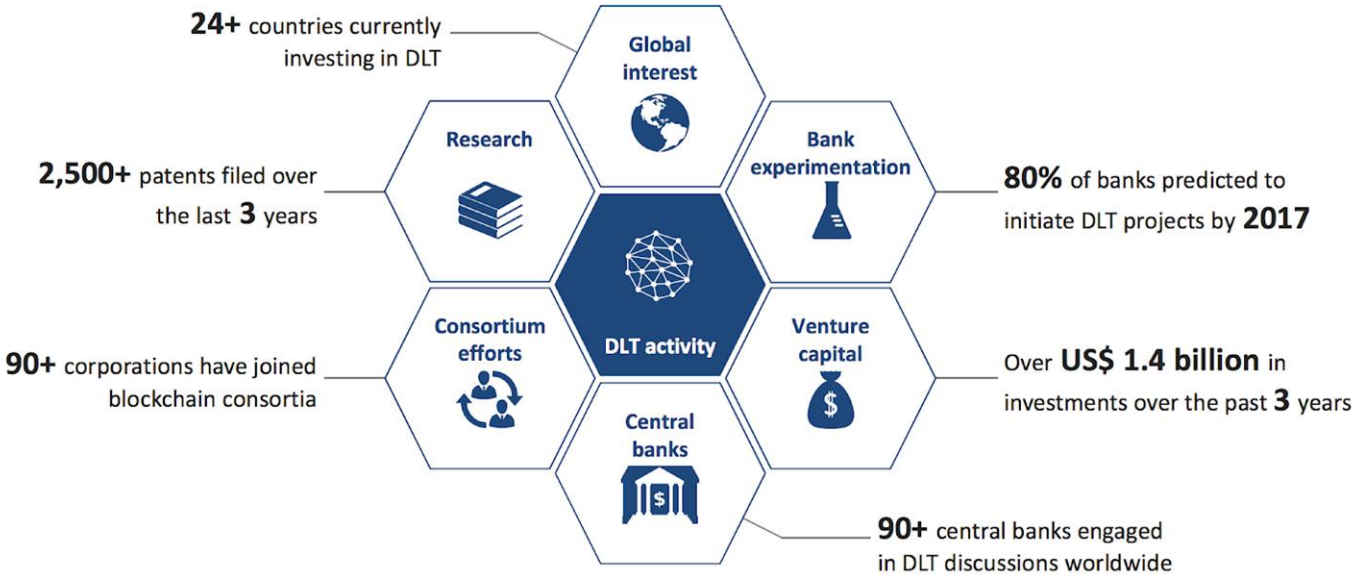
Критерии применения блокчейн



*- Do you need a Blockchain? - Karl Wüst, Arthur Gervaisy, Department of Computer Science ETH Zurich, Switzerland

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Distributed ledger technology (DLT), more commonly called “blockchain”, has captured the imaginations, and wallets, of the financial services ecosystem



Awareness of DLT has grown rapidly, but significant hurdles remain to large-scale implementation

- An uncertain and unharmonized regulatory environment
- Nascent collective standardization efforts
- An absence of formal legal frameworks

http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

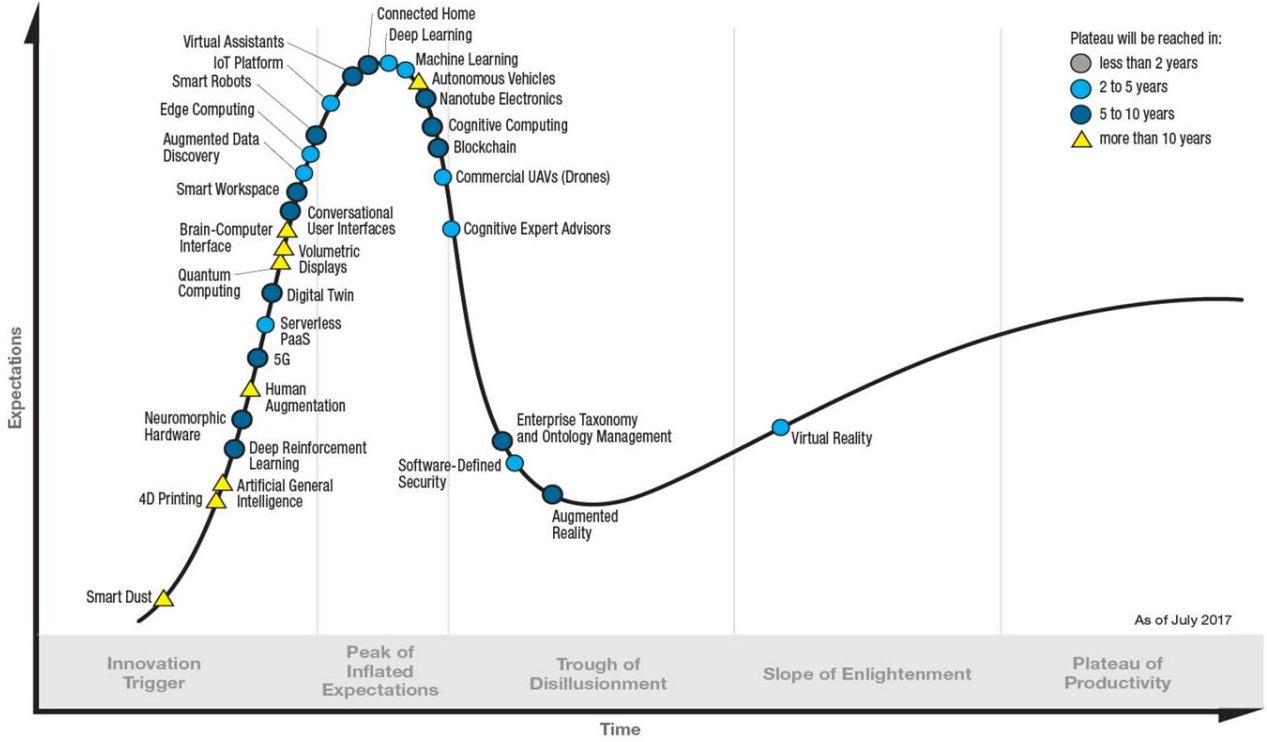
Hyperledger Fabric

Corda

Примеры

Выводы

Gartner Hype Cycle for Emerging Technologies, 2017



gartner.com/SmarterWithGartner

Source: Gartner (July 2017)

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

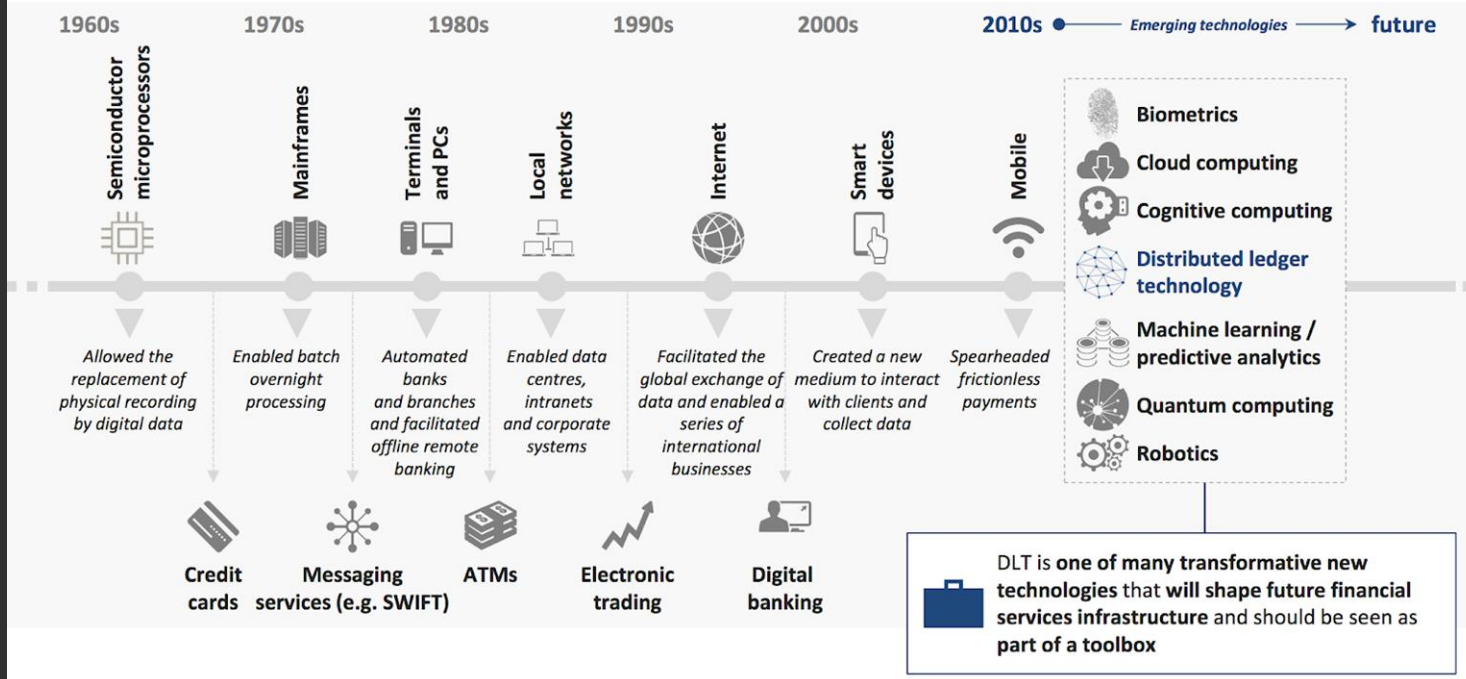
http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

2

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Distributed ledger technology is not a panacea; instead it should be viewed as one of many technologies that will form the foundation of next-generation financial services infrastructure

Over the last 50 years, technology innovation has been fundamental to financial services industry transformation. Today, multiple technologies poised to drive the next wave of financial services innovation are converging in maturity.



http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

ВТБ

Введение

Bitcoin

Консенсус

Криптовалюты

Смарт-контракты

Ethereum

Ripple

Hyperledger Fabric

Corda

Примеры

Выводы