НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Факультет Компьютерных Наук
Департамент Программной Инженерии

Выпускная квалификационная работа

Криптографические алгоритмы и протоколы для распределенных реестров

Cryptographic Algorithms and Protocols for Distributed Ledgers

Выполнил: студент гр.БПИ151 Куприянов Кирилл
Научный руководитель: Профессор, руководитель ДПИ,
к.т.н. Авдошин Сергей Михайлович

2019

Предметная область

1. Распределённые реестры – “база данных”, которая распределена между несколькими сетевыми узлами или вычислительными устройствами. Каждый узел получает данные из других узлов и хранит полную копию реестра. Обновления узлов происходят независимо друг от друга

2. Криптография – наука, изучающая математические методы защиты информации, методы преобразования, обеспечивающие ее конфиденциальность и аутентичность.
Разделы: асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции

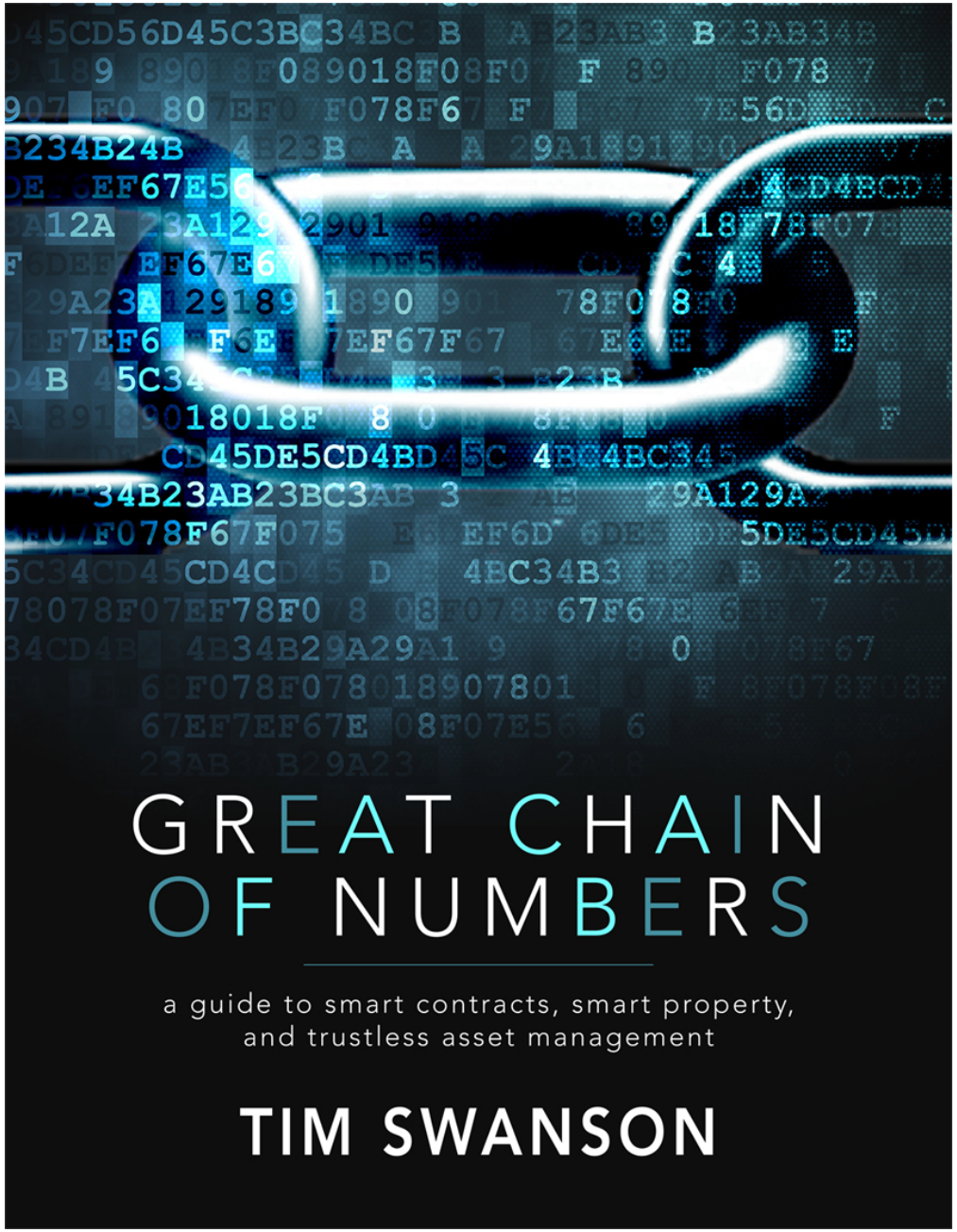


Рис. 1: Swanson, T., Great Chain of Numbers

II hekaj

Определения

- Распределённый реестр (Distributed Ledger) — Распределённая база данных между сетевыми узлами. Каждый из узлов может получать данные других, при этом храня полную копию реестра. Обновления этих узлов происходят независимо друг от друга
- Блокчейн — Постоянно растущий список записей, называемых блоками, которые связаны и защищены с помощью криптографии. Он копируется его пользователями и устойчив к модификации
- DAG — Направленный ациклический граф. Это ориентированный граф с данными, использующий топологическую сортировку (от ранних узлов к более поздним)
- Протокол консенсуса — стандарт, описывающий правила взаимодействия и способы достижения согласия в группе. Голосование происходит в пользу большинства, не учитывая интересы меньшинства, но с другой стороны, это гарантирует достижение соглашения, которое несет пользу всей группе

Оглавление ВКР

- Реферат **(95%)**
- Введение **(95%)**
- Глава 1. Обзор распределённых реестров **(95%)**
- Глава 2. Теоретический анализ алгоритмов и протоколов **(15%)**
- Глава 3. Реализация программной библиотеки **(0%)**
- Заключение **(80%)**
- Приложение А. Техническое задание **(95%)**
- Приложение Б. Руководство оператора **(0%)**
- Приложение В. Программа и методика испытаний **(0%)**
- Приложение Г. Текст программы **(0%)**

Обоснование актуальности работы

- Популярность темы (TON, IPFS)
- Устаревшая существующая классификация (на 2014 г.)
- Люди опираются на бизнес аналитику
- Отсутствие библиотеки с реализациями алгоритмов

Обоснование актуальности работы

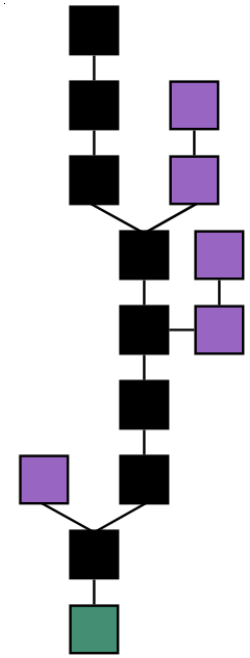


Рис. 2: Блокчейн

Рис. 3: Криптовалюты

Криптопротокол 2014г.

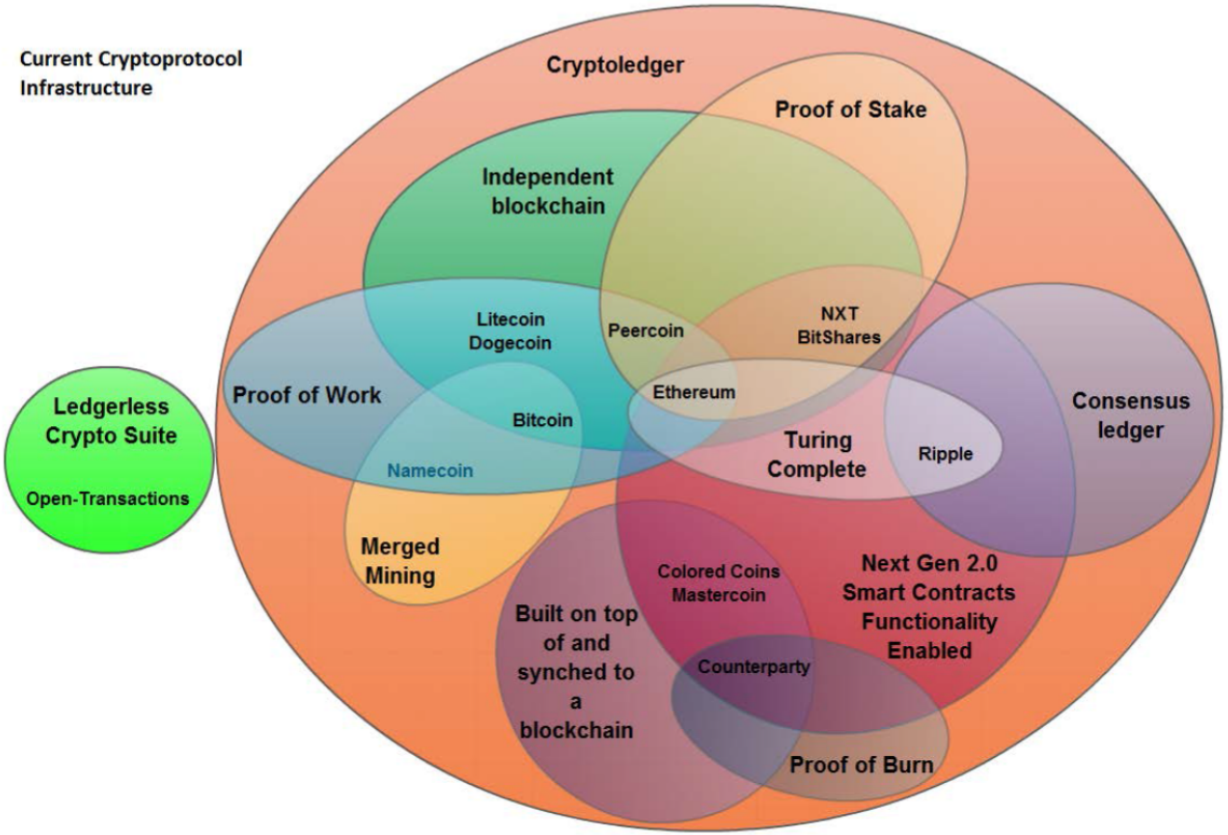


Рис. 4: Криптопротокол по состоянию на 2014 год [15]

Цель и задачи работы

Цель: Анализ и классификация актуальных криптографических алгоритмов для распределённых реестров в мире

Задачи:

- Выявить популярные распределённые реестры; выделить и изучить криптографические алгоритмы в них
- Изучить особенности реализации алгоритмов
- Расположить их на диаграмме Эйлера-Венна для создания новой классификации
- Написать библиотеку криптографических алгоритмов и протоколов

Распределённые реестры

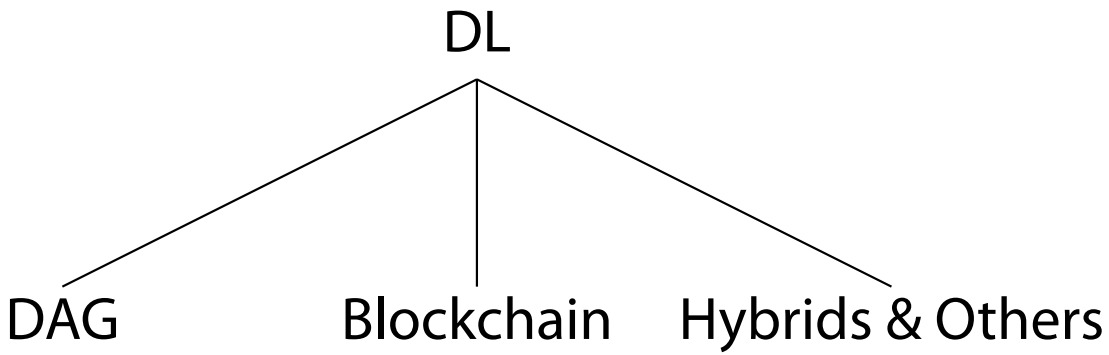


Рис. (5): Виды распределённых реестров

Классификация по открытости

Канада

- Public
- Private
- Consortium

Великобритания

- Permissioned private
- Permissioned public
- Unpermissioned public

Россия

- Public
- Private

Алгоритмы и протоколы

Протоколы консенсуса

- PoW
- PoS
- DPoS
- PoA
- PoWeight
- BFT

Алгоритмы хэширования

- SHA-256
- SHA-512
- Scrypt
- KECCAK-256
- Ethash
- X11
- X17
- Lyra2rev2
- myr-groestl
- blake2s

Алгоритмы генерации случайных чисел

- DRBG
- CPRNG

Существующая классификация криптопротоколов
На 2014 год

Задача: Расширение классификации

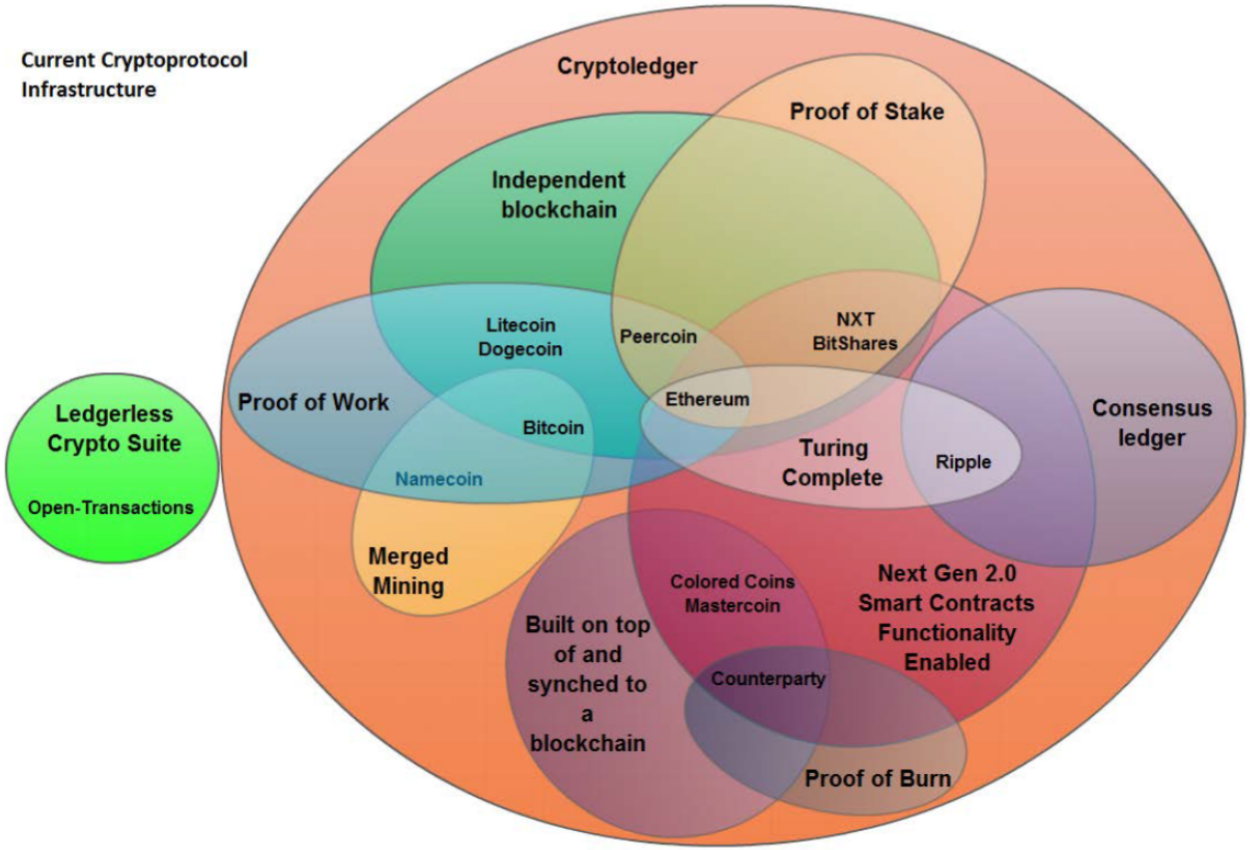


Рис. 6: Криптопротокол по состоянию на 2014 год [15]

Существующая классификация криптопротоколов*

На 2019 год

Результат: Расширенная классификация

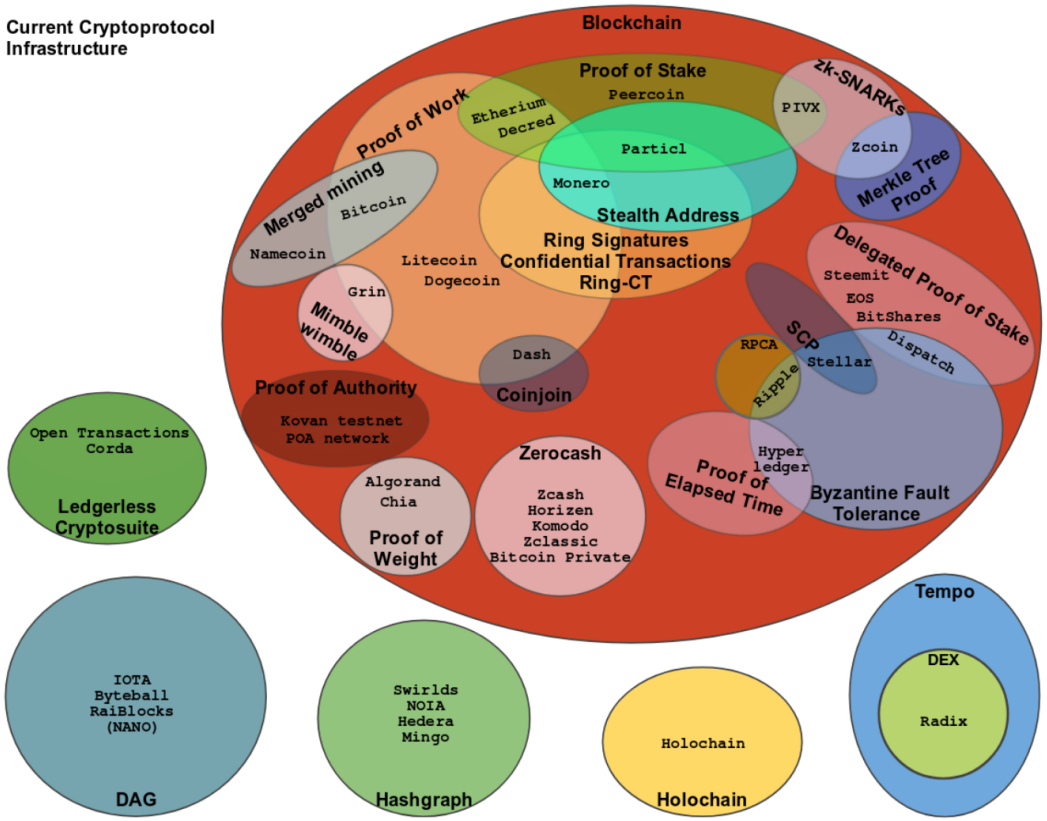


Рис. 7: Криптопротокол по состоянию на 2019 год*

*Альфа версия

Datapoints	Resources and History						
2518							
Coin	**Homepage**	**Announcement**	**Whitepaper**	**Block Explorer**	**Github**	**CMC**	**Founder(s)**
Bitcoin	https://bitcoin.o	https://bitcoin.org/bi	https://bitcoin.org	https://blockch	https://github.	https://coin	Satoshi Nakamoto
Ethereum	https://www.eth	https://bitcointalk.or	https://github.cor	https://etherscc	https://github.	https://coin	Vitalik Buterin
Monero	https://getmone	https://bitcointalk.or	https://cryptonote	https://minerga	https://github.	https://coin	thankful_for_today
Dash	https://www.das	https://bitcointalk.or	https://dashpay.a	https://chainz.(	https://github.	https://coin	Evan Duffield
ZCash	https://z.cash/_	https://blog.z.cash/l	not found	https://explorer	https://github.	https://coin	Zooko Wilcox
Verge	https://vergecur	https://bitcointalk.or	not found	https://verge-b	https://github.	https://coin	Justin "sunerok"
Bitcoin Private	https://btcprivat	https://bitcointalk.or	https://btcprivate	https://explorer	https://github.	https://coin	
Komodo	https://komodo	https://bitcointalk.or	https://komodopl	http://kmd.exp	https://github.	https://coin	James 'JL777' Lee
PIVX	https://pivx.org/	https://bitcointalk.or	https://pivx.org/w	http://www.pres	https://github.	https://coin	s3v3nh4cks
ZCoin	https://zcoin.io/	https://bitcointalk.or	https://zcoin.io/w	https://explorer	https://github.	https://coin	Poramin Insom
Particl	http://particl.io/	https://bitcointalk.or	https://github.cor	https://explorer	https://github.	https://coin	Ryno Mathee
Zencash	https://zensyst	https://bitcointalk.or	https://zencash.c	https://explorer	https://github.	https://coin	Rob Viglione and R
Groestlcoin	https://www.gro	https://bitcointalk.or	not found	http://groestlsi	https://github.	https://coin	
Nav-Coin	https://navcoin.	https://bitcointalk.or	https://cryptoratir	https://chainz.(	https://github.	https://coin	
ZClassic	http://zclassic.(	https://bitcointalk.or	https://zclassic.c	http://zcl-explo	https://github.	https://coin	HeyRhett
Bulwark	https://bulwarkc	https://bitcointalk.or	https://bulwarkcr	http://explorer.l	https://github.com/bulwark-crypto		
DeepOnion	https://deeponi	https://bitcointalk.org/index.php?topic		http://onionexp	https://github.	https://coin	
Phore	https://phore.io/	https://bitcointalk.or	https://phore.io/w	https://chainz.(	https://github.	https://coin	
Zoin	http://zoinoffici	https://bitcointalk.or	not found	http://explorer.:	https://github.	https://coin	
ColossusCoinXT	http://colossusc	https://bitcointalk.or	https://colossusc	https://chainz.(	https://github.	https://coin	
Spectrecoin	https://spectrep	https://bitcointalk.or	not found	https://chainz.(	https://github.	https://coin	
Sumokoin	https://www.sur	https://bitcointalk.or	https://cryptonote	https://explorer	https://github.	https://coin	Vu Quang

Рис. 8: Необходимые ресурсы для анализа

Алгоритмы

Сравнительный анализ

Bitcoin	Proof of Work	SHA256	n/a	1
Ethereum	Proof of Work	Ethash	n/a	Dynamic
Monero	Proof of Work	Cryptonight v7	n/a	Dynamic
Dash	Proof of Work	X11	n/a	2
ZCash	Proof of Work	Equihash	n/a	2
Verge	Proof of Work	Multiple, rotation	n/a	1
Bitcoin Private	Proof of Work	Equihash	n/a	2
Komodo	delayed Proof of	Equihash	n/a	2
PIVX	Zerocoin Proof o	SHA256	101	2
ZCoin	Proof of Work	Lyra2	n/a	1
Particl	Proof of Stake	PPoS	225	2
Zencash	Proof of Work	Equihash	n/a	2
GroestIcoin	Proof of Work	Grostl	n/a	1
Nav-Coin	Proof of Stake	SHA256	240	2
ZClassic	Proof of Work	Equihash	n/a	2
Bulwark	Proof of Stake	NIST5	101	1
DeepOnion	PoW/PoS Hybric	X13	1440	1
Phore	Proof of Stake	Quark	101	2
Zoin	Proof of Work	Lyra2Zoin	n/a	1
ColossusCoinXT	Proof of Stake	Quark	28800	1
Spectrecoin	Proof of Stake	Equihash	500	1
Sumokoin	Proof of Work	Cryptonite	n/a	Dynamic

Рис. 9: Алгоритмы хэширования, протоколы консенсуса и др.

Алгоритмы, обеспечивающие приватность

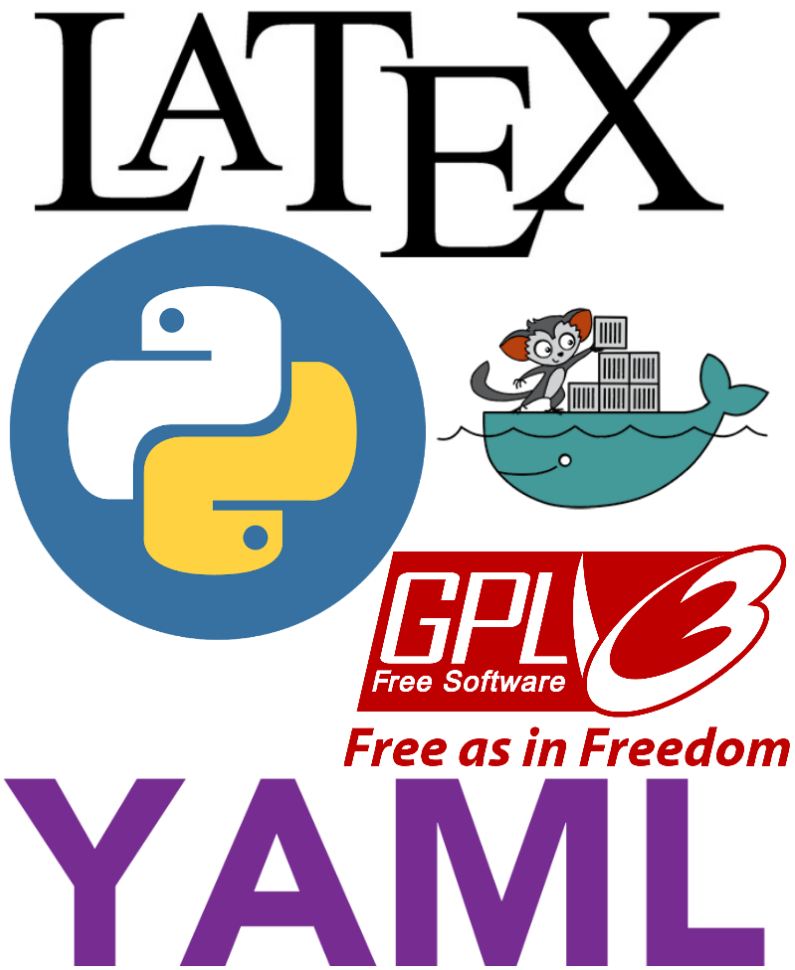
Сравнительный анализ

Coin	Privacy Choice Model	Cryptographic Privacy	Sender Privacy	Recipient Privacy	Hides Tx Amount	Tx Link Broken	Balances Visible
Bitcoin	n/a	No	No	No	No	No	Yes
Ethereum	n/a	No	No	No	No	No	Yes
Monero	default, partial opt-o	Cryptonote	Ring Signatures	RingCT/Stealth A	RingCT	No	No
Dash	opt-in	No	CoinJoin	No	Denominations	No	Yes
ZCash	opt-in	Zerocash	Zerocash	Zerocash	Zerocash	Yes	only T addresses
Verge	opt-in	No	No	Stealth Addresse	No	No	Yes
Bitcoin Private	opt-in	Zerocash	Zerocash	Zerocash	Zerocash	Yes	only T addresses
Komodo	opt-in	Zerocash	Zerocash	Zerocash	Zerocash	Yes	only T addresses
PIVX	optional	Zerocoin	Zerocoin	No	Denominations	Yes	only normal token
ZCoin	opt-in	Zerocoin	Zerocoin	No	Denominations	Yes	only normal token
Particl	opt-in	RingCT & CT	Ring Signatures	RingCT	CT	No	only public
Zencash	opt-in	Zerocash	Zerocash	Zerocash	Zerocash	Yes	only T addresses
GroestlCoin	opt-in	No	No	Stealth Addresse	No	No	Yes
Nav-Coin	opt-in	No	NavTech	No	No	Yes	Yes
ZClassic	opt-in	Zerocash	Zerocash	Zerocash	Zerocash	Yes	only T addresses
Bulwark	opt-in	No	CoinJoin	No	Denominations	No	Yes
DeepOnion	opt-in	No	No	Stealth Addresse	No	No	Yes
Phore	opt-in	Zerocoin	Zerocoin	No	Denominations	Yes	only normal token
Zoin	opt-in	Zerocoin	Zerocoin	No	Denominations	Yes	only normal token
ColossusCoinXT	opt-in	No	CoinJoin	No	Denominations	No	Yes
Spectrecoin	default, partial opt-o	Cryptonote	Ring Signatures	Stealth Addresse	No	No	Yes
Sumokoin	default, partial opt-o	Cryptonote	Ring Signatures	RingCT/Stealth A	RingCT	No	No

Рис. 10: Алгоритмы, обеспечивающие приватность

Методы, алгоритмы и технологии

- Сравнительный анализ алгоритмов и протоколов
- Язык Python 3.6.5
- LaTeX (дистрибутив XeTeX) для презентаций и текста
- YAML 1.2 как язык конфигурации библиотеки
- Лицензии на использование и распространение кодов



Сделано

- Исследовательская часть **(70%)**
- Программа **(80%)**
- Документация **(25%)**

#TODO

- Завершить классификацию
- Доработать полный обзор рассмотренных алгоритмов
- Проверить лицензии всех предполагаемых используемых кодов
- Добавить в программу генерацию кода (Python Metaprogramming)

Список используемых источников

[1] *Bitcoin Is Unsustainable*. URL: https://motherboard.vice.com/en%7B%5C_%7Dus/article/ae3p7e/bitcoin-is-unsustainable (дата обр. 23.04.2019).

[2] Sean Bowe и др. «ZEXE: Enabling decentralized private computation». В: (2019), с. 1—62. URL: https://eprint.iacr.org/2018/962.pdf.

[3] Crypto Ramble. *The Privacy Coin Guide Part 1 – Decentralize.Today*. URL: https://decentralize.today/the-privacy-coin-guide-part-1-520d61fc94f6 (дата обр. 22.04.2019).

[4] Cynthia Dwork и Moni Naor. «Pricing via Processing or Combatting Junk Mail». В: *Advances in Cryptology — CRYPTO' 92* (2007), с. 139—147. DOI: 10.1007/3-540-48071-4_10.

[5] Etherium. *TESTNET Kovan (KETH) Blockchain Explorer*. 2018. URL: https://kovan.etherscan.io/ (дата обр. 23.04.2019).

[6] Jens Groth и Markulf Kohlweiss. «One-out-of-many proofs: Or how to leak a secret and spend a coin». В: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9057 (2015), с. 253—280. ISSN: 16113349. DOI: 10.1007/978-3-662-46803-6_9.

[7] Leslie Lamport, Robert Shostak и Marshall Pease. «The Byzantine Generals Problem». В: *ACM Transactions on Programming Languages and Systems* 4.3 (2002), с. 382—401. ISSN: 01640925. DOI: 10.1145/357172.357176.

[8] Al C. de Leon и др. «Plastic Metal-Free Electric Motor by 3D Printing of Graphene-Polyamide Powder». В: *ACS Applied Energy Materials* 1.4 (2018), с. 1726—1733. ISSN: 2574-0962. DOI: 10.1021/acsaem.8b00240.

[9] Felix Konstantin Maurer и Martin Florian. «Anonymous CoinJoin Transactions with Arbitrary Values». В: ().

[10] Greg Maxwell. *Confidential Transactions*. 2015.

Список используемых источников

[11] Satoshi Nakamoto. «Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9.» В: *Journal for General Philosophy of Science* 1 (2008), с. 1—9. ISSN: 09254560. DOI: 10.1007/s10838-008-9062-0. arXiv: 43543534534v343453.

[12] Shen Noether, Adam Mackenzie и The Monero Research Lab. «Ring Confidential Transactions». В: *Ledger* 1 (2016), с. 1—18. DOI: 10.5195/ledger.2016.34.

[13] Andrew Poelstra. «Mimblewimble». В: 06 (2016), с. 1—19.

[14] Serguei Popov. «IOTA whitepaper v1.4.3». В: (2018), с. 1—28. ISSN: 0028-792X. URL: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1%7B%5C_%7D4%7B%5C_%7D3.pdf.

[15] Tim Swanson. *Great Chain of Numbers*. 2014. URL: https://www.scribd.com/document/210537698/Great-Chain-of-Numbers-a-Guide-to-Smart-Contracts-Smart-Property-and-Trustless-Asset-Management-Tim-Swanson (дата обр. 23.04.2019).

[16] Nicolas Van Saberhagen. «CryptoNote v 1.0». В: (2012), с. 1—16.

[17] Nicolas Van Saberhagen. «Monero: CryptoNote v 2.0». В: *White Paper* (2013), с. 1—20. URL: https://bytecoin.org/old/whitepaper.pdf%7B%5C%%7D0Ahttps://cryptonote.org/whitepaper.pdf.

[18] Vitalik Buterin. *On Public and Private Blockchains*. 2015. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (дата обр. 22.04.2019).

[19] Zerocoin Electric Coin Company. «ZCash». В: (2016), с. 1—56.

[20] Ольга Скоробогатова. *О российском консорциуме, национальной электронной валюте*. 2016. URL: https://bankir.ru/publikacii/20160419/olga-skorobogatova-o-rossiiskom-konsortsiume-natsionalnoi-elektronnoi-valyute-10007442/ (дата обр. 23.04.2019).

Спасибо за внимание!

Факультет Компьютерных Наук
Департамент Программной Инженерии

Выпускная квалификационная работа

Выполнил: студент гр.БПИ151 Куприянов Кирилл
Научный руководитель: Профессор, руководитель ДПИ,
к.т.н. Авдошин Сергей Михайлович

2019