# Lastenheft

AOS Security Token

| Version | Datum |
|---|---|
| **1.0** | 24. Januar 2019 |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 Ausgangssituation

Im Rahmen eines STO möchte Azhos einen ERC20-Token in Form eines Smart Contract auf der öffentlichen Ethereum Blockchain herausgeben. In einem noch zu definierenden Zeitraum wird Azhos einen Teil seiner Gewinne an Token Halter ausschütten, was den Token zu einem Security Token macht. Der Token ist ein „Security Token“. Nach der Ausgabe soll der Token von den Token Inhabern gehandelt werden können. Der Handel soll dabei nicht nur direkt zwischen Haltern des „AOS-Token“ stattfinden können, sondern auch auf Börsen/Exchanges. Da das Konzept der Security Token auf einer Blockchain relativ neu ist, gibt es noch kaum oder keine gesetzlichen Frameworks. Der AOS-Token soll zu einem der ersten legalen Token mit Security-Funktion werden. Exchanges und Börsen unterliegen Gesetzlichen Bestimmungen zu AML und KYC, deshalb muss der AOS-Token Smart Contract Funktionen mitbringen die diesen Ansprüchen gerecht werden. Azhos beauftragt für die Erstellung des AOS-Security Token Contracts die „micobo GmbH“. Die micobo GmbH wird den Ethereum Token Smart Contract nach den Vorgaben von Azhos bauen und parallel mit Börsen/Exchanges über die Funktionen verhandeln, die der Token Contract mitbringen muss, um öffentlich gelistet werden zu können.

# 2 Zielsetzung

Azhos benötigt ein ERC20 kompatibles Smart Contract Konstrukt, welches auf gängigen Börsen und Exchanges gelistet werden darf. Ein ERC-20 kompatibler Smart Contract, der die Erstellung, den Austausch und den Verkauf des Azhos Security Token verwaltet. Der Token soll im Rahmen eines Security Token Offering verkauft werden, Funktionen zur Ausschüttung des Gewinns bereitstellen, Börsen Whitelisting-Funktionalität bieten und Tokenholder ihre Tokens ERC20 kompatibel verwalten lassen können.

# 3 Produkteinsatz

Der Smart Contract wird von Azhos dazu verwendet werden den AOS-Token in Umlauf zu bringen. Dafür werden die Tokens von Azhos erstellt(gemintet) und in einem STO in mehreren runden verkauft. Die Aufgabe der KYC- und AML-Maßnahmendurchsetzung vergibt Azhos an eine externe Entität. Diese wird in einem anschließenden Schritt die Ethereum-Wallet-Adresse mit einem positiven Eintrag in der AOS-Token Whitelist versehen. Die Entität die in die Whitelist schreibt, besitzt diese nicht, Sie kann vom Custodian ausgetauscht werden. Dieser Custodian („Treuhänder“) bestimmt darüber, wer Einträge in der Whitelist verändern darf und kann diesen austauschen. Token-Besitzer werden den Smart Contract dazu benutzen Tokens zu tauschen oder zu halten. Börsen und Exchangen werden den Token mittels der ERC20-Funktionalität listen. In der Regel überträgt ein Token-Besitzer die Tokens an die Ethereum-Wallet-Adresse der Börse/Exchange, dort kann er mit den Tokens handeln. Sollen die Tokens von der Börse zurück auf eine reguläre Ethereum-Wallet-Adresse übertragen werden, muss sicher gegangen werden, dass die Know-Your-Customer Kette nicht unterbrochen wird. Die Börse oder Exchange wird eine vom Smart Contract bereitgestellte Whitelist-Funktionalität benutzen, um zu überprüfen ob die Zieladresse ebenfalls mit KYC-Maßnahmen bekannt ist.

## 3.1 Rollen

**Auflistung:**

1. Azhos
2. Custodian
3. Exchange
4. KYC-Entity
5. Token Holder

---

**Azhos:** Der Besitzer des Smart Contracts.

**Custodian:** Bestimmt darüber wer in die Whitelist schreiben darf und damit die KYC-Maßnahmen durchführt.

**Exchange:** Eine Börse auf der der AOS-Token gehandelt werden kann. Prüft anhand der Whitelist ob der User, der Token erhalten soll auch KYC und AML durchlaufen hat.

**KYC-Entity:** Führt KYC-Maßnahmen durch und verknüpft eine Ethereum Wallet Adresse mit einer Identität. Fügt die Wallet Adressen in die Whitelist ein.

**Token Holder:** Besitzer von AOS-Token. Kann seine Tokens mit den Standard-ERC20 Funktionen verwalten. Ruft in Intervallen den von seinen AOS-Token bereitgestellten Gewinnanteil von Azhos über den Smart Contract in Ether ab.

## 3.2 Aktivitäten:

**Auflistung:**

1. Check if Smart Contract is Paused
2. Check if User is Whitelisted
3. ERC20 Functions
4. Pay out Tokens to Address
5. Create Tokens
6. Whitelist User
7. Pause Smart Contract
8. Change Whitelist Manager
9. Call Dividend Contract
10. Check Events

---

**Check if Smart Contract is Paused:** Bevor ERC20 Funktionen ausgeführt werden, prüft der Smart Contract ob diese nicht für den Moment ausgesetzt wurden.

**Check if User is Whitelisted:** In der Whitelist wird geprüft, ob ein positiver Eintrag für den entsprechenden User vorliegt. Gilt für den Sender als auch für den Empfänger der Tokens.

**ERC20 Functions:** Enthält alle ERC20 Standardaktivitäten. Vor Ausführung wird geprüft ob der Aufrufende und Mögliche Empfänger einen positiven Eintrag in der Whitelist vorweisen können. Zusätzlich können die ERC20 Funktionen nur ausgeführt werden wenn

diese nicht pausiert oder für den Moment ausgesetzt sind.

**Pay out Tokens to Address:** Wenn ein User seine AOS-Token von einem Exchange fortbewegen will, muss er die Exchange anweisen diese an eine Ethereum Wallet Zieladresse zu übertragen. Exchanges transferieren die Tokens von ihrer Ethereum Token Wallet zu der der Zieladresse, dafür benutzen sie die ERC20 Funktionen. Da Exchanges die Einhaltung gesetzlicher Bestimmungen zu AML und KYC überprüfen müssen, prüfen sie vor Ausführung auf einen positiven Eintrag in der AOS-Token Whitelist.

**Create Tokens:** Für den STO wird Azhos Tokens im AOS-Token Smart Contract erstellen. Diese Tokens werden verkauft.

**Whitelist User:** Nachdem ein Tokenkäufer ausreichende KYC und AML Verfahren durchlaufen hat, wird ein Positiver Eintrag in der Whitelist des AOS-Token-Smart Contracts erstellt. Die Überprüfung und Eintragung erfolgt vom Manager der AOS-Token Smart Contract Whitelist.

**Pause Smart Contract:** Die ERC20 Funktionalität des AOS-Token Smart Contract können von Azhos ausgesetzt werden.

**Change Whitelist Manager:** Derjenige der in die AOS-Token Smart Contract Whitelist schreiben darf, kann vom Custodian ausgetauscht werden.

**Call Dividend Contract:** Der angefallene Gewinn kann über den Smart Contract in Ether abgerufen werden.

**Check Events:** Zur Überwachung und Überprüfung werden die Aktionen relevanter Smart Contract Funktionen mit Events kontinuierlich nachvollzogen.

## 3.3 Diagramme

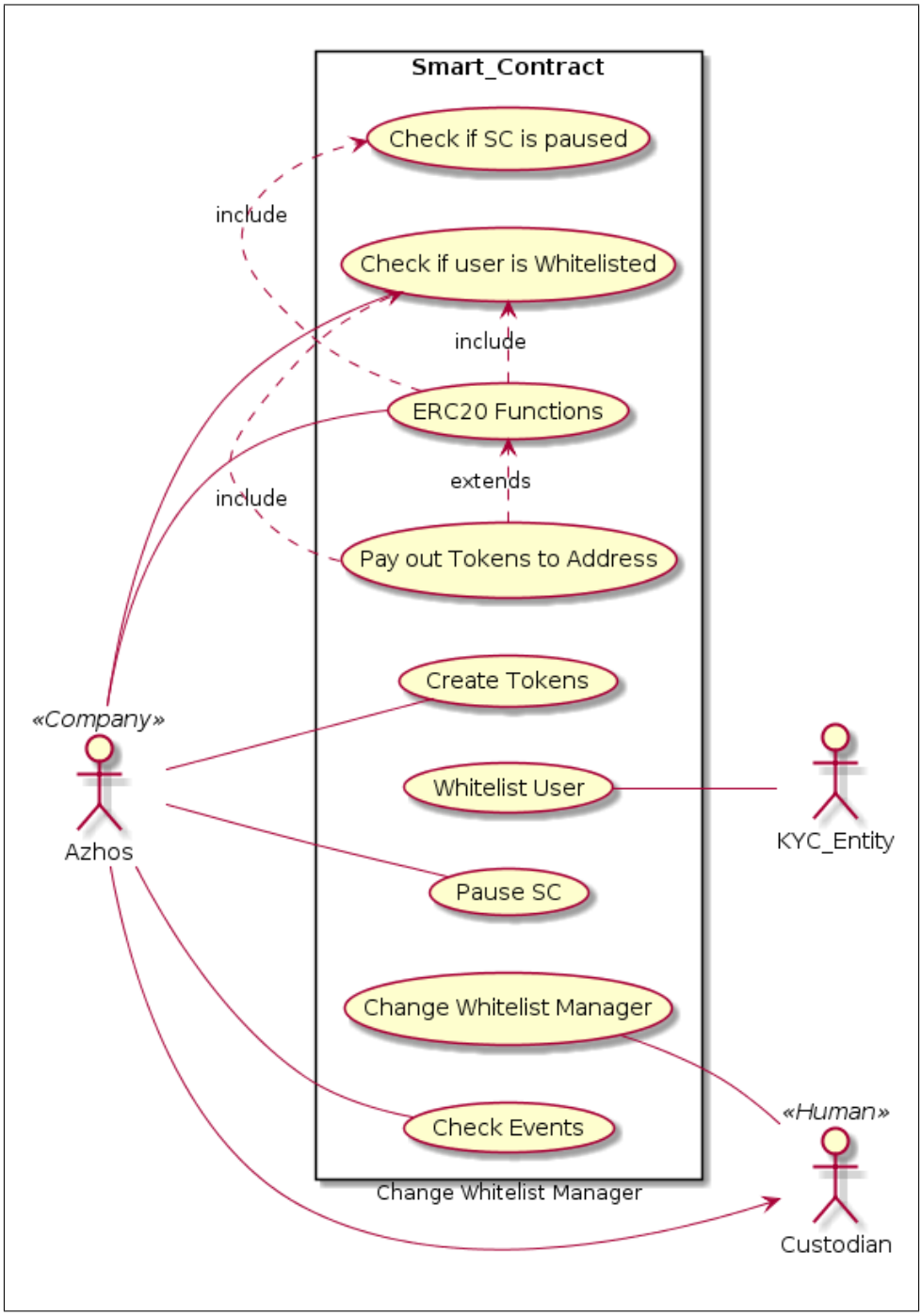


Abbildung 1: Azhos-Custodian-KYC_Entity

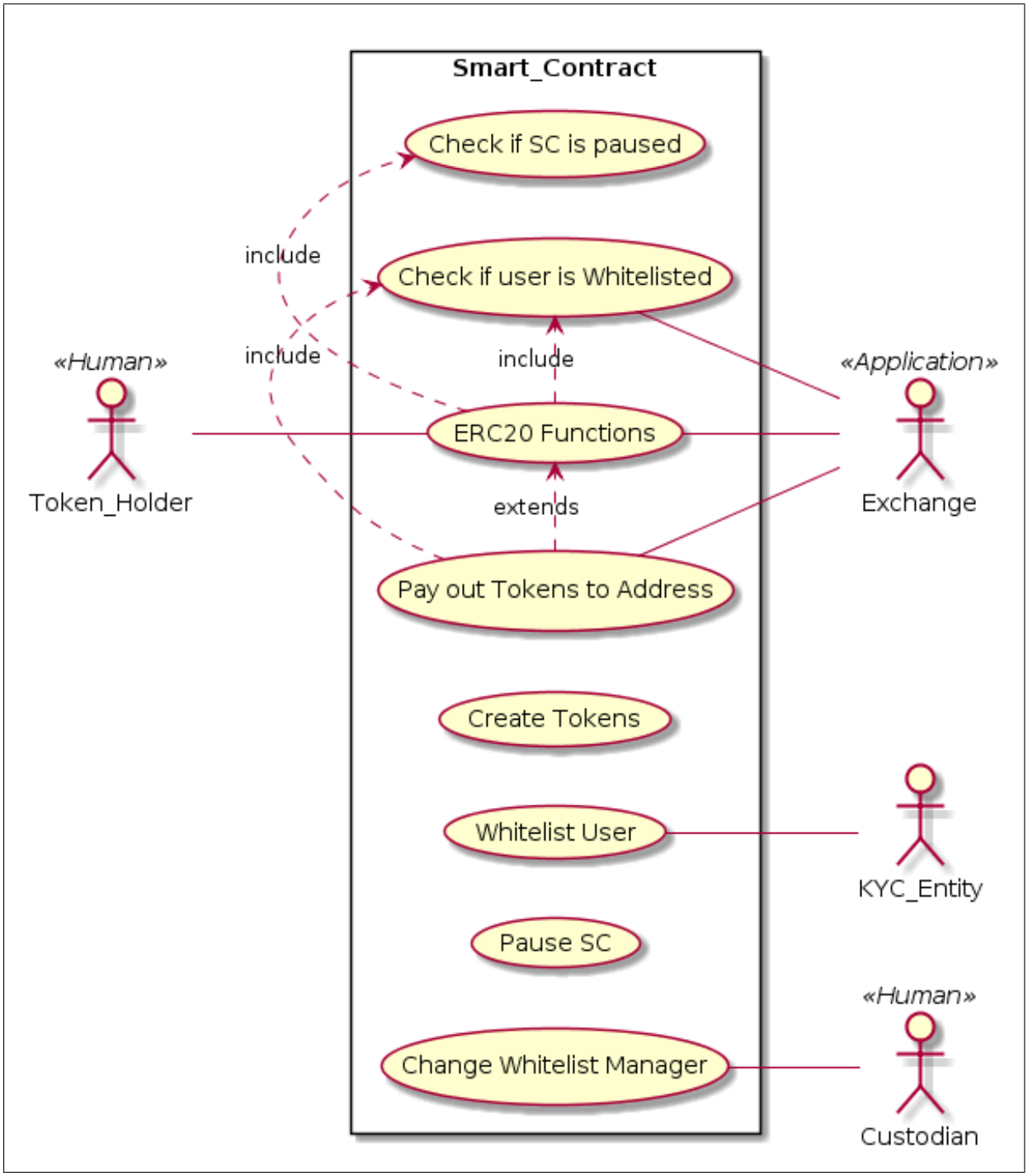


Abbildung 2: Exchange-Token_Holder-KYC_Entity-Custodian Activity

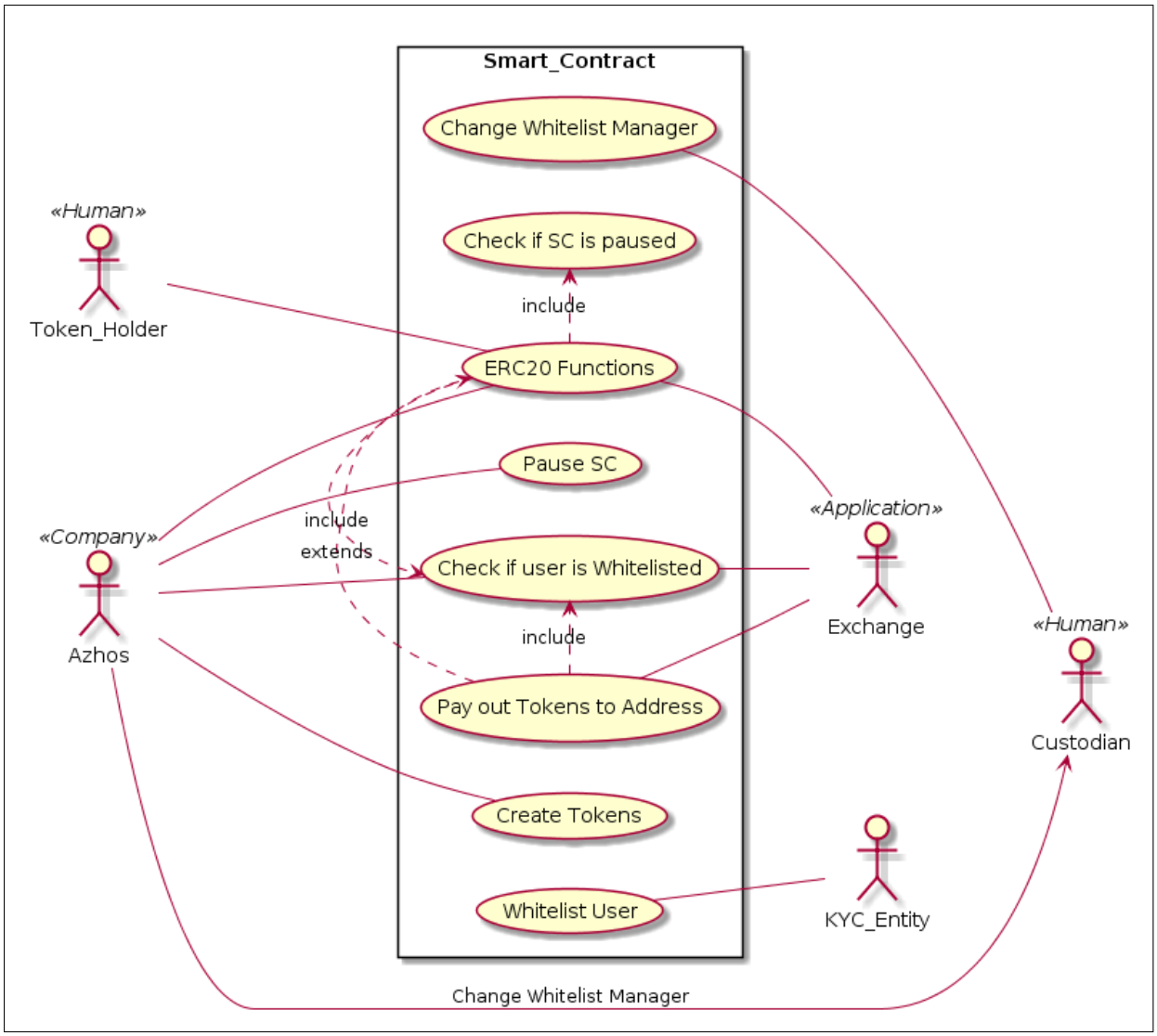


Abbildung 3: Combined Activity

# 4 Funktionale Anforderungen

| Item | Kurzbeschreibung |
|---|---|
| **FA100** | ERC20 Functions |
| | |
| **FA200** | Whitelisting |
| **FA210** | Whitelist User Address |
| **FA220** | Unwhitelist User Address |
| **FA230** | Change Whitelist Provider |
| **FA240** | Change Whitelist |
| | |
| **FA300** | Smart Contract Brake |
| **FA310** | Pause Smart Contract |
| **FA320** | Unpause Smart Contract |
| | |
| **FA400** | Ownership |
| **FA410** | Change Owner |
| | |
| **FA500** | Call Dividend Contract |
| | |
| **FA600** | Events |

# 5 Nichtfunktionale Anforderungen

- *FA100*, *FA200*, *FA300* und *FA400* sollen möglichst konstanten Gasverbrauch haben.
- Für *FA100*, *FA200*, *300* und *FA400* sollen die Kosten in Ether und Gas, für Smart Contracts und Calls im verhältnismäßigen Rahmen sein.
- Es soll maximal eine(1) bis zwei(2) Blockzeiten der öffentlichen Ethereum Blockchain dauern(circa zwanzig(20) Minuten), von der legitimen Transfer Anweisung in Verbindung mit Whitelisting-Überprüfung, bis zur Übertragung und Gutschrift auf die als Ziel angegebene Adresse.
- Der Token muss dem Anspruch gängiger Handelsplattformen genügen, damit er dort gelistet und verkauft werden darf.
- Der Smart Contract sollte auf einen Gewinnausschüttungsvertrag zeigen oder Funktonalität bereitstellen um diesen direkt abzurufen.
- Die implementierte Lösung für *FA200* soll die Möglichkeite haben, zwischen einer dezentralisierten Lösung in Form eines Smart Contracts, auf eine zentralisierte Lösung(Off Chain) umzuschalten.
- Die implementierte Lösung für *FA200* muss berücksichtigen dass die Kontrolle nicht dauerhaft im besitz einer Entität bleibt, die nicht Azhos ist und wirtschaftliches Interresse am AOS-Token hat oder haben könnte.

# 6 Lieferumfang

## 6.1 micobo

- Ein oder mehrere Smart Contracts in unkompiliertem Solidity Code, geschrieben in der Mindestversion-Release „0.5.2“(null fünf zwei).
- Smart Contract Deployment auf der Öffentlichen Ethereum Main Chain
- Ausführliche Dokumentation über die Bedienung und Verwendung des oder der Smart Contracts, in Text und UML-Form.
- Übergabe des Besitzes(ownership) der oder des Smart Contract auf der Ethereum Blockchain.
- Ein Off Chain KYC-Service
- Konzept für On-Chain Whitelist
-

## 6.2 Azos

- Wertprospekt
- Kontakte Azhos-FMA
- Spezifikationen
-

## 6.3 Orbit

-

# 7 Projektphasen und Meilensteine

## 7.1 Aufgaben

- Absprache mit gängigen Exchanges/Börsen welche Mechanismen im Smart Contract Code benötigt werden.
- Programmierung des Smart Contract Konstrukts
- Minting der Tokens
- Whitelisting und KYC
- Verkauf der Tokens

## 7.2 Meilensteine

1. Entwurf micobo (Pflichtenheft), ERC20, Whitelistfunktion
2. Azhos Auftragsbeginn
3. Programmierung ERC20
4. Fertigstellung
5. Abnahme
6. KYC der (Vor)-Registrierten Tokenkäufer
7. Whitelisting
8. Token Minting/Kreation
9. AZHOS Supply-Chain Day pre Minting
10. Verkauf der Tokens, STO Runde 1
11. Verkauf der Tokens, STO Runde 2
12. Verkauf der Tokens, STO Runde 3

# 8 Offene Punkte

1. Es ist vorgesehen das *FA200* On Chain(dezentral) über einen Smart Contract abgewickelt wird. Um dem Meilenstein des Azhos-Supply-Chain Day gerecht zu werden, wird jedoch zunächst auf eine zentralisierte Lösung von micobo gesetzt. Die Dezentralisierte Lösung soll zu einem späteren Zeitpunkt im Lebenszyklus des AOS-Smart Contract implementiert werden. Es beudeutet, dass es möglich sein muss zischen zentralisierter und dezentralisierter Lösung umzuschalten.
2. 
3. 
4. 

## 8.1 Fragen

1. Wer wird zur KYC-Entität ernannt?
2. Wer wird die Treuhänderische Funktion mit der Hoheit über die Whitelist übernehmen?
3. Die AOS-Token sollen zu einem späteren Zeitpunkt als Kollateral auf einer geplanten Finanzierungsplattform dienen. Inwiefern trägt der Smart Contract dem Rechnung?

# 9 Abnahmekriterien und Qualitätsanforderungen

- ERC20 Standardfunktionalität implementiert und Funktionsfähig.
- Smart Contract is pausierbar.
- Zentralisierte Whitelist vollständig Funktionsfähig.
- Schalter zum Umschalten auf dezentralisierte Whitelist implementiert.
- On Chain/Off Chain Abfrage mit Beantwortung der Abfrage erfolgt innerhalb von 20 Minuten.
- Code Audit des Smart Contracts erfolgreich.
- Exchanges oder Börsen haben die Implementierung der Whitelist Funktionalität akzeptiert.
- Dokumentierung in UML und Text.
- Der Smart Contract ist nach Best Practices Programmiert und Abweichungen davon begründet dokumentiert.
-