Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Blockchain-basierte Trusted Third Party Mobile App für Wetten/Abmachungen

Themenbereiche: Software-Erstellung

Studierende: Fischlin Bruno, Hartmann Kay

Dozent: Denzler Alexander

Experte: Schmidiger Rolf

Wirtschaftspartner: -

Keywords: Mobile App, Blockchain, Smart Contract, Use-Cases, Wetten

1. Aufgabenstellung

Man nehme folgende beispielhafte Situation, um die Problemstellung zu illustrieren: Sie sind mit Freunden unterwegs, verbringen einen unterhaltsamen Abend und möchten spontan eine Wette abschliessen. Wie kann nun sichergestellt werden, dass keine der Parteien die Wette und deren Konditionen im Nachhinein manipuliert? Dafür könnte man die Rahmenbedingungen der Wette schriftlich festhalten und von einem Notar beglaubigen lassen. Spontan einen Notar zu finden und die damit verbundene Zeit zu investieren, um ein Dokument aufzusetzen und dieses verifizieren zu lassen, ist jedoch sehr unwahrscheinlich. Daher entstand die Idee, dieses Dokument virtuell in Form eines Smart Contracts aufzusetzen und diesen auf die Blockchain zu schreiben.

2. Ergebnisse

Im Rahmen der Bachelor-Diplomarbeit (BDA) werden folgende Ergebnisse erarbeitet:

- **Evaluation Blockchain-Technologie:** Evaluation, welche Blockchain-Technologie sich am besten für die Umsetzung der Aufgabenstellung unter erarbeiteten Kriterien eignet.
- **Requirements Engineering:** Ermittlung, welche Komponenten für die Umsetzung der Aufgabenstellung benötigt werden.
- **Systemarchitektur:** Evaluation, welche Komponenten eingesetzt werden um die Aufgabenstellung mit dem ermittelten Requirements Engineering umsetzen zu können.
- **Identifikationskonzept:** Benutzer sollen sich eindeutig identifizieren und Wallets mit ihren Benutzeraccounts verbinden können.
- **Smart Contracts:** Entwurf und Implementierung eines Smart Contracts, welcher den Use Case Wette modelliert und für den Gebrauch nutzbar macht.
- **Mobile Applikation (Pilot):** Entwicklung einer Android Mobile App, welche die erarbeiteten Komponenten der Systemarchitektur verwendet, um so die Funktionalität einer Plattform für Wetten/Abmachungen unter Freunden anzubieten.
-

3. Lösungskonzept

Die Herausforderung der Arbeit liegt darin, dass zuerst Wissen über Blockchain und die umgesetzten Technologien erarbeitet werden muss. Dies beinhaltet die Smart Contracts, mit welchen der Use Case Wette/Abmachungen umgesetzt werden soll. Dies ist insbesondere

Herausfordernd, da Smart Contracts und Interaktionen mit der Blockchain Kosten mit sich tragen und somit die Lösung für die Benutzer optimiert werden muss.

3.1 System-Architektur

Es muss eine komplette System-Architektur mit den verschiedenen Komponenten Web-Server, Mobile App und Smart Contract umgesetzt und aufeinander abgestimmt werden. Die zu entwickelnden Komponenten, sowie deren Interaktion zwischen einander ist in **Error! Reference source not found.** zu sehen. Die Mobile App vereint alle erstellten Komponenten, um die volle Funktionalität des Systems für die Benutzer zu ermöglichen.

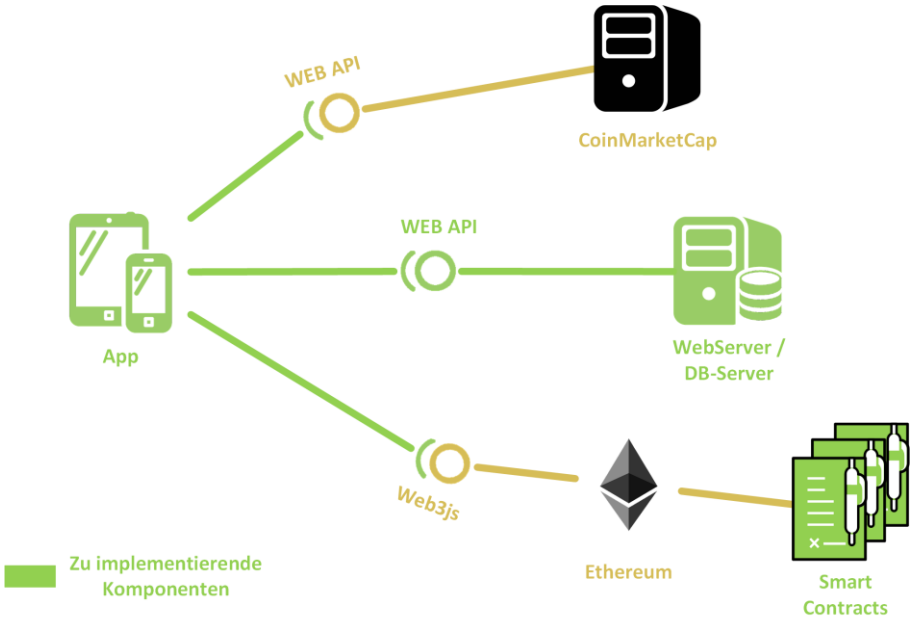

Abbildung 1: System-Architektur

Einige Screens der Mobile App sind in **Error! Reference source not found.** zu sehen. In der Mobile App können Benutzer sich registrieren/einloggen, ein Ethereum Wallet erstellen oder ein bestehendes vernetzen, diesen Ethereum Account verwalten, sie können andere Benutzer der Mobile App als Freunde hinzufügen, Wetten (und somit Smart Contracts) mit den hinzugefügten Freunden erstellen, diese in einer Übersicht verwalten und schliesslich mit den erstellen Wetten interagieren.

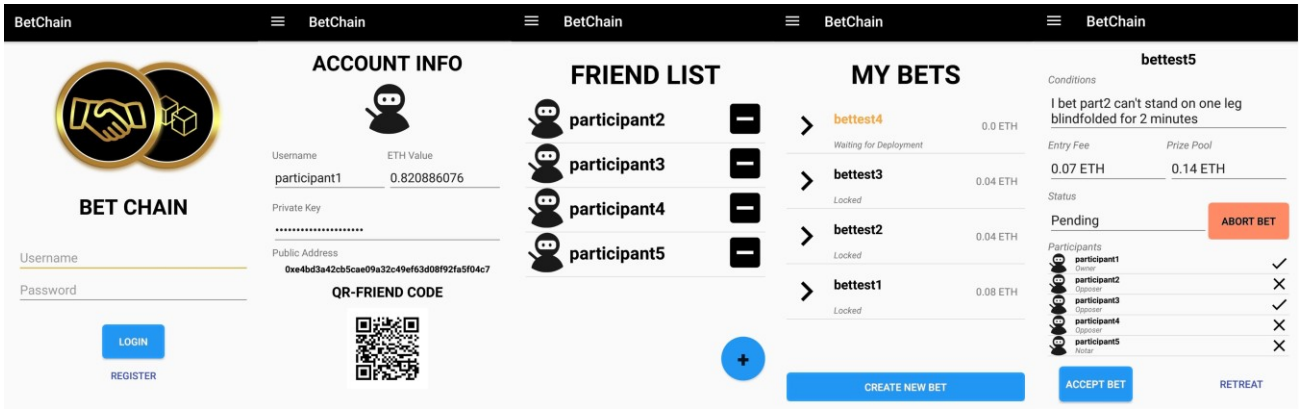

Abbildung 2: Mobile App Screenshots

4. Spezielle Herausforderungen

Eine Herausforderung brachte die Ermittlung und Umsetzung der System-Architektur. Das ganze System musste so entwickelt werden, dass die Komponenten aufeinander abgestimmt sind. Dies forderte auch Wissen in verschiedenen Bereichen wie PHP und SQL für den Web-Server, als auch Android App-Entwicklung für die Mobile App.

Die Programmierung des Smart Contract für den Use Case Wette stellte eine spezielle Herausforderung dar, da dies aufgrund der Auswahl von Ethereum in einer noch nicht bekannten Sprache (Solidity) getan werden musste. Diese ist zwar an Java angelehnt, jedoch variiert die Art wie programmiert wird stark. Die Funktionen mussten stark optimiert werden, da Änderungen, welche auf dem Smart Contract und somit auf der Blockchain getätigt werden, Kosten für den Benutzer mit sich bringen und diese Kosten mit grösserem Aufwand/Komplexität der Funktion wachsen.

Die Erstellung der Smart Contracts auf der Blockchain brachte eine weitere Herausforderung mit sich, auf der Blockchain dauert es eine Weile bis Blöcke und somit die Informationen auf die öffentliche Chain geschrieben werden. Solange der Smart Contract noch nicht gemined wurde, existiert dieser nur als Transaktions-Hash. Der Smart Contract ist somit zu diesem Zeitpunkt noch auf keine Weise mit einem Ethereum Account verbunden. Der Transaktions-Hash ist bei der Erstellung nur der App, welche die Erstellung angefordert hat, bekannt. Wenn somit die App während der Erstellung einer Wette geschlossen wird, geht diese Information verloren. Auch die Teilnehmer der Wette und somit des Smart Contracts besitzen kein Wissen darüber, an welchen Wetten sie teilnehmen. Die Blockchain hat diese Informationen zwar öffentlich zugänglich, man müsste dazu aber die Blockchain danach durchsuchen. Dies ist mit enormen Zeitaufwand verbunden und somit nicht geeignet. Deshalb wurden einige Meta-Informationen der Wetten auf dem Web-Server persistiert, um den Informationsverlust zu verhindern und eine Synchronisation von Informationen zu ermöglichen.

5. Ausblick

Da die Rechtslage in der Schweiz das öffentliche Wetten um Geld verbietet, kann die Mobile App im aktuellen Zustand nicht veröffentlicht werden. Jedoch könnte man den Use Case anpassen und auf dem entwickelten System aufbauen.

Gegenstandsverleih:

Bei einem Verleih-Service geht es darum, dass der Besitzer eines Gegenstandes diesen an jemandem verleihen kann und zur Absicherung ein Depot für diesen Gegenstand hinterlegt wird, dies könnte über einen Smart Contract verwaltet werden.

Ideenfindung in einer Unternehmung:

Unternehmen können ein Wettsystem verwenden, um so beispielsweise Firmenentscheide besser zu steuern. Dies könnte getan werden, indem die Firma ihren Mitarbeitern eine gewisse Anzahl an Wett-Tokens (Firmeninterne Pseudowährung) für einen kommenden Entscheid zum Einsatz gibt und diese dann selbst entscheiden können, wie viel dieser Währung sie auf welchen Entscheid setzen. Dies führt dazu, dass Benutzer automatisch mehr Zeit und Recherche in ihre Entscheide investieren. Die Pseudowährung könnte firmenintern beispielsweise für ein Belohnungssystem in Form von Essensgutscheinen eingetauscht werden, was die Benutzer weiter motiviert an diesem System teilzunehmen, in ihre Entscheide Zeit zu investieren und sich untereinander darüber auszutauschen.