Kod szkolenia: **QUORUM**

Tytuł szkolenia: **Blockchain i poufność w praktyce na przykładzie Quorum**

Dni: 2

Opis:

Adresaci szkolenia

Osoby, które w praktyce chcą uruchomić i poznać zasady działania blockchain zapewniającego poufność danych i transakcji. Programiści myślący o tworzeniu kontraktów, ludzie biznesu szukający ciekawych zastosowań blockchain, administratorzy i wdrożeniowcy uruchamiający blockchain, konsultanci i architekci systemów transakcyjnych i rozproszonych.

Cel szkolenia

Uczestnicy poznają zasady działania i zastosowania blockchain zapewniającego poufność danych oraz utworzą węzły blockchain Quorum i konstelacje. Zrealizują transakcje we własnym łańcuchu bloków z zachowaniem poufności.

Mocne strony szkolenia

Podczas warsztatów uczestnicy:

- skonfigurują konstelację Quorum zapewniającą poufność,
- utworzą własne blockchain w środowisku Quorum wykorzystujące algorytm konsensusu Raft i Istanbul BFT,
- wykonają prywatne transakcje w blockchain,
- utworzą prywatne inteligentne kontrakty oraz zaobserwują ich zachowanie w różnych węzłach,
- użyją narzędzia Cakeshop do obserwacji i zarządzania instancją Quorum.

Wymagania

Od uczestników wymagana jest znajomość obsługi komputera, pracy w konsoli oraz znajomość podstawowych zasad programowania. Wskazane jest uczestnictwo w szkoleniu ETHER.

Specjalne wymagania techniczne

Uczestnicy w trakcie zajęć korzystają z komputera z systemem Windows, Linux lub macOS podłączonego do sieci.

Parametry szkolenia

2 * 8 godzin (2 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Wprowadzenie

    - blockchain jako rozproszona baza danych
    - integralność, uwierzytelnienie, niezaprzeczalność i poufność a blockchain
    - funkcje skrótu, ich właściwości i zastosowania (SHA-256, SHA3, Keccak)
    - szyfrowanie, algorytmy symetryczne (AES) i asymetryczne (krzywa eliptyczna Curve25519, ECIES), koperta elektroniczna
    - koncepcja i realizacja podpisu cyfrowego (algorytm ECDSA)
    - sieci P2P (*peer to peer*)
    - podstawowe elementy systemu opartego o blockchain: przechowywanie danych, protokół komunikacyjny i algorytm konsensusu
    - rozszerzenia implementacji mające za zadanie realizację poufności
    - proces zatwierdzania transakcji, tworzenie bloków i kopanie (*mining*)
    - dowód pracy (*proof of work*, PoW), dowód stawki (*proof of stake*, PoS) i inne techniki zatwierdzania bloków

2. Quorum i jego działanie

    - architektura Quorum, węzły blockchain i konstelacja
    - implementacje węzłów Quorum, cechy węzła geth w odniesieniu do Ethereum
    - budowa blockchain Quorum oraz wykorzystywane algorytmy
    - działanie oraz przeznaczenie konstelacji (*constellation*) i menadżera transakcji (ang. *transaction manager*)
    - algorytm konsensusu Raft, węzeł lidera i węzły śledzących
    - algorytm konsensusu Istanbul BFT
    - algorytm konsensusu QuorumChain, węzły obserwatorów, głosujących i tworzących bloki
    - przetwarzanie transakcji prywatnej
    - poufność w odniesieniu do węzła i użytkownika
    - konfiguracja i uruchomienie sieci Quorum
    - konfiguracja połączeń P2P pomiędzy węzłami, ograniczenia dostępu
    - komunikacja pomiędzy węzłami oraz pomiędzy menadżerami transakcji (w konstelacji)
    - zlecanie i zatwierdzanie transakcji
    - praca w konsoli geth Quorum
    - rozszerzenia w web3 API dla Quorum
    - obserwacja i zarządzanie łańcuchem za pomocą Cakeshop

3. Inteligentne kontrakty (*smart contracts*) w Quorum

    - na czym polega prywatność w kontrakcie
    - kod i magazyn kontraktu
    - prywatne kontrakty i transakcje w nich
    - uruchomienie i wykorzystanie przykładowych kontraktów: token, przechowywanie danych
    - bezpieczeństwo kontraktów w Quorum
    - wykorzystanie koncepcji wiedzy zerowej w warstwie zabezpieczeń sieci (ang. *zero-knowledge security layer*, ZSL)
    - kontrakty prywatne i z-kontrakty

4. Podsumowanie

    - zalety, wady i ograniczenia implementacji poufności w Quorum
    - przykładowe zastosowania blockchain Quorum
    - aktualne plany rozwoju Quorum

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl