Технические аспекты информационных систем автоматизации голосования

Писковский Виктор Олегович, с.н.с., к.ф.-м.н., ВМК МГУ

Выполнено при поддержке РФФИ, проект № 18-29-16145

Требования к системе

- Традиционные требования к ИС
- Децентрализация хранения и учета
- Невозможность обоснованного подтверждения выбора
- Невозможность локального контроля выборами
- Проверка корректности учёта голосов
- Производительность

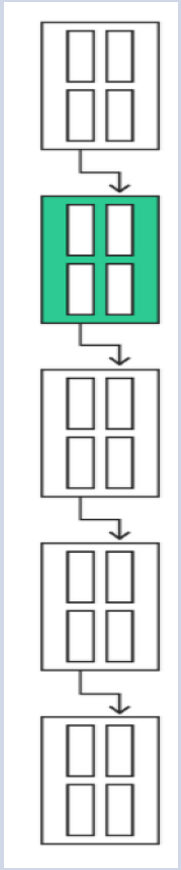
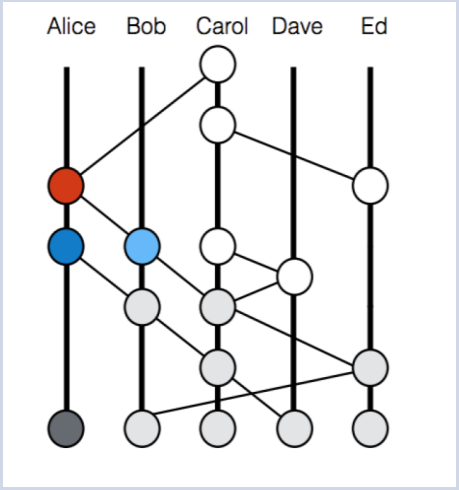
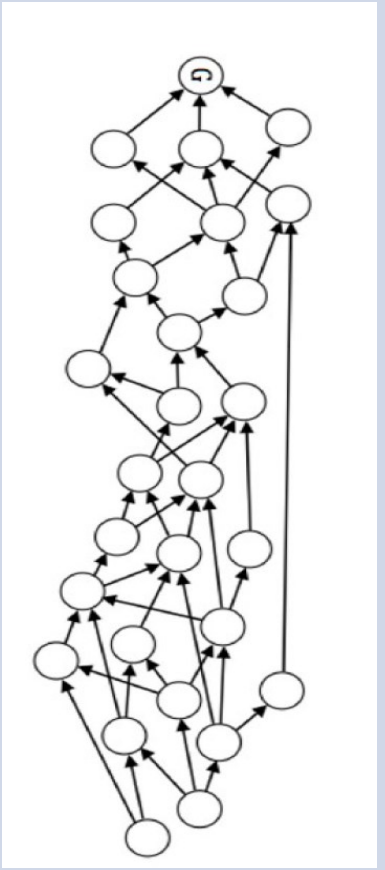
Хранение и учет

№ п.п	Модель DLT	Протокол достижения консенсуса	Производительность (TPS)	Примечание
1	BlockChain	Proof of Work (PoW)	10	Регулируется соглашением
2		Proof of Storage (PoSt)	100-200	
3		Proof of Stake (PoS)	100-200	
4		Byzantine Fault Tolerance (BFT)	1 тыс	Отдельные решения до 1 млн
5	HashGraph	Asynchronous BFT (ABFT)	250 - 350 тыс.	SWIFT-VISA (50 тыс. TPS)
6	DAG	BlockDAG/TxDAG	> 1 млн	

Модель DLT

Технология	Модель DLT	Комментарий
Связный список	Blockchain	Связный список вытянутых в цепочку блоков, связанных соотношением один к одному
Направленный ациклический граф	HashGraph	Каждый узел хранит свою историю "событий“. Протокол "слухов" (gossip protocol)
	blockDAG	Каждая вершина содержит набор транзакций (аналог блока). Каждый блок хеш-ориентирован на несколько родительских блоков
	txDAG	Каждая вершина содержит уникальную транзакцию. Ветви содержат непересекающиеся транзакции

Модели DLT

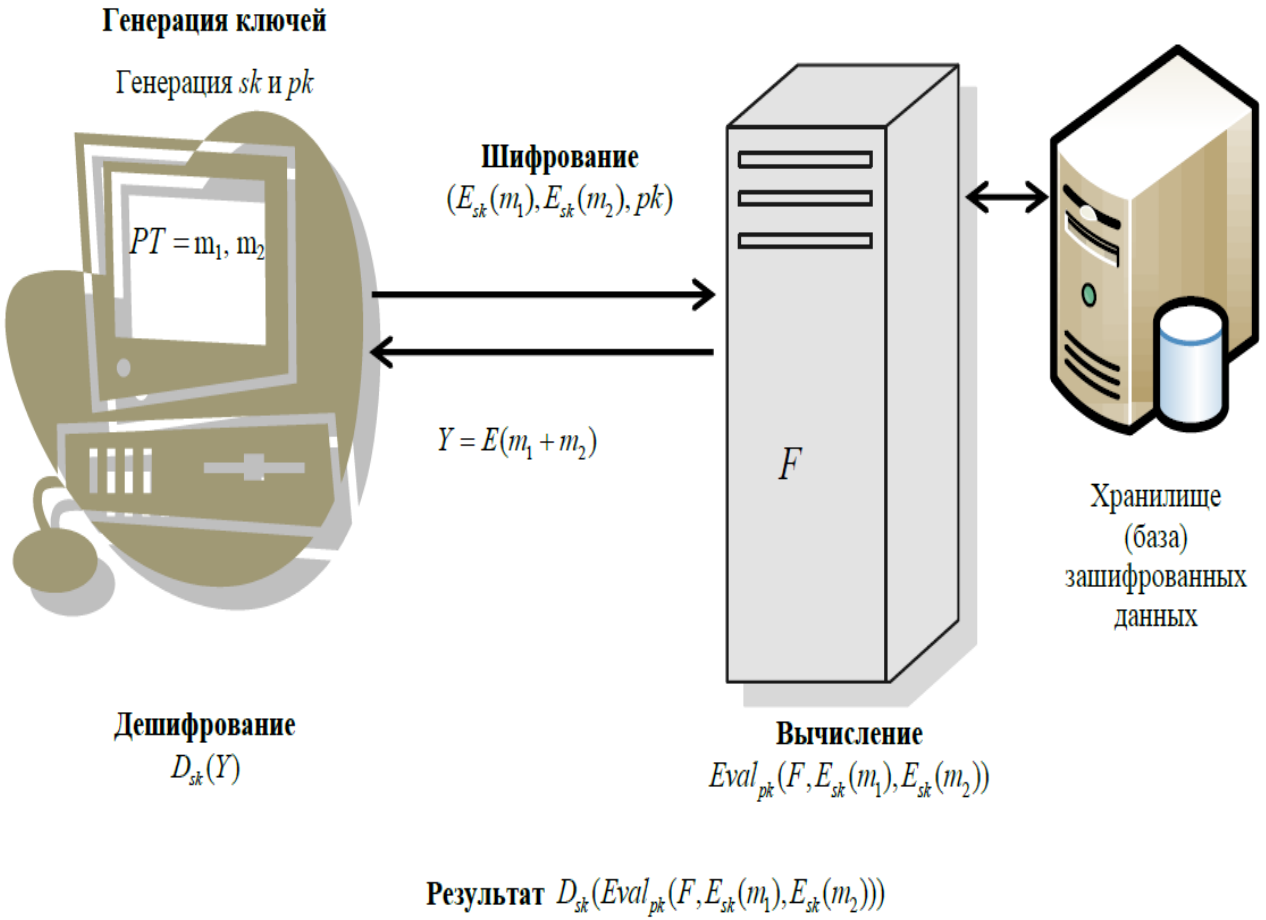
Blockchain	Hashgraph	DAG
		

https://cryptor.net/kriptovalyuty/different-types-of-dlts

Другие привлекаемые технологии

Технология	Назначение
Доказательство с нулевым разглашением	Возможность подтвердить факт голосования и не допустить возможности достоверно подтвердить сделанный выбор
Конфиденциальное вычисление	Интерактивное вычисления без предоставления к данным источников
Гомоморфное шифрование	Облачные вычисления без знания содержимого
Распределённая схема подписи	Независимость участников при постановке подписи, не интерактивный, асинхронный протокол выдачи проекций секретного ключа, не требует участия дилера. Для проверки достаточно наличия, порогового количества подписантов

Схема гомоморфного шифрования



А.И. Трубей. Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор) // Информатика. – 2015. – № 1.

Схема голосования Бенало

С криптосистемой, гомоморфной относительно сложения:

- Передача участникам открытого ключа системы
- Шифрование данных бюллетеня и отправка выборным представителям
- Агрегация зашифрованных данных без доступа к данным и передача в центр
- Финальная агрегация без доступа к данным и дешифрование полученных результатов

Josh Benaloh. Simple verifiable elections. In EVT, 2006.

Схемы голосования. E2E (Pret a Voter)