

004.738.5:339

B67



BLOCKCHAIN

AND DECENTRALIZED SYSTEMS

VOLUME 3

DISTRIBUTED LAB

P. Kravchenko,
B. Skriabin, O. Kurbatov, O. Dubinina

BLOCKCHAIN AND DECENTRALIZED SYSTEMS

Authors' test edition

In three volumes

Volume 3



Kharkiv

2022

UDC 004.738.5:336]:007-057.21](07)

K78

Authors:

P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina

Kravchenko, P.

K78 Blockchain and decentralized systems : in three volumes.

V.3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. –

Kharkiv : PROMART, 2022. – 288 p. : 178 figures; 7 tables;

references: 145 titles.

ISBN 978-617-7634-27-9

ISBN 978-617-7634-79-8 (v. 3)

The textbook covers the topic of decentralized technologies that became popular due to the advancements of the cryptocurrency concept. Initially, the authors focus on the technical and fundamental aspects of cryptocurrencies, blockchain technology, and the application level, giving the reader an opportunity to deeply understand the basics. The main feature of the book is that the material is presented at the intersection of operational principles as well as the advantages and risks of innovative information technologies.

The textbook is created for a wide audience: scientists, teachers, graduate students, students with basic knowledge in the field of cryptography and information technology - for everyone interested in the topic of decentralized technologies.

UDC 004.738.5:336]:007-057.21](07)

ISBN 978-617-7634-79-8 (v. 3)

ISBN 978-617-7634-27-9

© P. Kravchenko, B. Skriabin,
O. Kurbatov, O. Dubinina, 2022

CONTENTS

INTRODUCTION.....	8
ABOUT DISTRIBUTED LAB.....	10
1 APPLYING DECENTRALIZED APPROACHES FOR VARIOUS SYSTEMS DESIGN.....	12
1.1 Operational principles and development of mesh networks.....	12
The global goal of mesh networks.....	13
Popular protocols for designing mesh networks.....	16
Applying mesh networks in practice.....	18
Disadvantages of mesh networks.....	20
1.2 Decentralized digital identity systems.....	21
Design and operational principles of the OAuth protocol.....	26
OpenID and OpenID Connect protocols.....	28
Limitations of the described protocols.....	32
Principles of building the global identity system.....	33
Extending capabilities of the global identity system with blockchain technology.....	37
Digital identity for IoT.....	40
1.3 Decentralized e-voting platforms.....	42
Challenges of traditional approaches to voting.....	43
E-voting in Estonia.....	45
E-voting in Switzerland.....	49
A decentralized e-voting approach.....	51
Example of a voting scheme with no central authority.....	52
Using blockchain technology for an e-voting system.....	59
1.4 Technology of decentralized exchanges.....	60
Operational principles of decentralized exchanges.....	62
Escrow.....	63
Atomic swap.....	64
Ox protocol.....	65

Internal exchanges.....	67
1.5 Decentralized auction.....	69
Operation principle of an online auction.....	70
The operational principle of a decentralized online auction.....	72
2 SCHNORR SIGNATURES AND RELATED UPDATES.....	75
2.1 Features of Schnorr signatures and the possibility of their implementation in accounting systems.....	75
Schnorr signature advantages.....	76
Schnorr signature design.....	79
Multisignature using the Schnorr algorithm.....	80
The Rouge Key Attack.....	81
Bellare-Neven scheme.....	85
MuSig scheme.....	86
Schnorr signature restrictions.....	87
Features of Schnorr signatures implementation.....	89
2.2 MAST concept in Bitcoin.....	90
Abstract Syntax Tree.....	91
What is the MAST?.....	94
Simplified scheme of MAST.....	95
Advantages and features of MAST with a large number of alternative conditions.....	98
Practical application of MAST.....	101
Concept development and current status.....	101
2.3 Taproot operational principles.....	103
Alternative conditions are needed to resolve the disagreements between the parties to the contract.....	103
Schnorr Signatures as a base component of Taproot.....	105
Cascades of Taproot scripts.....	109
2.4 Graftroot design.....	110
Separate signature of each alternative condition.....	110
Ability to add new conditions.....	114

3 USING SHARDING, OFF-CHAIN, AND DAG TO SCALE AN ACCOUNTING SYSTEM.....	117
3.1 Using off-chain protocols.....	118
3.2 Sharding concept.....	120
Sharding in blockchain-based systems.....	123
TON architecture.....	126
Chain of blocks structure in TON.....	126
Splitting and merging shardchains.....	128
Making decisions regarding the state of the system.....	129
Communication between shardchains.....	131
3.3 Design and applying of DAG.....	133
Directed acyclic graph.....	133
The concept of directed acyclic graphs.....	134
DAG-based decentralized accounting system architecture.....	136
Reaching a consensus and resolving disagreements.....	137
IOTA.....	139
IOTA.....	139
The structure and purpose of the Bundle.....	142
4 PRIVACY AND ANONYMITY IN THE INTERNET.....	146
4.1 Operational principles and usage of Tor.....	146
Ways to anonymize a user in the network.....	146
Tor application features.....	148
Obtaining a list of Tor nodes.....	150
Methods for deanonymizing dark networks users.....	151
4.2 Internet invisible project.....	154
Garlic routing.....	154
Selecting intermediate nodes and creating tunnels.....	156
Addressing and searching for nodes.....	157
4.3 The design and structure of Tox.....	159
How accounts in Tox work.....	160
Types of nodes and applications.....	161

The principle of onion routing.....	162
Connection of parties.....	164
TCP Relay nodes.....	167
Using DHT to find contacts in the network.....	168
4.4 Steganographic methods of hiding information.....	169
Features and Benefits.....	170
Classic steganography.....	171
Computer steganography.....	172
Digital steganography.....	173
Specific aspects of usage and attacks.....	176
5 FEATURES AND ROLE OF CRYPTOGRAPHIC COMMITMENTS IN ACCOUNTING SYSTEMS.....	177
5.1 Features and methods of building cryptographic commitments.....	178
Adding randomness as a component of commitments.....	179
Pedersen commitments.....	181
Knowledge substitution and Nothing Up My Sleeve approaches.....	182
One commitment for a value vector.....	185
ElGamal commitment scheme.....	186
5.2 Schnorr identification protocol as a zero-knowledge proof interactive scheme.....	187
Schnorr identification scheme.....	187
In which case is the prover is able to fake the proof.....	189
Turning an interactive protocol into a non-interactive.....	190
5.3 Using Pedersen commitments for zero-knowledge proofs.....	191
Using Pedersen commitments in Confidential Transaction.....	196
Using Pedersen commitments for Range Proofs.....	197
6 QUANTUM COMPUTING AND POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS.....	199
6.1 Introduction to quantum computing.....	199
Basic principles of quantum mechanics.....	200
Quantum computer capabilities.....	205
6.2 Basic operations with qubits.....	208

Operating with multiple qubits.....	213
6.3 Using quantum gates.....	216
Single-qubit quantum gates.....	216
Multi-qubit quantum gates.....	219
Quantum circuits.....	221
Circuit for creating Bell states.....	223
Quantum teleportation circuit.....	224
6.4 The mathematical base of post-quantum cryptographic algorithms.....	226
Cryptographic primitives that vulnerable to quantum computer attacks.....	228
How urgent is it to switch to algorithms that are resistant to quantum computer attacks?.....	231
Possible solutions.....	232
Families of post-quantum primitives.....	234
Lattice-based cryptography.....	234
Code-based cryptography.....	236
Multivariate polynomial cryptography.....	237
Hash-based cryptography.....	238
Alternative groups.....	239
6.5 Hash-based signature algorithms.....	240
HORS construction.....	241
Merkle signature scheme.....	245
Sphincs algorithms family.....	249
CONCLUSION.....	256
GLOSSARY OF TERMS.....	258
ACKNOWLEDGEMENTS.....	269
ABOUT THE AUTHORS.....	270
USED SOURCES AND LINKS.....	272