

Blockchain : przewodnik po technologii łańcucha bloków. Kryptowaluty, inteligentne kontrakty i aplikacje rozproszone / Lorne Lantz, Daniel Cawrey. – Gliwice, © 2023

Spis treści

Przedmowa	13
1. Początki technologii blockchain	15
Systemy elektroniczne i zaufanie	15
Rozproszony kontra scentralizowany kontra zdecentralizowany	16
Poprzednicy sieci Bitcoin	21
DigiCash	21
E-gold	22
Hashcash	22
B-money	23
Bit gold	23
Eksperyment Bitcoin	24
Kryzys finansowy 2008 roku	24
Whitepaper	25
Wprowadzenie serwera z sygnaturą czasową	26
Przechowywanie danych w łańcuchach bloków	27
Urzeczywistnienie sieci Bitcoin	30
Przekonujące komponenty	30
Dojście do konsensusu	31
Wczesna podatność	33
Adopcja	34
Podsumowanie	34
2. Fundamenty kryptowaluty	35
Klucze publiczne i prywatne w systemach kryptowalut	35
Model UTXO	37
Transakcje	38
Korzeń Merkle'a	39
Podpisywanie i potwierdzanie transakcji	42
Transakcja podstawowa (coinbase)	42
Bezpieczeństwo transakcji Bitcoin	43
Skróty (hasze)	44
Skróty (hasze) bloku	45
Powiernictwo: kto trzyma klucze	47
Rodzaje portfeli: powierniczy kontra bez powiernictwa	47
Wariacje w obrębie rodzajów portfeli	48
Podstawy bezpieczeństwa	49
Fraza odzyskiwania (recovery seed)	50

Kopanie	52
W kopaniu chodzi o nagrody	52
Generowanie bloku	53
Konsensus	54
Dowód pracy	54
Dowód stawki	60
Inne koncepcje konsensusu	61
Interesariusze	63
Brokerzy	63
Giełdy	63
Usługi powiernicze	64
Usługi analityczne	64
Serwisy informacyjne	65
Podsumowanie	65
3. Forki i altchainy	66
Propozycje ulepszenia sieci Bitcoin	66
Forki (rozwidlenia)	67
Sporny hard fork	68
Rozwidlenie Bitcoin Cash	71
Altcoiny (alternatywne coiny)	73
Litecoin	74
Inne altcoinowe eksperymenty	75
Łańcuchy „2.0”	76
NXT	76
Counterparty	76
Kryptowaluty z nastawieniem na prywatność	77
Dash	77
Monero	77
Zcash	77
Ripple i Stellar	78
Ripple	78
Stellar	79
Skalowanie łańcuchów bloków	79
SegWit Lightning	80
Inne altchainowe rozwiązania	81
Klasyczny fork	82
Ethereum	83
Podsumowanie	84
4. Ewolucja do Ethereum	85
Ulepszenie ograniczonej funkcjonalności sieci Bitcoin	85
Kolorowane monety i tokeny	85
Mastercoin i inteligentne kontrakty	86
Czym jest Omni Layer	86
Ethereum, czyli Mastercoin na wyższym poziomie	90

Ether i gaz	90
Przypadek użycia: ICO	91
Zdecentralizowane autonomiczne organizacje (DAO)	92
Kluczowe organizacje w ekosystemie Ethereum	93
Zdecentralizowane aplikacje (dapps)	95
Przypadki użycia	95
Wyzwania związane z tworzeniem zdecentralizowanych aplikacji	96
Wdrażanie inteligentnych kontraktów w Ethereum	96
Maszyna Wirtualna Ethereum (EVM)	97
Gaz i ustalanie cen	103
Interakcja z kodem	105
Podsumowanie	105
5. Tokenizacja wszystkiego	106
Tokeny w platformie Ethereum	108
Tokeny wymienialne i niewymienialne	108
Czy token jest konieczny?	109
Airdropy, czyli krypto walutowe naloty	109
Różne typy tokenów	110
Standard ERC (Ethereum Requests for Comment)	110
ERC-20	111
ERC-721	114
ERC-777	116
ERC-1155	117
Kontrakty wielopodpisowe	118
Zdecentralizowane kontrakty giełdowe	120
Podsumowanie	122
6. Infrastruktura rynku	123
Ewolucja ceny bitcoina	123
Rola giełd	125
Arkusze zleceń (order book)	126
Poślizg cenowy (slippage)	127
Wykres głębokości rynku (depth chart)	128
Jurysdykcja	128
Wash trading	129
Grube ryby	130
Instrumenty pochodne	132
Struktura rynku kryptowalut	132
Arbitraż	133
Ryzyko drugiej strony	133
Dane o rynku	135
Analiza	137
Kryptowalutowa analiza fundamentalna	137
Krypto walutowa analiza techniczna	139
Trading arbitrażowy	141

Wycucie czasu i zarządzanie dostępnymi środkami	141
Konfiguracja środków nr 1	141
Konfiguracja środków nr 2	142
Konfiguracja środków nr 3	143
Trudności regulacyjne	143
Ryzyko bankowe	143
Ryzyko giełdowe	144
Podstawowe błędy	144
API giełdy i boty traderskie	145
Otwartoźródłowe technologie traderskie	147
Limit prędkości	148
REST kontra WebSocket	148
Testowanie w piaskownicy	148
Agregatory rynku	148
Podsumowanie	149
7. Decentralizacja finansów i sieci	150
Redystrybucja zaufania	150
Tożsamość i niebezpieczeństwo ataków hakerskich	150
Portfele	151
Klucze prywatne	152
Usługi nazewnicze	152
Decentralizacja finansów	153
Istotne definicje	153
Stablecoiny	155
Usługi DeFi	157
Udzielanie pożyczek	158
Oszczędzanie	158
Instrumenty pochodne (derywaty)	158
Zdecentralizowane giełdy	159
Giełdy zdecentralizowane kontra scentralizowane	159
Błyskawiczne pożyczki	167
Stworzenie kontraktu błyskawicznej pożyczki	168
Wdrożenie kontraktu	169
Realizacja błyskawicznej pożyczki	170
Błyskawiczne pożyczki w arbitrażu	173
Podatność Fulcrum	173
Prywatność	175
Dowód z wiedzą zerową	176
Zcash	178
Podpisy pierścieniowe	179
Web 3.0	179
Podsumowanie	180
8. Złap mnie, jeśli potrafisz	181
Ewolucja prania kryptopieniędzy	181

Wytyczne FinCEN i początki regulacji	184
FATF i Travel Rule	186
Lekceważenie prawa	186
Unikanie prześwietleń: arbitraż regulacyjny	188
Malta	188
Singapur	188
Hongkong	189
Bahamy	189
Kryptostablecoiny	190
NuBits	190
Digix	191
Basis	191
Tether	191
Zbiórki typu Initial Coin Offerings	192
Intencje twórców	193
Ekonomia tokena	193
Whitepaper	193
Hakowanie giełd	194
Mt. Gox	194
Bitfinex	196
Coincheck	196
NiceHash	197
Inne włamania	197
Kradzież bitcoinów na antenie Bloomberg TV	197
Przekierowanie EtherDelta	197
CryptoLocker i ransomware	197
Podmiana SIM	198
Podsumowanie	199
9. Inne łańcuchy bloków	200
Do czego się nadają łańcuchy bloków?	200
Bazy danych i księgi główne (rejestry)	201
Decentralizacja kontra centralizacja	202
Uczestnicy	202
Kluczowe cechy rozproszonych weryfikowalnych rejestrów (ksiąg głównych)	203
Prywatne implementacje oparte na Ethereum	203
Nightfall	204
Quorum	204
Implementacje biznesowe	204
Hyperledger	204
Corda	204
DAML	208
Łańcuch bloków jako usługa	208
Bankowość	209
Mennica królewska	209

Banque de France	209
Chiny	210
Rezerwa Federalna USA	210
JPMorgan	211
Zastosowania księgi głównej z kontrolą dostępu	211
IT	211
Bankowość	211
Cyfrowe waluty banków centralnych	211
Prawo	212
Gaming	212
Opieka zdrowotna	213
Internet Rzeczy	213
Płatności	213
Diem (pierwotnie Libra)	214
Diem Association (pierwotnie Libra Association)	214
Zapózyczenia z istniejących łańcuchów bloków	215
Novi	215
Jak działa protokół Diem	216
Podsumowanie	218
10. Przyszłość łańcucha bloków	219
Im bardziej rzeczy się zmieniają...	220
Łańcuchy do obserwowania	221
Jak działa Monero	222
Mimewimble, Beam i Grin	224
Problem skalowania	224
Łańcuchy poboczne	225
Sharding	225
STARK	225
DAG (skierowany graf acykliczny)	225
Avalanche	226
Liquid	226
Lightning	226
Skalowanie Ethereum	231
Prywatność	232
Interoperacyjność	233
Tokenizacja wszystkiego	233
Podsumowanie	234