

VENNSTER



Creating the Value Circle

Oracle Blockchain Platform

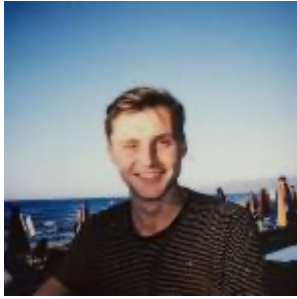
a case study

Vennster

June 25th | LuxOUG Virtual Tech Days

Agenda

- ❑ Introduction
- ❑ Oracle Blockchain Platform
- ❑ Technical setup of the platform
- ❑ Design decisions, chain code, security
- ❑ Next steps



Cas Bertrams



Lonneke Dikmans



Mathijs Kemp



Ronald van Luttikhuizen

Who are we?

INTRODUCTION

Introductie

About Vennster

- Dutch Startup, partnership between experience and innovation
- Large network
- Social Corporate Responsibility
- Co-creation

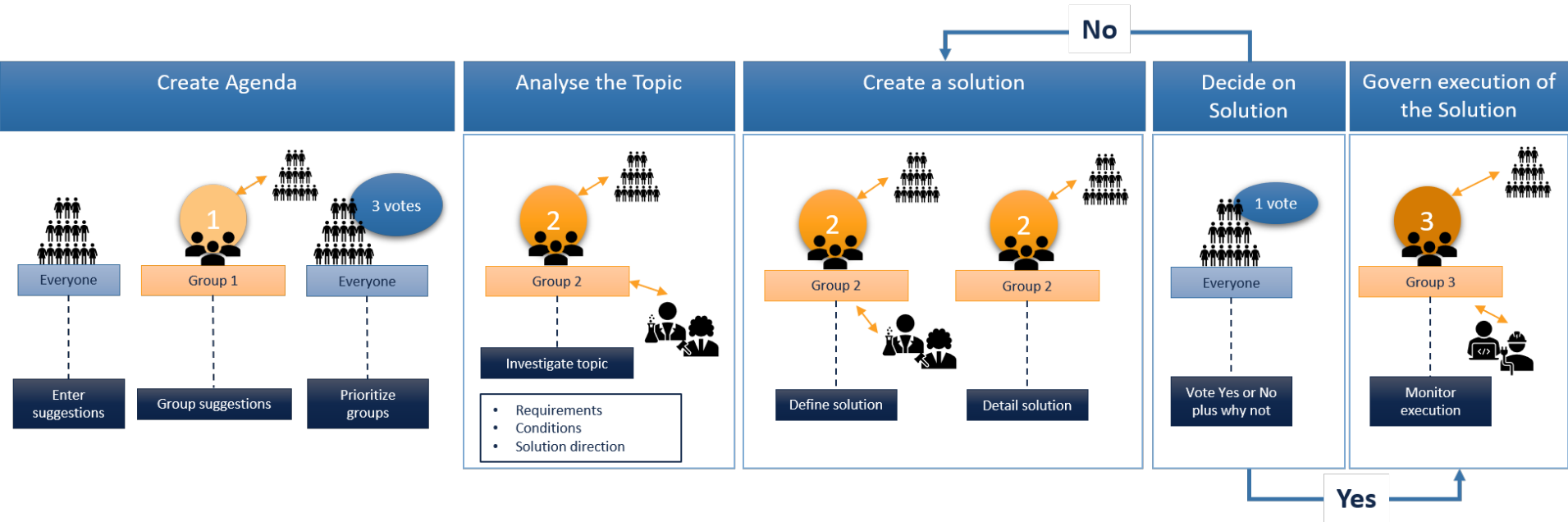
DoeMee

- Digital Decision making
- Applicable for government, parties, foundations, union, companies, etc
- Emancipation and democracy at the core
- Transparency, privacy and security

Lonneke Dikmans

- Oracle Ace Director
- Oracle Groundbreaker ambassador
- In IT since 1995
- Working with Oracle since 2000
- Founder

The Process



What is Oracle Blockchain

ORACLE BLOCKCHAIN PLATFORM

Oracle Blockchain platform | Hyperledger

Permissioned blockchain

Open source and supported by multiple cloud vendors

Multiple mainstream languages

Added features for usability

Intermezzo: what is Blockchain?

A blockchain keeps track of transactions, in a so-called ledger. Data is immutable, and each transaction has a link to the previous transaction. Before a transaction is put on the ledger, it is validated by peers, so there is no 'man in the middle' and no single point of failure.

Nodes Summary As of June 23, 2020 8:19:21 PM UTC-00:00

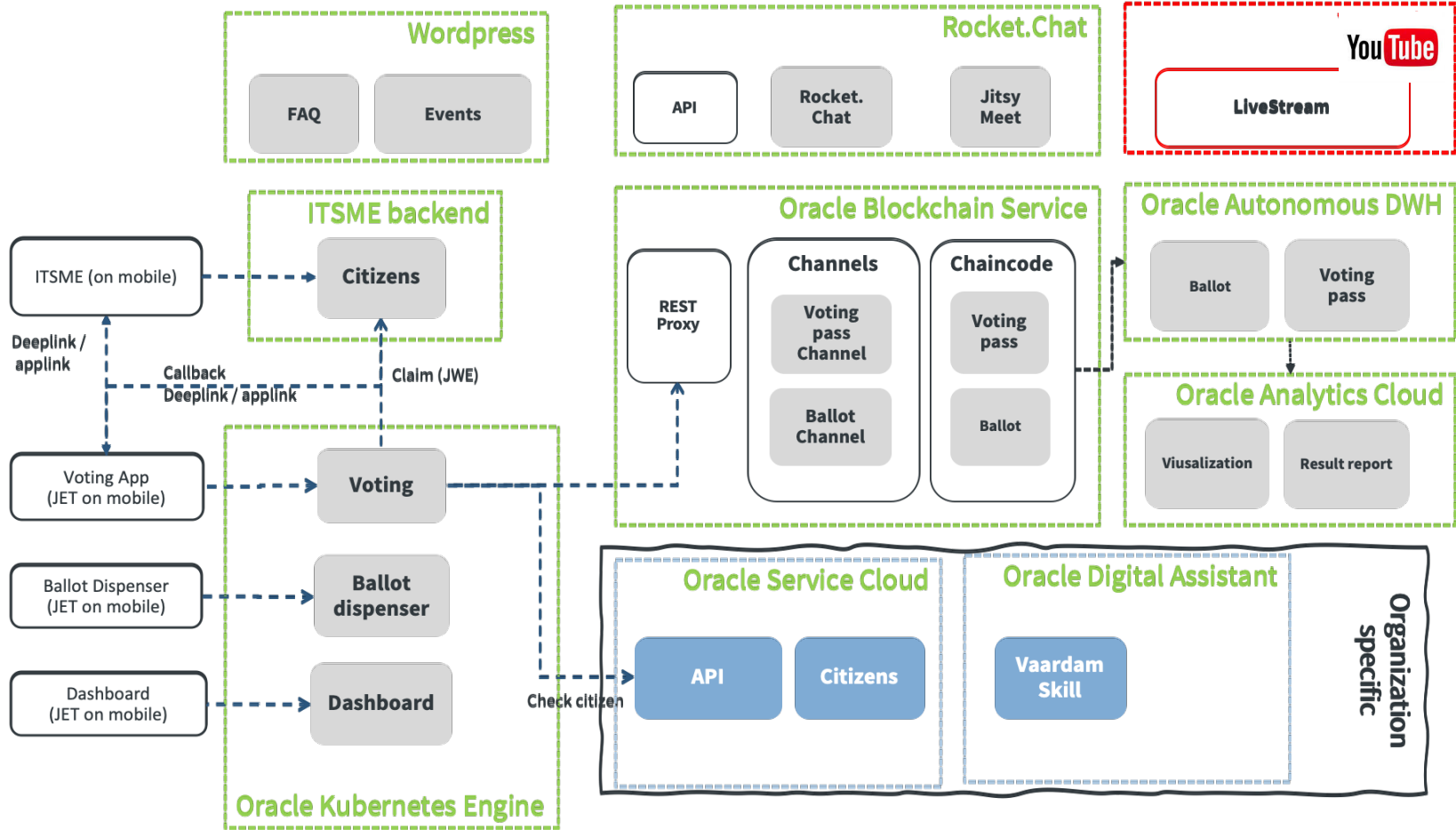
9 Nodes	2 Peers	1 Orderer	1 CA	4 REST Proxies	0 Remote Peer
-------------------	-------------------	---------------------	----------------	--------------------------	-------------------------

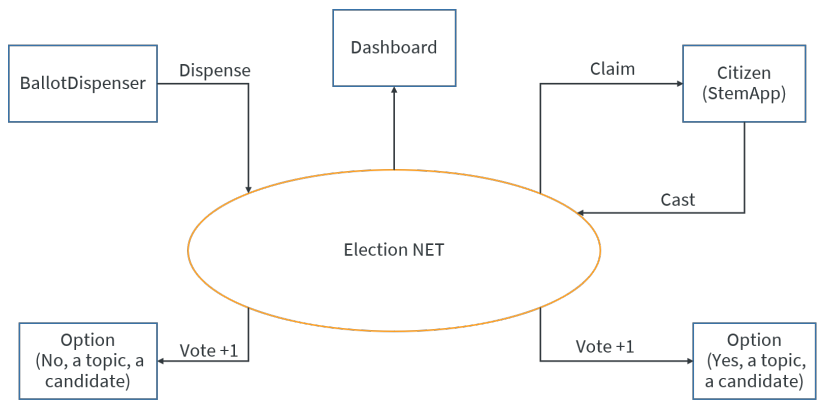
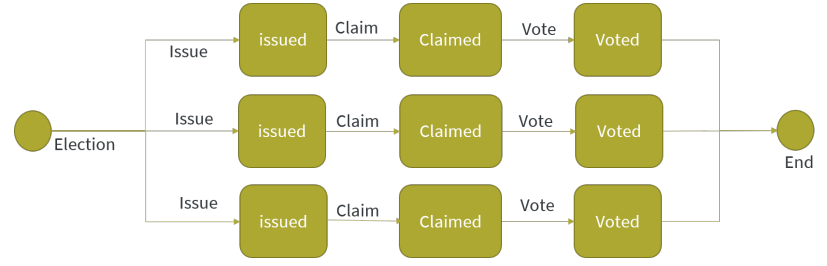
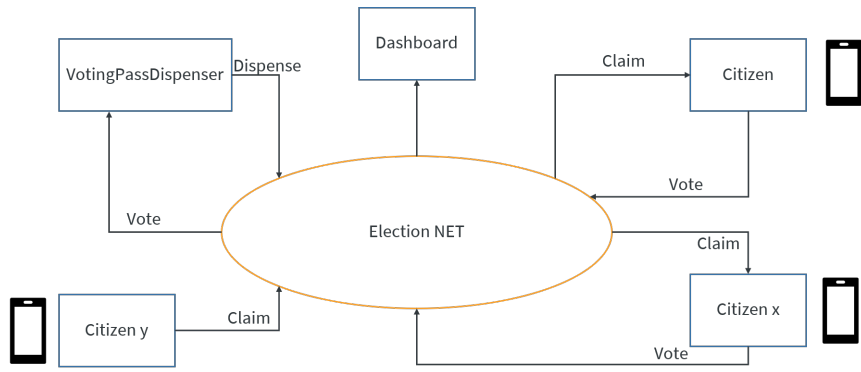
Status: Up
Type: All

Name	Route	Type	MSP ID	Status	
console	https://FE4CA7F4CA054A97BDB8D5C870FC5339.blockchain.ocp.oraclecloud.com:443	Console	pdoemee	● up	
peer0	grpcs://B64053D6EFFD42DFBC59E0D6FB29D11B-private.blockchain.ocp.oraclecloud.com:7100	Peer(Member)	pdoemee	● up	
peer1	grpcs://B64053D6EFFD42DFBC59E0D6FB29D11B-private.blockchain.ocp.oraclecloud.com:7102	Peer(Member)	pdoemee	● up	
orderer0	grpcs://B64053D6EFFD42DFBC59E0D6FB29D11B-private.blockchain.ocp.oraclecloud.com:7301	Orderer	pdoemee	● up	
ca	https://FE4CA7F4CA054A97BDB8D5C870FC5339.blockchain.ocp.oraclecloud.com:443	CA	pdoemee	● up	
restproxy1	https://FE4CA7F4CA054A97BDB8D5C870FC5339.blockchain.ocp.oraclecloud.com:443/restproxy1	REST Proxy	pdoemee	● up	
restproxy2	https://FE4CA7F4CA054A97BDB8D5C870FC5339.blockchain.ocp.oraclecloud.com:443/restproxy2	REST Proxy	pdoemee	● up	
restproxy3	https://FE4CA7F4CA054A97BDB8D5C870FC5339.blockchain.ocp.oraclecloud.com:443/restproxy3	REST Proxy	pdoemee	● up	
restproxy4	https://FE4CA7F4CA054A97BDB8D5C870FC5339.blockchain.ocp.oraclecloud.com:443/restproxy4	REST Proxy	pdoemee	● up	

The platform

TECHNICAL SETUP





Platform

DESIGN DECISIONS

Design decisions

Minimize code in chaincode

Description	The business logic in the chaincode is limited to the ledger, no process information or other information is put in there.
Rationale	Chaincodes are immutable, so you can't change the code without starting a new ledger.
Impact	Need for backends (nodejs) microservices

Design decisions

Define two independent chaincodes

Description	Each citizen receives a voting pass to make sure they can only cast their vote once (or multiple times in case of selecting options). The ballot, so the option or candidate the vote goes to is in a separate ledger and there are no links between the two.
Rationale	Voting should be anonymous, that is a ground rule in democracy. However we do need to make sure there is no fraud by people voting more often than allowed.
Impact	We can't directly link citizen data to votes. This makes it GDPR compliant We need logic that checks if a citizen has voted outside of the ledger (backend) or a one-way encryption in case we do want to check if someone voted already.

Design decisions

Hyperledger as blockchain technology

Description	For the blockchain we use Hyperledger, a permissioned blockchain.
Rationale	For elections, all voting districts in a municipality can have a node, validation can be done by the municipality, thus controlling the voting passes (who can vote) For companies, validation can be limited to the organization, preventing outside participation
Impact	Create nodes per voting district? Create nodes per organization?

Design decisions

OCI Kubernetes Engine as container platform

Description	We will deploy our microservices in Kubernetes
Rationale	<p>The code runs in node, we would like to have light weight containers that can handle peak. Load for chat and video chat varies greatly, and needs horizontal scaling (video bridges)</p> <p>There are going to be changes, preferably with 0 downtime</p> <p>Ease of use of deployment</p>
Impact	Create docker containers for our backends and front ends

Design decisions

Authentication	
Description	We will use a pluggable identification service
Rationale	We don't want to store information about voters. This means that to identify and determine eligibility for a vote, we need to rely on third party identification services. Otherwise we have to ask for personal data and store it with the account
Impact	Select an identification service, potentially per country ?

Design decisions

Security	
Description	Security in every layer
Rationale	Decisions can have a big impact and can involve budget allocation. DoeMee is a consumer application that will be available in the Google Playstore and Apple store. This means it can be targeted.
Impact	Have regular Pen tests ISO certification is needed Pick platform known for security and privacy

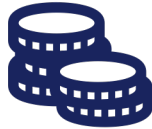
Platform

NEXT STEPS

Next steps



Security



Budgeting



Accessibility



Complete redesign
(Ionic/React)

VENNSTER



Creating the Value Circle

Oracle Blockchain Platform

a case study

Vennster

June 25th | LuxOUG Virtual Tech Days