Diploma als smart contract

Frank Brinkkemper

Afstudeeropdracht Business & IT
Universiteit Twente & Topicus.Finance

Deze presentatie

- Probleem
- Hoofdvraag
- Blockchain fresh-up
- Smart contract platformen
- Toegevoegde waarde technologie
- Case
- Demo
- Uitrol procedure
- Conclusie & limitaties

Probleemstelling

Diploma fraude

- Daardoor: tijdverspilling sollicitatieproces
- Universiteiten – visum fraude

Diploma verificatie is tijdsintensief – geen standaard

- Per universiteit ~2 per dag.

Oplossingsrichting

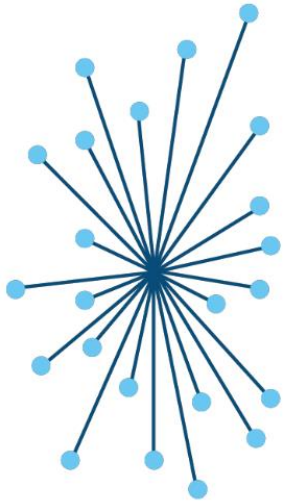
- Digitaal betrouwbaar verifieerbaar diploma
- Wereldwijde toepassing, dus:
  - Universele standaard
  - Altijd beschikbaar
- Centrale (super-user) niet gewenst, dus:
- Decentrale oplossing

“Wat is de toegevoegde waarde van blockchain technologie en smart contracts bij het creëren van een digitaal diploma?”

Methode

- Literatuuronderzoek
  - Blockchain
  - Smart contract platformen
  - Digitale diploma oplossingen
- PoC verifieerbaar diploma
- Demo ter validatie
  - Survey volgt

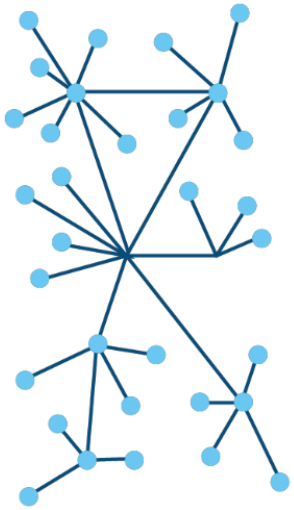
Blockchain fresh-up



Centralized

Block: batch van transacties
Chain: verwijzingen van block n -> block n-1

Append only, zonder delete



Decentralized

Bv: Bank

Bv. Bitcoin

Uitbreiding blockchain: Smart contract platformen

- Sinds 2014 Ethereum
- Bijhouden van de **staat** van zelfbedachte variabelen
- Idealiter: netwerk van alle waardevolle variabelen
- Maar, (momenteel) slecht schaalbaar.

- Overige oplossingen: NEO, EOS, Rootstock, ETC, …

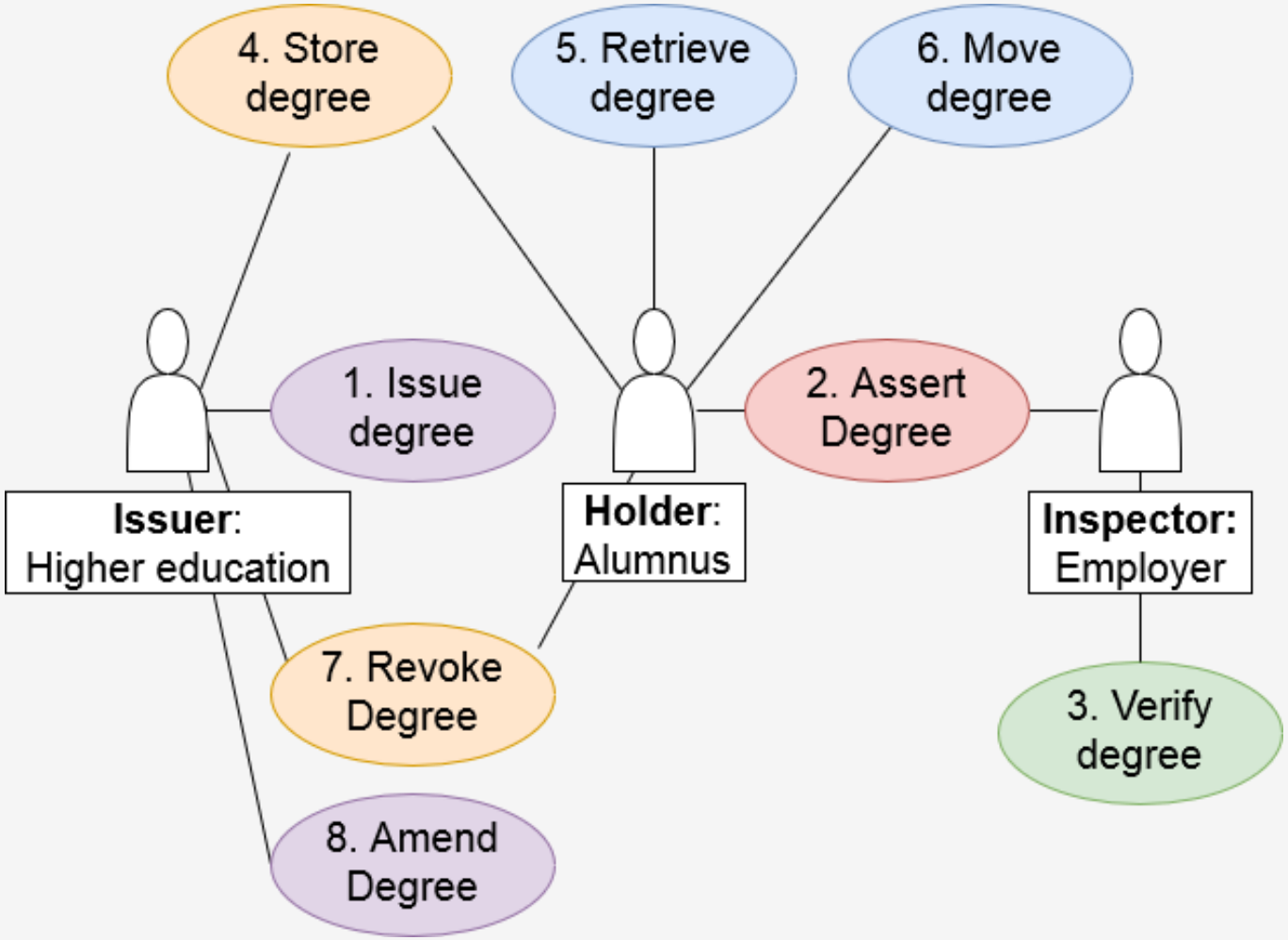
- Meeste development/developers op ETH

Toegevoegde waarde technologie

- Blockchain:
  - Decentralisatie van transactievalidatie
  - Verificatie back-end zonder eigen infrastructuur
  - Terugdateren is niet mogelijk

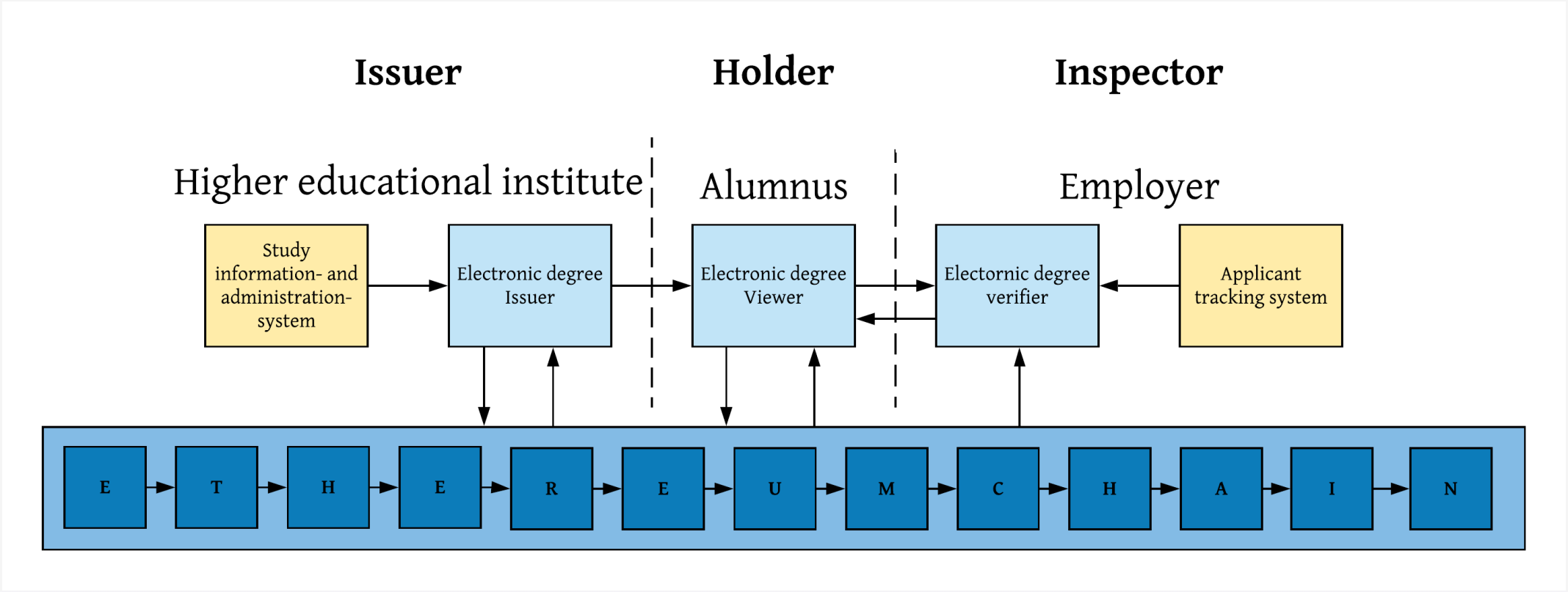
- + Smart contracts:
  - Bijhouden van staat

Case: Wat zijn de user needs?

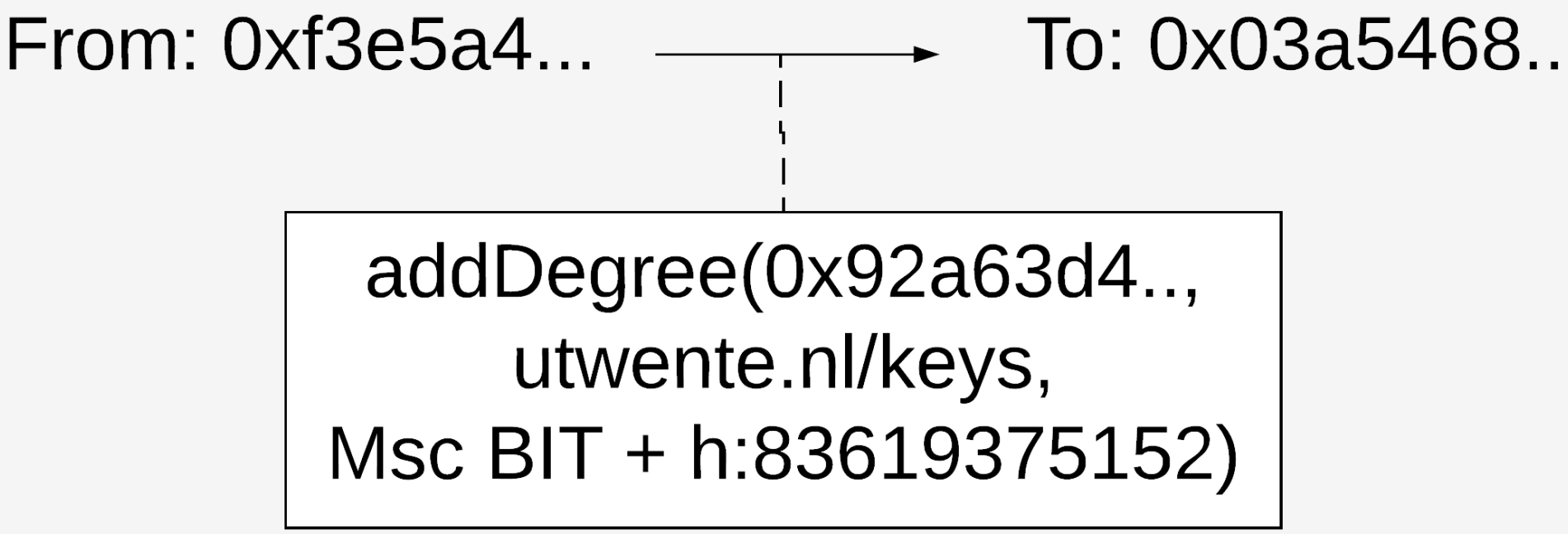


Hoe ziet het eruit? - Deployment

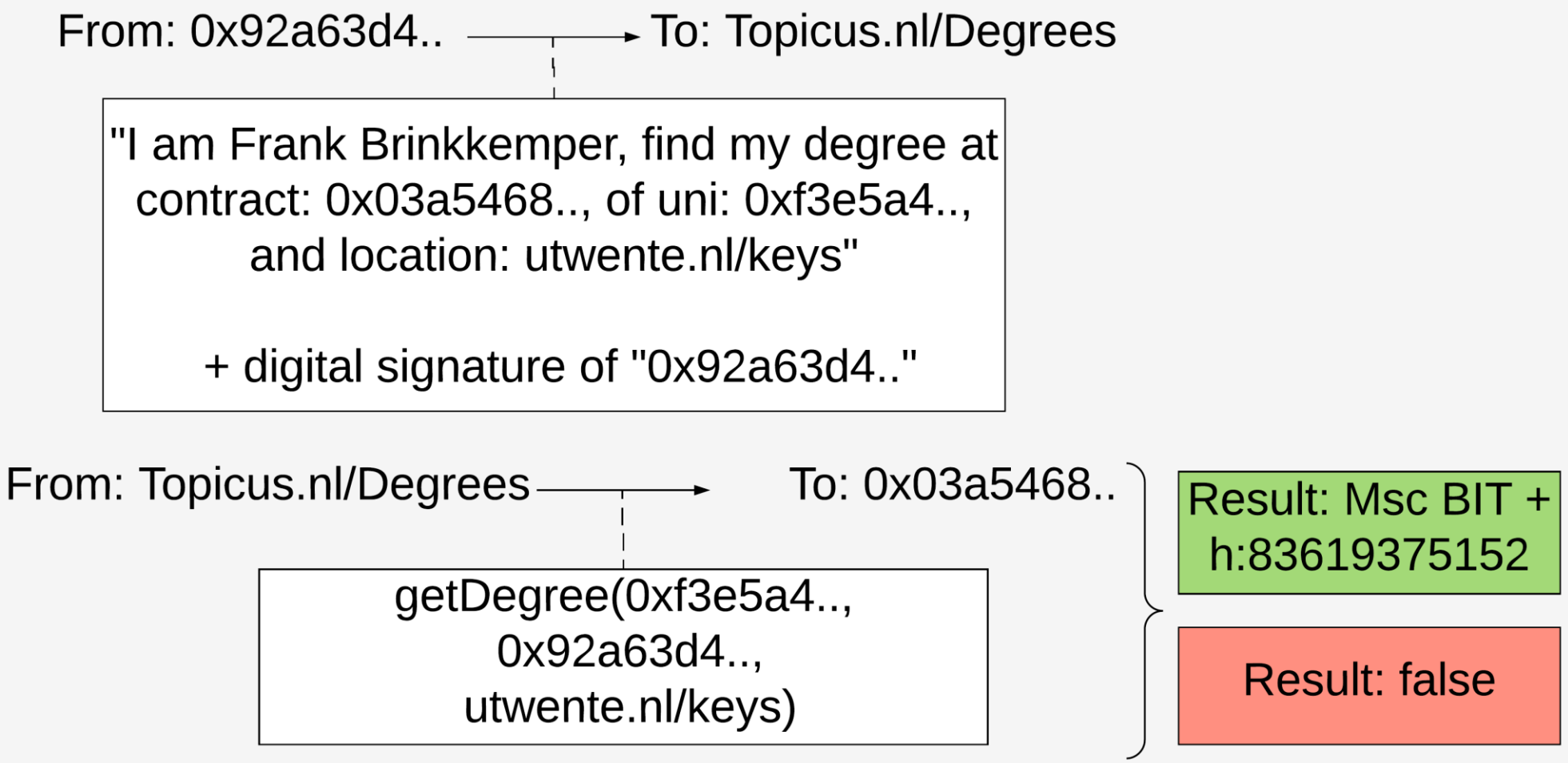
- Aangesloten bij BlockCerts + ERC780 standaarden



Hoe ziet het eruit? – Ethereum **transactie** UC1: issue degree



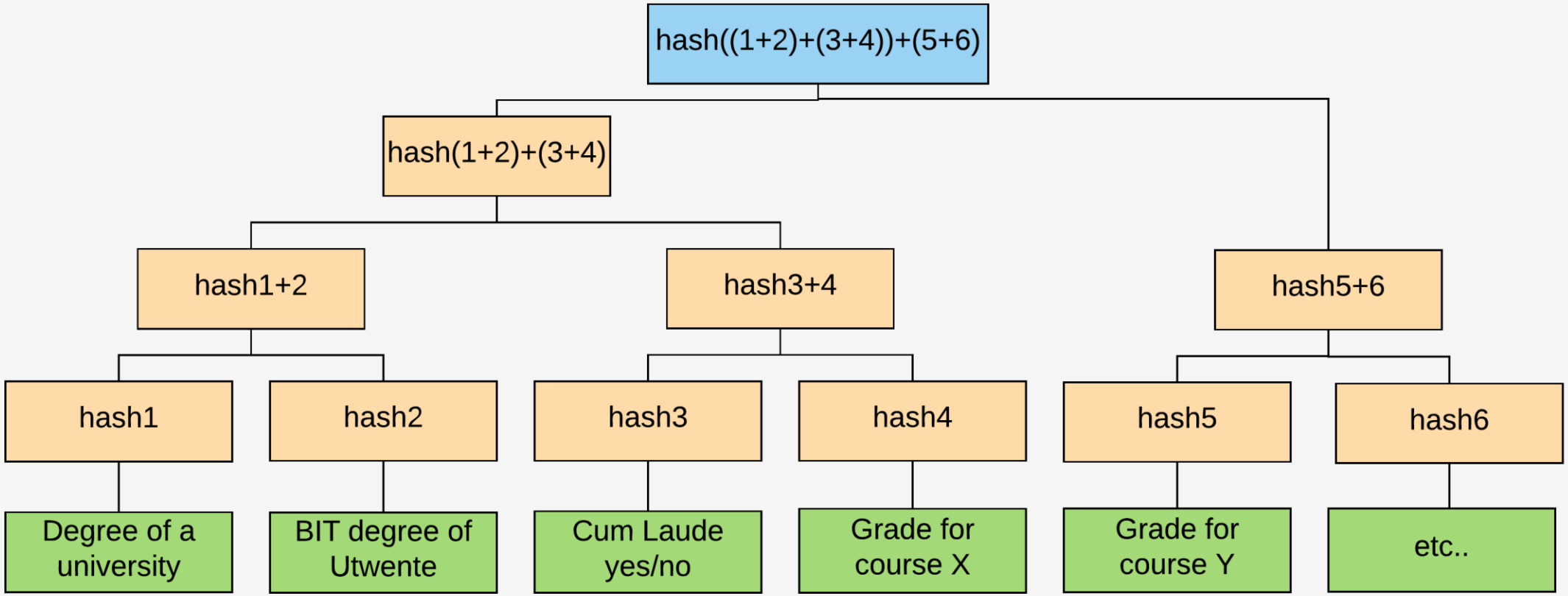
Hoe ziet het eruit? – UC2+3: Verificatie calls



Hoe ziet het eruit? - Demo

- Demo

Hash boom verificatie van context



Alumnus view

Validaties

1. Daadwerkelijk uitgegeven door de instelling
2. Geen aanpassingen gedaan in certificaat
3. De hash is gelijk aan de hash van de blockchain
4. Certificaat is niet teruggetrokken
5. Certificaat is uitgegeven op een moment dat de keys geldig zijn.

Uitrol procedure: fase 1 - **pilot**

- Selecte groep hogere onderwijsinstellingen
- LMS: Toevoegen van public key ontvanger
- Draaien op eigen Ethereum netwerk
- 3 views maken
  - Issuer
  - Alumnus
  - Employer

Fase 1:
3-6 maanden

Fase 2:
1 jaar

Fase 3:
Lange termijn

Uitrol procedure: fase 2 - **testnetwerk**

- Deelnemers opschalen
- Tests draaien op publiek Ethereum test netwerk
- User experience tests met alle partijen
- Aansluiten bij Blockchain identiteits-standaard
- Veiligheidsvoorschriften uitwerken

Fase 1: 3-6 maanden | Fase 2: 1 jaar | Fase 3: Lange termijn

Uitrol procedure: fase 3 – **live!**

- Professionele audit van smart contract code
- Uitrol naar het publieke Ethereum netwerk
- Elke hogere onderwijsinstelling wereldwijd kan gebruik maken

Fase 1:
3-6 maanden

Fase 2:
1 jaar

Fase 3:
Lange termijn

Conclusie & limitaties

- Het is zeker mogelijk.
- Breed inzetbaar
- Te integreren met badges

- Kosten momenteel variabel (0,1 – 2 euro p/s)
- Pas echt goed zodra identiteit op blockchain
  - Nu erbuiten verifiëren dat pk: 0x2347d5a.. = Universiteit Twente?

Vragen

- Komt u maar!

- Graag invullen: http://bit.do/DigitaalDiploma

- Mail: f.l.brinkkemper@student.utwente.nl

Probleem voor universiteiten

- Garantie dat op de Ethereum blockchain niet onder hun naam diploma's uitgegeven kunnen worden.

- Hiervoor oplossing:
  - Interne database is leidend
  - Transaction overruling.