

# Системный анализ технологии обмена и хранения данных блокчейн

Лабораторная работа №1 по ТСиСА  
“Формализация сложных систем”  
Астахов Сергей ИУ6-72Б



# Введение

Системный анализ — это научно-методологическая дисциплина, которая изучает принципы, методы и средства исследования сложных объектов посредством представления их в качестве систем и анализа этих систем.

При изучении сложного объекта главное внимание уделяется внешним связям объекта с другими системами, а не его детальной внутренней структуре, т.е. СА – это макроподход.

При изучении сложного объекта приоритет отдается его целям и функциям, из которых выводится структура (а не наоборот), т.е. СА – это функциональный подход.



# Рассматриваемая система

Рассматриваемая система - система хранения и обмена данными блокчейн.

Блокчейн - реестр децентрализованных данных, обмен которыми выполняется по безопасным каналам. В настоящей работе под блокчейном понимается также совокупность вспомогательных подсистем, позволяющих осуществлять взаимодействие с этим реестром.



# Цель рассматриваемой системы

Целью рассматриваемой системы является децентрализованное хранение и изменение данных, а также обеспечение верификации транзакций изменения этих данных.



# Свойства системы

- искусственная;
- сложная;
- распределенная;
- по реакции на возмущающие воздействия активная;
- статическая по степени изменчивости свойств.

# Структура системы (на примере Hyperledger Fabric)





# Подсистемы и их цели

Подсистема	Цель
Клиентское приложение	Хранение приватных ключей и подпись транзакций
Реестр	Хранение информации
Умный договор	Выполнение сложных операций с реестром
Узел эмуляции транзакций	Проверка соблюдения условий выполнения транзакций



## Подсистемы и их цели (продолжение)

Подсистема	Цель
Узел подтверждения транзакций	Подпись корректных транзакций узлом-валидатором
Служба управления членством	Регистрация в реестре новых пользовательских адресов
Служба упорядочивания запросов	Добавление транзакции в блок согласно алгоритму консенсуса





# Целевые показатели

- согласованность данных — во всех узлах в один момент времени данные не противоречат друг другу;
- доступность — любой запрос к системе завершается корректным откликом, однако без гарантии, что ответы всех узлов системы совпадают;
- устойчивость к разделению — расщепление системы на несколько изолированных секций не приводит к некорректности отклика от каждой из секций;
- надежность верификации транзакций.



## Факторы, влияющие на целевой показатель

- количество узлов в сети;
- тип и параметры используемого алгоритма консенсуса;
- быстродействие сетевой инфраструктуры;
- криптографическая стойкость используемых алгоритмов.



# Входные переменные

- количество выполняемых транзакций;
- вычислительная сложность транзакций;
- уровень противоречивости транзакций.



# Формальное описание системы

$$S = \langle \psi_a, \psi_b, P_0(\psi_a, \psi_b) \rangle$$

$S$  – система

$\psi_a$  – подмодель, определяющая поведение системы

$\psi_b$  – это подмодель, определяющая структуру системы, при её внутреннем рассмотрении

$P_0$  – предикат целостности, определяющий назначение системы, семантику моделей

$$\psi_a = \langle x, y, z, f, g \rangle$$

$x=x(t)$  – входной поток (набор предлагаемых транзакций)

$y=y(t)$  – выходной поток (набор событий + информация о цепочке блоков по запросу)

$z=z(t)$  – состояние модели (содержимое цепочки блоков)

$f, g$  – функционалы (глобальные уравнения системы), задающие текущие значения выходного сигнала  $y(t)$  и внутреннего состояния  $z(t)$ .



# Модель “Черного ящика”

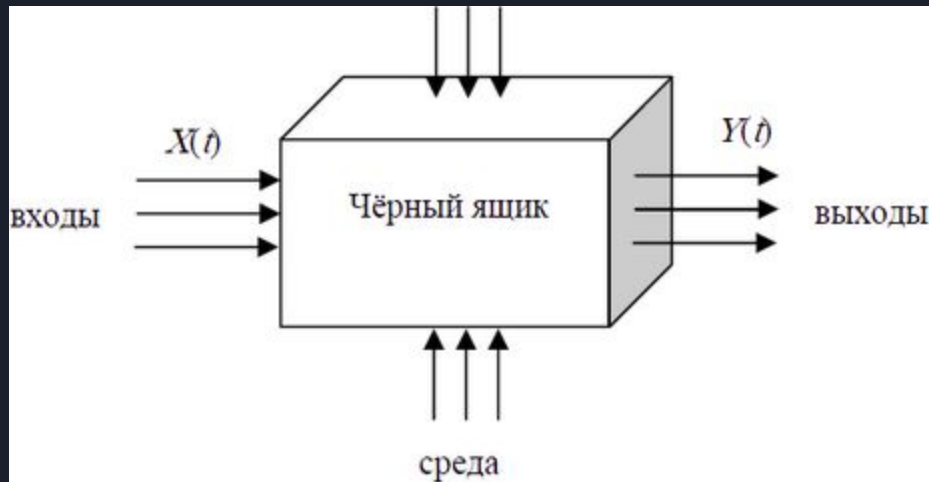
Черный ящик – термин, используемый для обозначения системы, внутреннее устройство и механизм работы которой очень сложны, неизвестны или неважны в рамках данной задачи.


Свойства ящика: целостность и обособленность от среды. Он обособлен, то есть выделен из среды, но не является полностью изолированным от нас, то есть ящик (система) связан со средой связями. Как среда действует на него, так и он действует на среду.

«Метод чёрного ящика» — метод исследования таких систем, когда вместо свойств и взаимосвязей составных частей системы, изучается реакция системы, как целого, на изменяющиеся условия.

# Модель “Черного ящика”

Так как внутренняя структура системы слишком сложна для формального описания, предлагается рассматривать систему в качестве черного ящика.



A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. The background of the entire slide is a dark navy blue with subtle, lighter blue diagonal stripes.

Спасибо за  
внимание