Wykorzystanie technologii blockchain do budowy bezpiecznego systemu aukcji elektronicznych

Wstęp

Cel pracy

Zakres pracy

Rozdział I - Wprowadzenie do problemu

1.1 **Modele aukcji** – krótkie przedstawienie najczęściej spotykanych w literaturze i praktyce typów aukcji, i.e. aukcji angielskiej, holenderskiej, Vickreya, etc.

1.2 **Blockchain** – przedstawienie idei, założeń i cech technologii blockchain

1.3 **Smart Contract** – przedstawienie i wyjaśnienie zasad działania inteligentnych kontraktów

1.4 **Zalety i wady** wynikające z wykorzystania technologii blockchain do zaimplementowania rozważanego systemu

Rozdział II - Analiza wymagań biznesowych

Wysoko poziomowa analiza wymagań i pożądanych właściwości systemu, która na celu ma określenie cech, które poszukiwane będą w trakcie porównania dostępnych technologii w następnym rozdziale.

2.1 **Grupy użytkowników** – przedstawienie aktorów-użytkowników projektowanego systemu

2.2 **Przypadki użycia** - określenie celów użytkowników, dostępnych dla nich operacji i ich przebiegu za pomocą standardowej analizy przypadków użycia

2.3 **Scenariusze i stany systemu** – pogłębienie, lub poszerzenie analizy z poprzedniego podrozdziału za pomocą dodatkowych narzędzi

Rozdział III - Porównanie dostępnych technologii, ich własności i właściwości

3.1 **Permission-less vs Permissioned Blockchain** – przedstawienie i porównanie publicznych i prywatnych sieci blockchain, ich cech i ograniczeń technologicznych. Związane z tym tematem jest też wybór cyklu pomiędzy order-execute a execute-order

3.2 **Byzantine Fault Tolerant, a Crash Fault Tolerant** – wyjaśnienie tych niezwykle istotnych w kontekście sieci blockchain, ale także wielu innych systemów rozproszonych, własności, ale też analiza kosztu ponoszonego, by je uzyskać

3.3 **Otwartość, bezpieczeństwo, a wydajność** – analiza wymienionych właściwości i korelacji między nimi w kontekście dostępnych technologii, tego jak aby poprawić jedną z nich zawsze poświęcić w pewnym stopniu musimy inną, albo obie inne

3.4 **Podsumowanie** – przedstawienie w zwięzły sposób, np. w postaci tabeli, cech przeanalizowanych przeze mnie technologii oraz omówienie procesu decyzyjnego stojącego za ostatecznym wyborem Hyperledger Fabric

Rozdział IV - Projekt systemu z uwzględnieniem wybranej technologii

4.1 **Przestawienie komponentów systemu** – węzłów działających i współpracujących w obrębie sieci opartej na Hyperledger Fabric, ich przeznaczenia i sposobu działania

4.2 **Diagramy sekwencji, komunikacji** – użycie tych standardowych diagramów notacji UML do zaprojektowania i wyjaśnienia działania systemu, w szczególności transakcji i ich zatwierdzania

4.3 **Diagramy stanów –** poszerzenie analizy z poprzedniego podrozdziału za pomocą kolejnego typu diagramów. W toku powstawania pracy mogą okazać się potrzebne dodatkowe typy diagramów

4.4 **Ustalanie konsensusu –** opis głównego algorytmu odpowiadającego za osiągnięcie konsensusu w sieci Hyperledger Fabric z uwzględnieniem mojej konkretnej implementacji

Rozdział V - Implementacja

5.1 **Opis technologii** – analiza i wyjaśnienie najciekawszych i najistotniejszych niskopoziomowych aspektów systemu i samej technologii Hyperledger Fabric

5.2 **Omówienie kodów źródłowych** – przedstawienie i objaśnienie kluczowych fragmentów kodu źródłowego

Rozdział VI - Analiza bezpieczeństwo zaimplementowanego systemu

6.1 **Wybrane ataki** – przedstawienie częstych, rozpoznanych już ataków na sieci blockchain, które wykorzystują ich wady, opisywanych w literaturze, lub znanych z praktyki

6.2 **Zachowanie systemu –** określenie poziomu wrażliwości zaimplementowanego przeze mnie systemu na ataki przedstawione w poprzednim podrozdziale

Podsumowanie