

SZKOLENIE ŚREDNIO ZAAWANSOWANE

Blockchain i poufność w praktyce na przykładzie Quorum

QUORUM

Czas trwania: 2 dni (16h)

Działanie i wykorzystanie blockchain oraz kontraktów inteligentnych z usługą poufności na praktycznych przykładach z użyciem platformy Quorum

Cele szkolenia

- Poznanie zasad działania, możliwych zastosowań oraz zalet i wad blockchain zapewniającego poufność danych na przykładzie Quorum
- Zrozumienie działania oraz celów stosowania prywatnych transakcji i prywatnych kontraktów inteligentnych

Zalety

- Podczas warsztatów uczestnicy samodzielnie uruchomią własną instancję środowiska Quorum wykorzystując GoQuorum, przygotują konfigurację węzłów i połączą je we wspólną sieć
- Uczestnicy zrealizują publiczne i prywatne transakcje pomiędzy utworzonymi kontami
- Uczestnicy utworzą prywatne kontrakty inteligentne oraz zaobserwują ich działanie w różnych węzłach
- Wykorzystując Cakeshop uczestnicy będą zarządzać i monitorować instancję Quorum
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretność umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

- Osoby, które w praktyce chcą uruchomić i poznać zasady działania blockchain zapewniającego poufność danych i transakcji
- Programiści myślący o tworzeniu kontraktów
- Administratorzy i wdrożeniowcy uruchamiający blockchain, konsultanci i architekci systemów transakcyjnych i rozproszonych
- Ludzie biznesu z zacięciem technicznym szukający ciekawych zastosowań blockchain



Wymagania

- Od uczestników wymagana jest znajomość obsługi komputera, pracy z wierszem poleceń oraz znajomość podstawowych zasad programowania
- Wskazane jest uczestnictwo w szkoleniu Praktyczne wykorzystanie blockchain na przykładzie Ethereum (ETHER)

Program

1. Architektura systemów opartych o blockchain i wykorzystywane algorytmy
 - a. Blockchain jako rozproszona baza danych
 - b. Integralność, uwierzytelnienie, niezaprzeczalność i poufność a blockchain
 - c. Funkcje skrótu, ich właściwości i zastosowania (SHA-256, SHA3, Keccak)
 - d. Szyfrowanie, algorytmy symetryczne (AES) i asymetryczne (krzywa eliptyczna Curve25519, ECIES), koperta elektroniczna
 - e. Koncepcja i realizacja podpisu cyfrowego (algorytm ECDSA)
 - f. Sieci P2P (peer to peer)
 - g. Podstawowe elementy systemu opartego o blockchain: przechowywanie danych, protokół komunikacyjny i algorytm konsensusu
 - h. Rozszerzenia implementacji mające za zadanie realizację poufności
 - i. Proces zatwierdzania transakcji, tworzenie bloków i kopanie (mining)
 - j. Dowód uprawnień (proof of authority, PoA) i inne techniki zatwierdzania bloków
2. Quorum i jego działanie
 - a. Architektura Quorum, węzły blockchain i zarządzanie kluczami
 - b. Implementacje węzłów Quorum, cechy węzła GoQuorum w odniesieniu do Ethereum
 - c. Budowa blockchain Quorum oraz wykorzystywane algorytmy
 - d. Zapewnianie prywatności z użyciem Tessera
 - e. Algorytmy konsensusu
 - f. Algorytm QBFT
 - g. Algorytmy Istanbul BFT (IBFT), Raft i Clique
 - h. Przetwarzanie transakcji prywatnej
 - i. Poufność w odniesieniu do węzła i użytkownika
 - j. Konfiguracja i uruchomienie sieci Quorum
 - k. Konfiguracja połączeń P2P pomiędzy węzłami, zasady tworzenia reguł dostępu
 - l. Komunikacja pomiędzy węzłami
 - m. Lekki węzeł GoQuorum (qlight)
 - n. Zlecenie i zatwierdzanie transakcji
 - o. Praca w konsoli GoQuorum
 - p. Rozszerzenia w web3 API dla Quorum
 - q. Obserwacja i zarządzanie łańcuchem za pomocą Cakeshop
 - r. Inne narzędzia monitorowania i zarządzania siecią
3. Kontrakty inteligentne (smart contracts) w Quorum
 - a. Na czym polega prywatność w kontrakcie?
 - b. Kod i magazyn kontraktu
 - c. Prywatne kontrakty i transakcje w nich



- d. Uruchomienie i wykorzystanie przykładowych kontraktów: token, przechowywanie danych
 - e. Bezpieczeństwo kontraktów w Quorum
 - f. Kontrakty prywatne
4. Zastosowania i kierunki rozwoju Quorum
- a. Zalety, wady i ograniczenia implementacji poufności w Quorum
 - b. Przykładowe zastosowania blockchain Quorum
 - c. Aktualne plany rozwoju Quorum

