

Kod szkolenia: **ETHER**

Tytuł szkolenia: **Praktyczne wykorzystanie blockchain na przykładzie Ethereum**

Dni: 3

## Opis:

### Adresaci szkolenia

Osoby, które w praktyce chcą uruchomić i poznać zasady działania blockchain. 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 oraz utworzą i zrealizują różnorodne transakcje we własnym łańcuchu bloków.

### Mocne strony szkolenia

Podczas warsztatów uczestnicy:

- utworzą własny blockchain w środowisku Ethereum,
- uruchomią proces kopania bloków,
- wykonają transakcje pomiędzy kontami,
- utworzą inteligentne kontrakty do realizacji funkcji współdzielonego portfela, własnej kryptowaluty oraz zdecentralizowanej organizacji autonomicznej,
- zaimplementują własne kontrakty w języku Solidity oraz umieszczą je w blockchain.

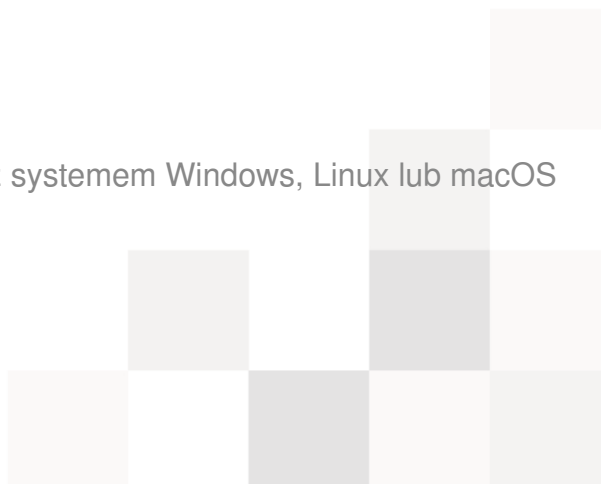
### Wymagania

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

### Specjalne wymagania techniczne

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

### Parametry szkolenia



3 \* 8 godzin (3 \* 7 godzin netto) wykładów i warsztatów.

## Program szkolenia:

### 1. Wprowadzenie

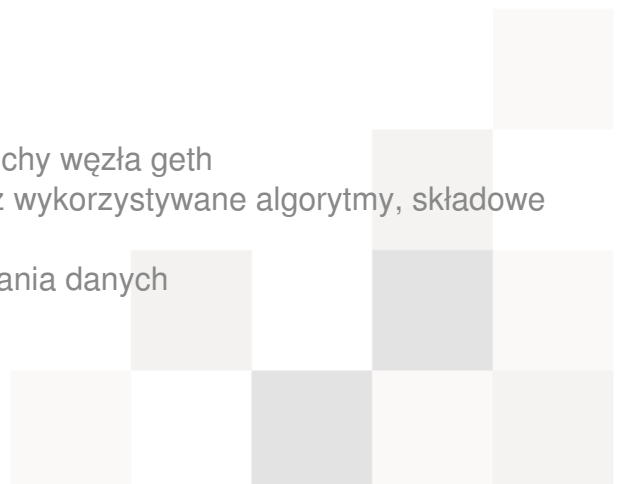
- transakcje w systemach scentralizowanych, zdecentralizowanych i rozproszonych
- zapewnianie wiarygodności transakcji
- czym jest blockchain

### 2. Zasady działania blockchain

- blockchain jako rozproszona baza danych
- integralność, uwierzytelnienie, niezaprzeczalność i poufność a blockchain
- funkcje skrótu, ich właściwości i zastosowania (SHA-256, SHA3, Keccak)
- algorytmy asymetryczne oparte o krzywe eliptyczne
- koncepcja i realizacja podpisu cyfrowego (algorytm ECDSA)
- sieci P2P (*peer to peer*)
- elementy systemu opartego o blockchain: przechowywanie danych, protokół komunikacyjny i algorytm konsensusu
- adresy użytkowników i sposób ich tworzenia
- transakcja w blockchain i jej elementy, proces zatwierdzania transakcji
- bezpieczeństwo klucza prywatnego
- tworzenie bloków i kopanie (*mining*)
- dowód pracy (*proof of work*, PoW), dowód stawki (*proof of stake*, PoS) i inne techniki
- blockchain jako rejestr transakcji, kryptowaluty
- aplikacja jako element blockchain, inteligentne kontrakty
- problem centralizacji mocy obliczeniowej, rozgałęzień
- zmiany zasad działania sieci blockchain (*soft fork* i *hard fork*)
- charakterystyka wybranych blockchain: Bitcoin, Litecoin, Dash, Ripple, projekty z rodziny Hyperledger i Ethereum

### 3. Ethereum i jego działanie

- architektura Ethereum
- implementacje węzłów Ethereum, cechy węzła geth
- budowa blockchain w Ethereum oraz wykorzystywane algorytmy, składowe transakcji
- techniki przechowywania i wyszukiwania danych



- blok genesis i uruchomienie prywatnego łańcucha bloków w Ethereum
- typy kont w Ethereum, tworzenie kont
- uruchomienie węzła, komunikacja za pomocą IPC i RPC
- komunikacja pomiędzy węzłami
- proces kopania (*mining*) bloków
- zlecanie i zatwierdzanie transakcji
- Ether i gas jako paliwo dla transakcji w blockchain
- praca w konsoli geth oraz z klientem Ethereum Wallet/Mist
- światowa sieć Ethereum i Ethereum Classic

## 4. Inteligentne kontrakty (*smart contracts*) w Ethereum

- język Solidity
- podstawy działania i tworzenia kontraktów
- maszyna wirtualna Ethereum
- działanie przykładowych kontraktów: współdzielony portfel, token, zdecentralizowana organizacja autonomiczna (*democratic autonomous organization, DAO*)
- implementacja kontraktu dla tokenu
- bezpieczeństwo kontraktów, przykładowe błędy implementacyjne w kontraktach
- aplikacje rozproszone Dapps
- komunikacja z siecią blockchain poprzez przeglądarkę

## 5. Podsumowanie

- zalety i wady blockchain w kontekście jego zastosowań
- ograniczenia i mity o blockchain: zużywane zasoby, brak pełnego zaufania, odpowiedzialność i szkodliwe działania użytkowników, identyfikacja i anonimowość
- blockchain jako część rozproszonej sieci Internet: rozproszone systemy plików (Swarm) i rozproszona komunikacja (Whisper)
- możliwe kierunki rozwoju blockchain

