



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

Популярность блокчейна

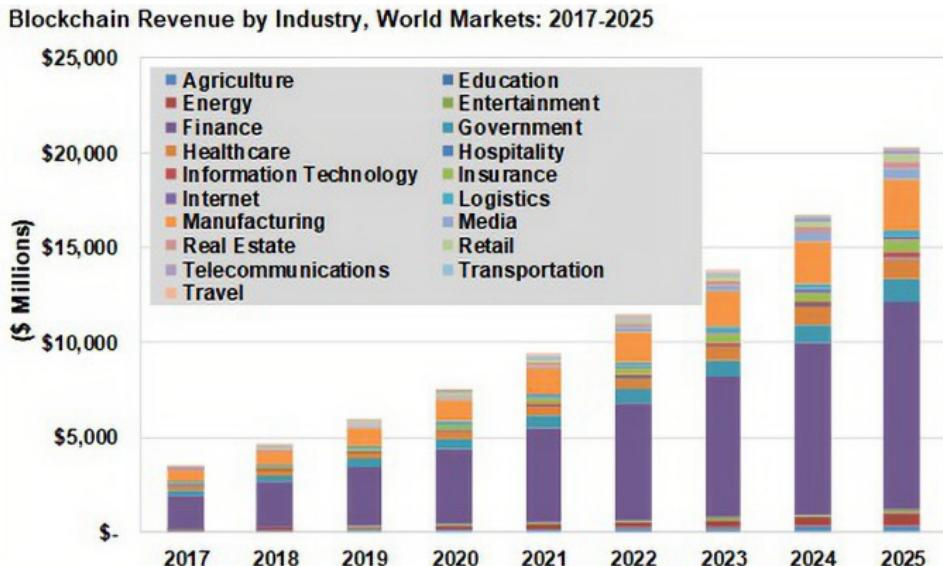


Рис. 1: Рост выручки в индустриях с применением блокчейна [22]

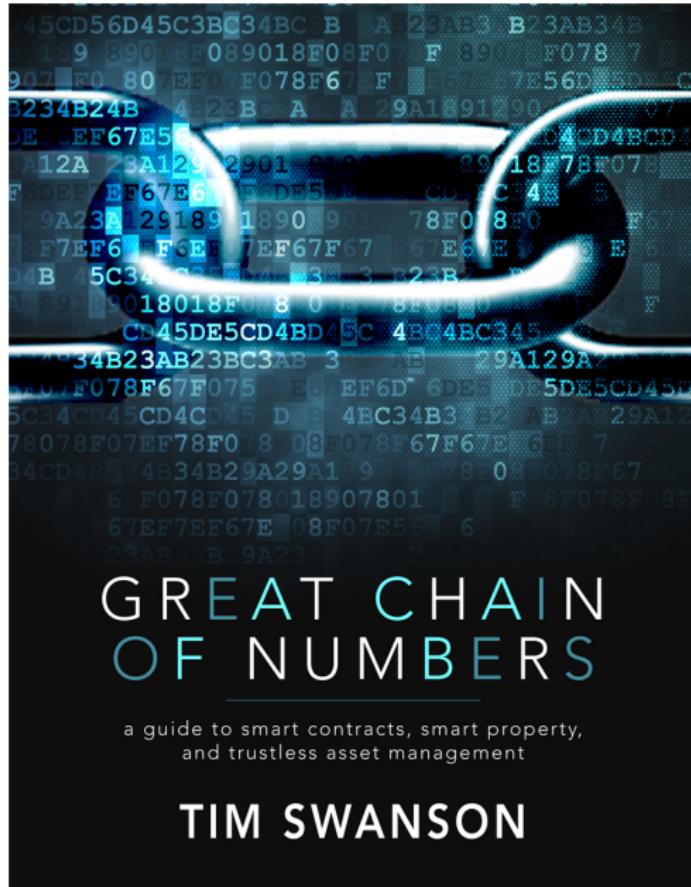


Рис. 2: Swanson, T., Great Chain of Numbers



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
- *Приватный и публичный ключи* — сущности системы асимметричного шифрования для безопасной передачи сообщений между парой субъектов
- *Цифровая подпись* — реквизит электронного документа, полученный в результате криптографического преобразования информации и позволяющий проверить отсутствие искажения информации, принадлежность подписи владельцу сертификата ключа подписи
- *Майнер* — лицо, обеспечивающее достижение консенсуса о том, какие транзакции считать валидными с целью предотвращения траты уже использованной в другой транзакции монеты



Цель и задачи

Расширить существующую классификацию по использованию в реестрах [30] алгоритмов и протоколов, а так же создать приложение для автоматизации создания кода распределённого реестра.

Задачи:

- Выявить популярные распределённые реестры; выделить и изучить криптографические алгоритмы и протоколы в них
- Расположить их на диаграмме Эйлера-Венна для создания обновлённой классификации
- Реализовать код блокчейна с интерфейсом встраивания вариаций алгоритмов
- Создать модуль на языке Python3.6.5, позволяющий пользователю генерировать код работающего с использованием выбранных алгоритмов блокчейна
- Автоматизировать работу системы с набором существующих алгоритмов





DECENTRALIZE.TODAY

Your Daily Dose of Decentralization

R^G

W



DECENTRALIZE.TODAY

Your Daily Dose of Decentralization



DECENTRALIZE.TODAY

Your Daily Dose of Decentralization



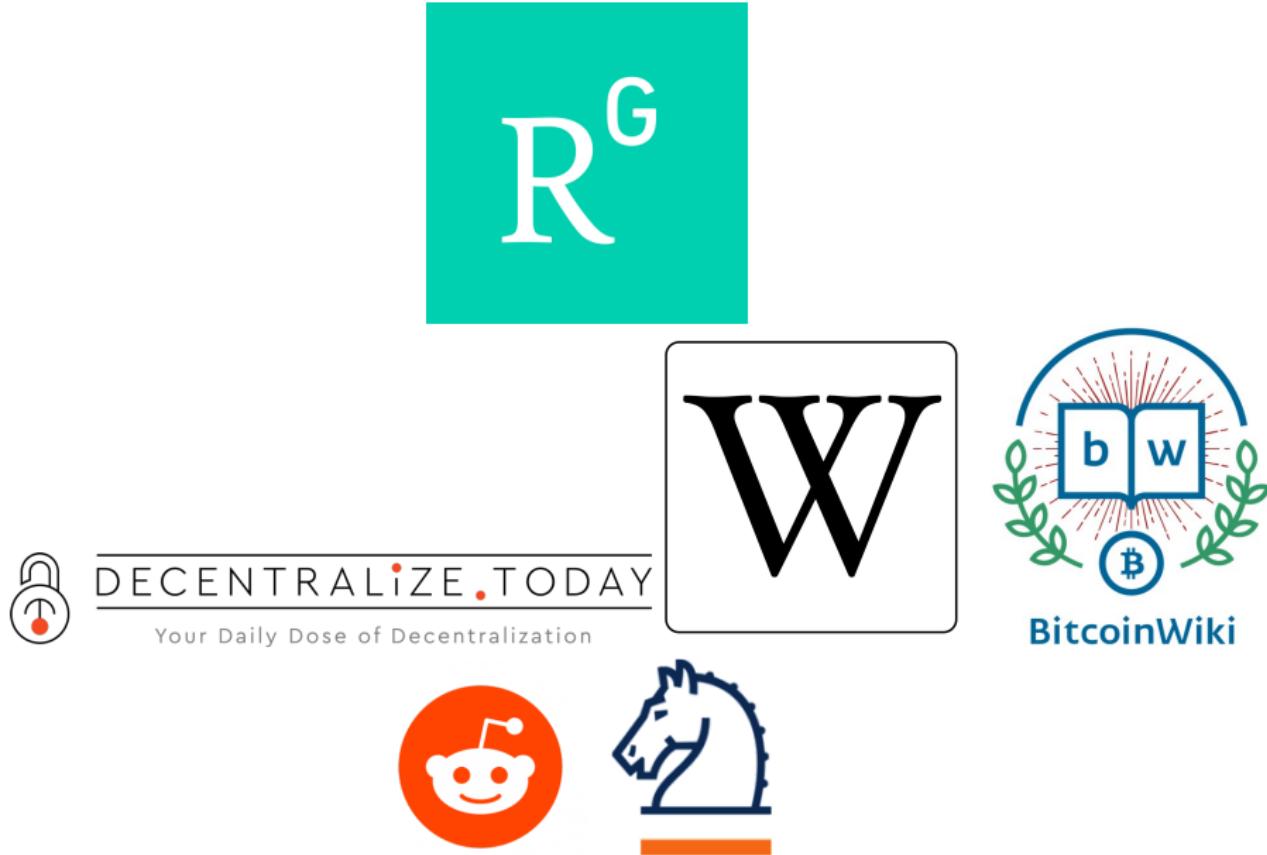


Рис. 3: Источники информации

Классификация от Tim Swanson [30]

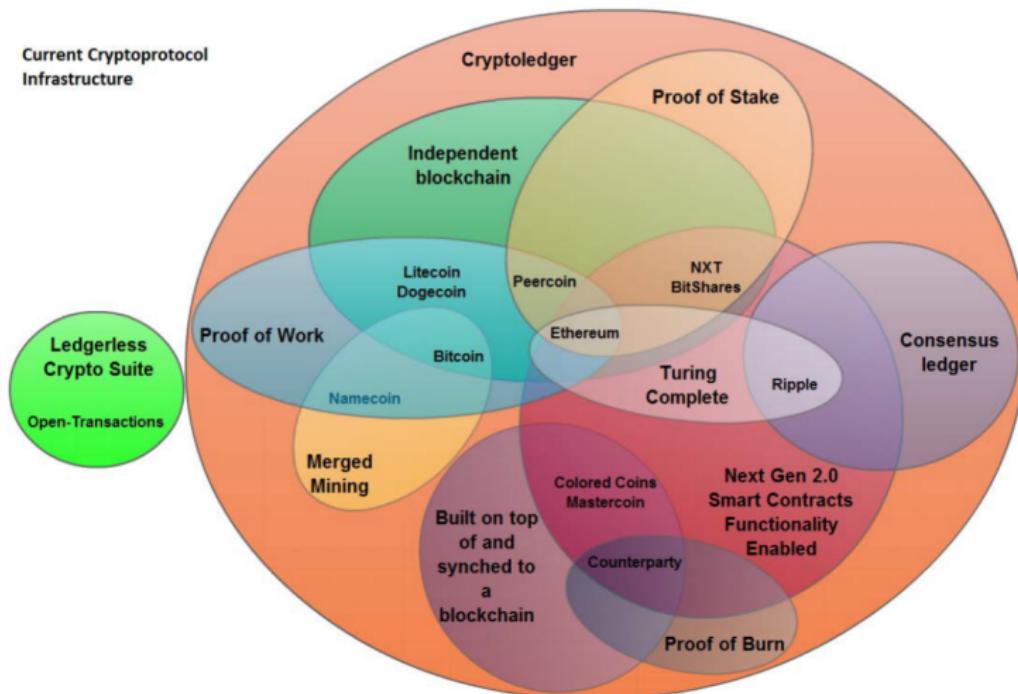


Рис. 4: Криптовидокол по состоянию на 2014 год [30]

Обновлённая классификация

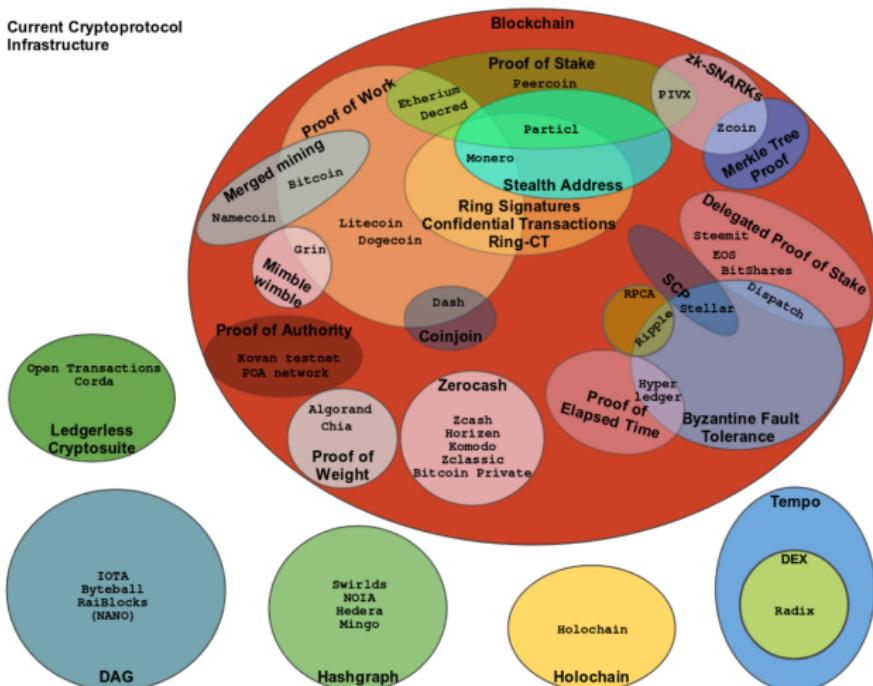


Рис. 5: Криптопротокол по состоянию на 2019 год

Программа

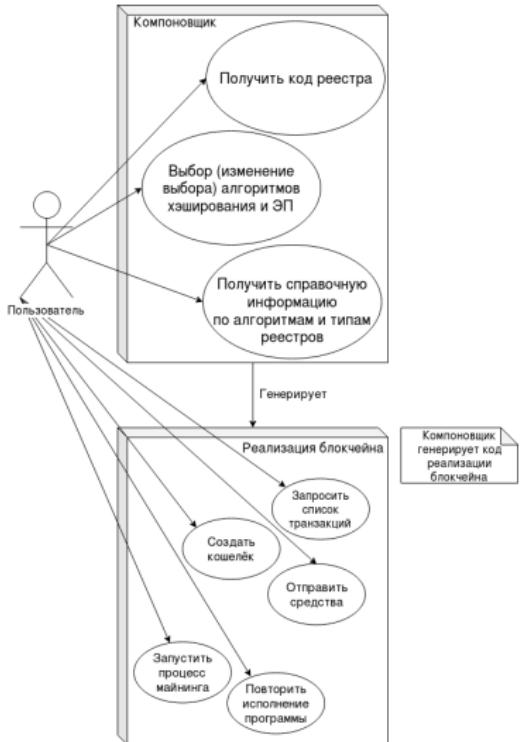


Рис. 6: Диаграмма use case



Особенности архитектуры

- Сервер автообновления поддерживает консистентность реализаций алгоритмов
- **Continuous integration** позволяет отслеживать работоспособность автообновляемой версии реализаций алгоритмов
- Спроектировано для упрощения дальнейшей масштабируемости
- Реализации алгоритмов были адаптированы под **Python3**
- Использование **конфигурационных** файлов вместо разрастания количества аргументов командной строки

Технологии реализации



Рис. 7: Инструменты реализации

Демонстрация



- ✓ Устаревшая классификация обновлена
- ✓ В новой отражены не только новые алгоритмы и протоколы, но и современные распределённые реестры
- ✓ Разработано средство автоматизации программирования
- ✓ Создан автоматизированный процесс по работе с кодами реализаций алгоритмов и их обновлению



Направления дальнейшей работы

- Новые реестры
- Новые алгоритмы
- Реализации алгоритмов Python → С
- Исследование новых реестров
- Поддержание актуальности классификации



Список используемых источников

1. 279 questions in Blockchain | Science topic. — URL: <https://www.researchgate.net/topic/Blockchain> (дата обр. 20.05.2019).
2. 97 questions in Cryptocurrency | Science topic. — URL: <https://www.researchgate.net/topic/Cryptocurrency> (дата обр. 20.05.2019).
3. API — Flask 0.12.4 documentation. — URL: <http://flask.pocoo.org/docs/0.12/api/#%7Dflask.Flask> (дата обр. 20.05.2019).
4. *Ashish Kotbsbtechdac.* DAG will overcome Blockchain Problems DAG VS. BLOCKCHAIN. — 2018. — URL: <https://medium.com/coinmonks/dag-will-overcome-blockchain-problems-dag-vs-blockchain-9ca302651122> (дата обр. 20.05.2019).
5. Bitcoin Is Unsustainable. — URL: https://motherboard.vice.com/en%7B%5C_%7Dus/article/ae3p7e/bitcoin-is-unsustainable (дата обр. 23.04.2019).
6. Blockchain. — URL: <https://www.reddit.com/r/BlockChain/> (дата обр. 20.05.2019).
7. *Code Creator.* BlockChain. — URL: <https://www.codecreator.com/index.php/blockchain/> (дата обр. 20.05.2019).
8. Continuous Integration and Delivery - CircleCI. — URL: <https://circleci.com/> (дата обр. 20.05.2019).
9. Cryptocurrency news and discussions. — URL: <https://www.reddit.com/r/CryptoCurrency/> (дата обр. 20.05.2019).
10. Distributed Messaging - zeromq. — URL: <http://zeromq.org/> (дата обр. 20.05.2019).
11. *Dwork C., Naor M.* Pricing via Processing or Combating Junk Mail // Advances in Cryptology — CRYPTO' 92. — 2007. — С. 139—147. — DOI: 10.1007/3-540-48071-4_10.
12. *Etherium.* TESTNET Kovan (KETH) Blockchain Explorer. — 2018. — URL: <https://kovan.etherscan.io/> (дата обр. 23.04.2019).
13. *Groth J., Kohlweiss M.* One-out-of-many proofs: Or how to leak a secret and spend a coin // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). — 2015. — Т. 9057. — С. 253—280. — ISSN 16113349. — DOI: 10.1007/978-3-662-46803-6_9.
14. gRPC. — URL: <https://grpc.io/> (дата обр. 20.05.2019).
15. *Jim.* Hash codes are not unique. — 2012. — URL: <http://blog.mischel.com/2012/04/13/hash-codes-are-not-unique/> (дата обр. 20.05.2019).



Список используемых источников

16. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem // ACM Transactions on Programming Languages and Systems. — 2002. — Т. 4, № 3. — С. 382—401. — ISSN 01640925. — DOI: 10.1145/357172.357176.
17. Magic Code Generator – Tools for blockchain-based application development. — URL: <https://magiccodegenerator.com/> (дата обр. 20.05.2019).
18. Maurer F. K., Florian M. Anonymous CoinJoin Transactions with Arbitrary Values. —.
19. Maxwell G. Confidential Transactions. — 2015.
20. Microsoft Azure. Blockchain Technology and Applications. — URL: <https://azure.microsoft.com/en-us/solutions/blockchain/> (дата обр. 20.05.2019).
21. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. // Journal for General Philosophy of Science. — 2008. — № 1. — С. 1–9. — ISSN 09254560. — DOI: 10.1007/s10838-008-9062-0. — arXiv: 43543534v343453.
22. Niranjanamurthy M., Nithya B. N., Jagannatha S. Analysis of Blockchain technology: pros, cons and SWOT // Cluster Computing. — 2018. — Март. — С. 1–15. — ISSN 1386-7857. — DOI: 10.1007/s10586-018-2387-5. — URL: <http://link.springer.com/10.1007/s10586-018-2387-5>.
23. Noether S., Mackenzie A., Research Lab T. M. Ring Confidential Transactions // Ledger. — 2016. — Т. 1. — С. 1–18. — DOI: 10.5195/ledger.2016.34.
24. Poelstra A. Mimblewimble. — 2016.
25. Popov S. IOTA whitepaper v1.4.3. — 2018. — URL: https://assets.ctfassets.net/r1drfvzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1%7B%5C_%7D4%7B%5C_%7D3.pdf.
26. Shippable. — URL: <https://app.shippable.com/accounts/5aad7d3e76ee0c1700c1d8d2/dashboard> (дата обр. 20.05.2019).
27. Sir Mark Walport. Distributed Ledger Technology: beyond block chain. — 2018. — DOI: 10.1021/acsaelm.8b00240.
28. SQLite. — URL: <https://sqlite.org/index.html> (дата обр. 20.05.2019).
29. The Official YAML Web Site. — URL: <https://yaml.org/> (дата обр. 20.05.2019).



Список используемых источников

30. *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).
31. *Travis CI.* — URL: <https://travis-ci.org/> (дата обр. 20.05.2019).
32. *Using etcd.* — URL: <https://coreos.com/etcd/> (дата обр. 20.05.2019).
33. *Van Saberhagen N. CryptoNote v 1.0.* — 2012.
34. *Van Saberhagen N. Monero: CryptoNote v 2.0 // White Paper.* — 2013. — С. 1–20. — URL: <https://bytecoin.org/old/whitepaper.pdf%7B%5C%7D0Ahttps://cryptonote.org/whitepaper.pdf>.
35. *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).
36. *Wikipedia.* — URL: <https://www.wikipedia.org/> (дата обр. 20.05.2019).
37. *Zerocoin Electric Coin Company. ZCash.* — 2016.
38. *ZEXE: Enabling decentralized private computation / S. Bowe [и др.].* — 2019. — URL: <https://eprint.iacr.org/2018/962.pdf>.
39. *Направленный ациклический граф — Википедия.* — URL: https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9%7B%5C_%7D%D0%B0%D1%86%D0%B8%D0%BA%D0%BB%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9%7B%5C_%7D%D0%B3%D1%80%D0%B0%D1%84 (дата обр. 22.05.2019).
40. *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

+7-910-008-3926
kikupriyanov@edu.hse.ru
kupriyanovkirill@gmail.com
[@SsinopsysS](https://twitter.com/SsinopsysS)

2019