

ONTWIKKELING VAN EEN GEDISTRIBUEERDE BLOCKCHAIN

Bouw een blockchain implementatie zonder gebruik te maken van bestaande blockchain libraries.

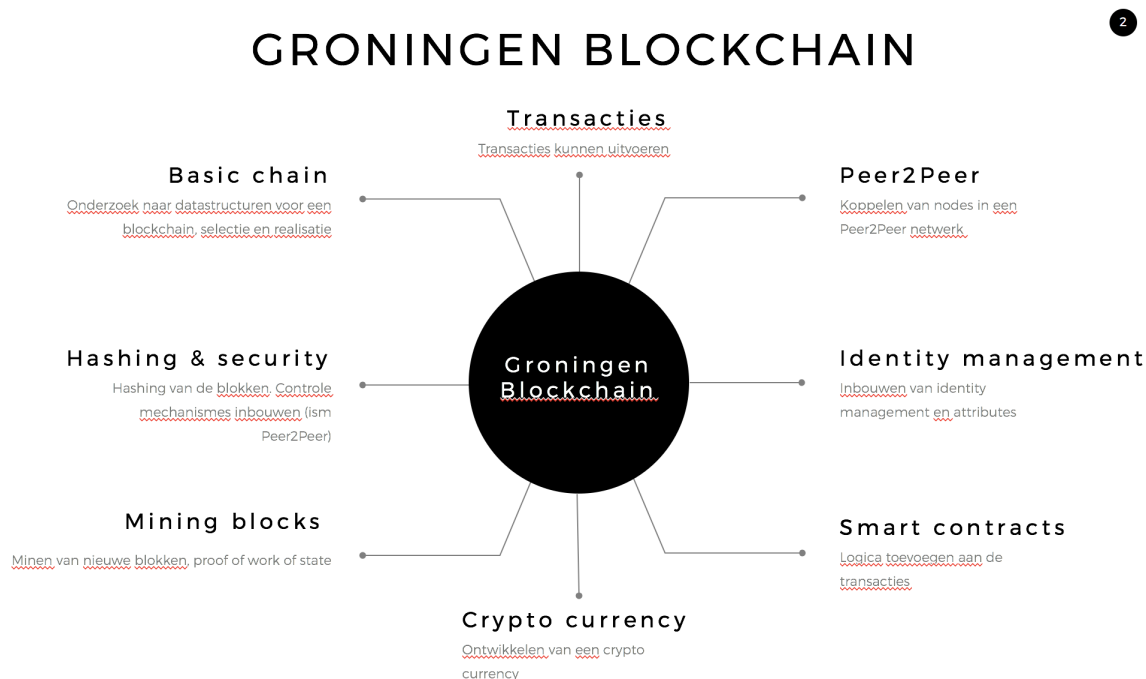
Organisatie

Quintor is een toonaangevend bedrijf op het gebied van Agile software development, Enterprise Java / .NET technologie en mobile development. Wij hebben sinds onze oprichting in 2005 een gezonde groei doorgemaakt en hebben inmiddels 150 personeelsleden. Vanuit onze vestigingen in Amersfoort, Groningen en Den Haag ondersteunen wij onze klanten bij de uitdagingen die grootschalige enterprise projecten met zich meebrengen. Quintor beschikt over een Software Factory waarin wij inhouse projecten voor onze klanten uitvoeren.

Probleemstelling

Voor de ontwikkeling van een blockchain dienen een aantal software componenten te worden ontwikkeld:

1. Een gegevensstructuur voor een node
2. Hashing functionaliteit
3. Mining van blokken
4. Synchronisatie van nodes (peer2peer)
5. Transacties
6. Identity management
7. Eventueel een crypto currency en smart contracts.



Deze opdracht richt zich op het ontwikkelen van een gedistribueerd netwerk(4) en identity management(6).

De overige onderdelen zullen in andere opdrachten gerealiseerd worden.

Aanpak

Allereerst worden in afstemming met de opdrachtgever (Johan Tillema) de uitgangspunten bepaald voor de te ontwikkelen blockchain. Deze gaan over snelheid, beveiligingsniveau en toepassingsmogelijkheden.

Vervolgens worden voor 4) en 6) de verschillende architectuur alternatieven in kaart gebracht. Dit wordt gedaan door het uitvoeren van literatuur onderzoek en door te kijken welke keuzes zijn gemaakt in andere blockchain implementaties zoals Ethereum, Hyperledger of BitCoin.

Samen met de opdrachtgever wordt een keuze gemaakt voor de toe te passen architectuur.

Vervolgens wordt een eerste gedistribueerde blockchain geïmplementeerd in Java of in .NET.

Achtergrond probleemstelling

Blockchains garanderen integriteit van data door gebruikmaking van cryptografische primitieven zoals hash functies en public-private key cryptografie. Door het ondertekenen van berichten wordt authenticiteit gegarandeerd en de hash functies zorgen voor een keten die mutaties van oude data onmogelijk maakt.

Op basis van deze onderzoeksvragen wordt een proof of concept verwacht. Op te leveren producten: een basaal blockchain implementatie die aan de volgende eisen voldoet;

- 1) er worden geen blockchain libraries gebruikt
- 2) het moet resistent tegen aanvallen zijn
- 3) het moet gedistribueerd zijn
- 4) er wordt op decentrale wijze consensus bereikt