

**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

**Факультет компьютерных наук
Департамент программной инженерии**

Согласовано

Профессор департамента
программной инженерии факультета
компьютерных наук, канд. техн. наук

_____ С.М. Авдошин

" ____ " _____ 2019 г

Утверждаю

Академический руководитель
образовательной программы
«Программная инженерия»
профессор, канд. техн. наук
В. В. Шилов

_____ В. В. Шилов

" ____ " _____ 2019 г

**Криптографические алгоритмы и протоколы для распределенных
реестров**

Текст программы

ЛИСТ УТВЕРЖДЕНИЯ

RU.17701729.04.01 12 01-1

Студент группы БПИ 151 НИУ ВШЭ

_____ Куприянов К. И.

" ____ " _____ 2019 г

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2019

УТВЕРЖДЕНО
RU.17701729.04.01 12 01-1

Криптографические алгоритмы и протоколы для распределенных реестров

Текст программы

RU.17701729.04.01 12 01-1

Листов 5

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2019

Содержание

1	Текст программы	2
2	Приложение 1. Список используемой литературы	3

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.04.01 12 01-1				
Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата

1. Текст программы

Текст программы на исходном языке находится на хостинге программных преков Github по адресу

<https://github.com/Sinopsys/gsl>

или по qr-коду (рис. 1) в связи с большим количеством строк кода.

Код также доступен на прилагаемом к работе CD диске в архиве ТекстПрограммы.zip



Рис. 1: ссылка на программу

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.04.01 12 01-1				
Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата

2. Приложение 1. Список используемой литературы

Список литературы

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/%7B%5C#%7Dflask.Flask> (дата обр. 20.05.2019).
4. *Ashish Kotsbtechcdac*. 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. *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).
10. Cryptocurrency news and discussions. — URL: <https://www.reddit.com/r/CryptoCurrency/> (дата обр. 20.05.2019).
11. Distributed Messaging - zeromq. — URL: <http://zeromq.org/> (дата обр. 20.05.2019).
12. *Dwork C., Naor M.* Pricing via Processing or Combatting Junk Mail // *Advances in Cryptology — CRYPTO'92*. — 2007. — С. 139—147. — DOI: 10.1007/3-540-48071-4_10.
13. *Ethereum*. TESTNET Kovan (KETH) Blockchain Explorer. — 2018. — URL: <https://kovan.etherscan.io/> (дата обр. 23.04.2019).
14. gnu.org. — URL: <https://www.gnu.org/licenses/gpl-3.0.en.html>.
15. *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.
16. gRPC. — URL: <https://grpc.io/> (дата обр. 20.05.2019).
17. *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).
18. *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.
19. Magic Code Generator – Tools for blockchain-based application development. — URL: <https://magiccodegenerator.com/> (дата обр. 20.05.2019).
20. *Maurer F. K., Florian M.* Anonymous CoinJoin Transactions with Arbitrary Values. —
21. *Maxwell G.* Confidential Transactions. — 2015.
22. *Microsoft Azure*. Blockchain Technology and Applications. — URL: <https://azure.microsoft.com/en-us/solutions/blockchain/> (дата обр. 20.05.2019).

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.04.01 12 01-1				
Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата

23. *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: 43543534534v343453.
24. *Noether S., Mackenzie A., Research Lab T. M.* Ring Confidential Transactions // Ledger. — 2016. — Т. 1. — С. 1–18. — DOI: 10.5195/ledger.2016.34.
25. *Poelstra A.* Mumblewimble. — 2016.
26. *Popov S.* IOTA whitepaper v1.4.3. — 2018. — URL: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw45eae33637ca92f85dd9f4a3a218e1ec/iota1%7B%5C_%7D4%7B%5C_%7D3.pdf.
27. Privacy Coin Matrix. — URL: <https://www.reddit.com/r/PrivacyCoinMatrix> (дата обр. 24.04.2019).
28. Shippable. — URL: <https://app.shippable.com/accounts/5aad7d3e76ee0c1700c1d8d2/dashboard> (дата обр. 20.05.2019).
29. *Sir Mark Walport.* Distributed Ledger Technology: beyond block chain. — 2018. — DOI: 10.1021/acsaem.8b00240.
30. SQLite. — URL: <https://sqlite.org/index.html> (дата обр. 20.05.2019).
31. The Official YAML Web Site. — URL: <https://yaml.org/> (дата обр. 20.05.2019).
32. *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).
33. Travis CI. — URL: <https://travis-ci.org/> (дата обр. 20.05.2019).
34. Using etcd. — URL: <https://coreos.com/etcd/> (дата обр. 20.05.2019).
35. *Van Saberhagen N.* CryptoNote v 1.0. — 2012.
36. *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>.
37. *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).
38. Wikipedia. — URL: <https://www.wikipedia.org/> (дата обр. 20.05.2019).
39. *ZeroCoin Electric Coin Company.* ZCash. — 2016.
40. ZEXE: Enabling decentralized private computation / S. Bowe [и др.]. — 2019. — URL: <https://eprint.iacr.org/2018/962.pdf>.
41. 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).
42. *Ольга Скоробогатова.* О российском консорциуме, национальной электронной валюте. — 2016. — URL: <https://bankir.ru/publikacii/20160419/olga-skorobogatova-o-rossiiskom-konsortsiуме-natsionalnoi-elektronnoi-valyute-10007442/> (дата обр. 23.04.2019).

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.04.01 12 01-1				
Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.04.01 12 01-1				
Инв. №подл.	Подп. и дата	Взам. инв. №	Инв. №дубл.	Подп. и дата