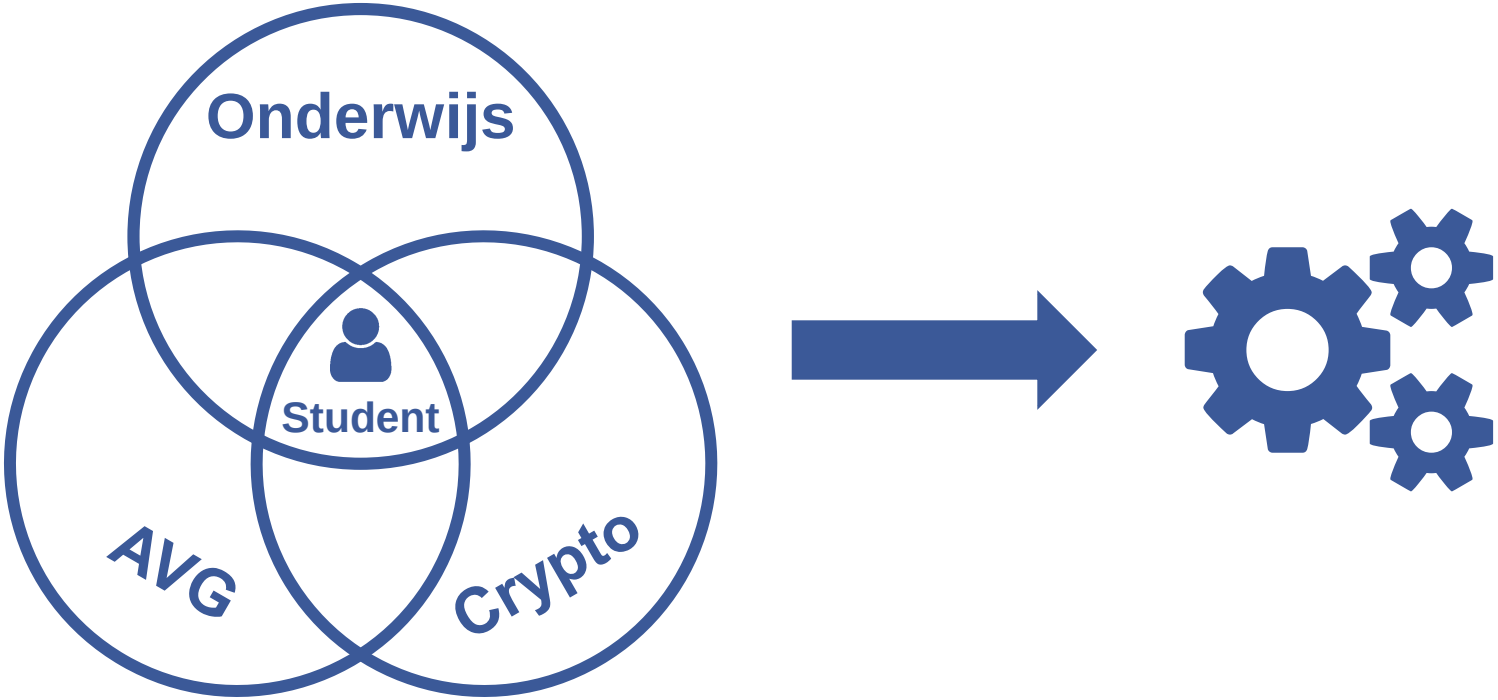
De student centraal zetten

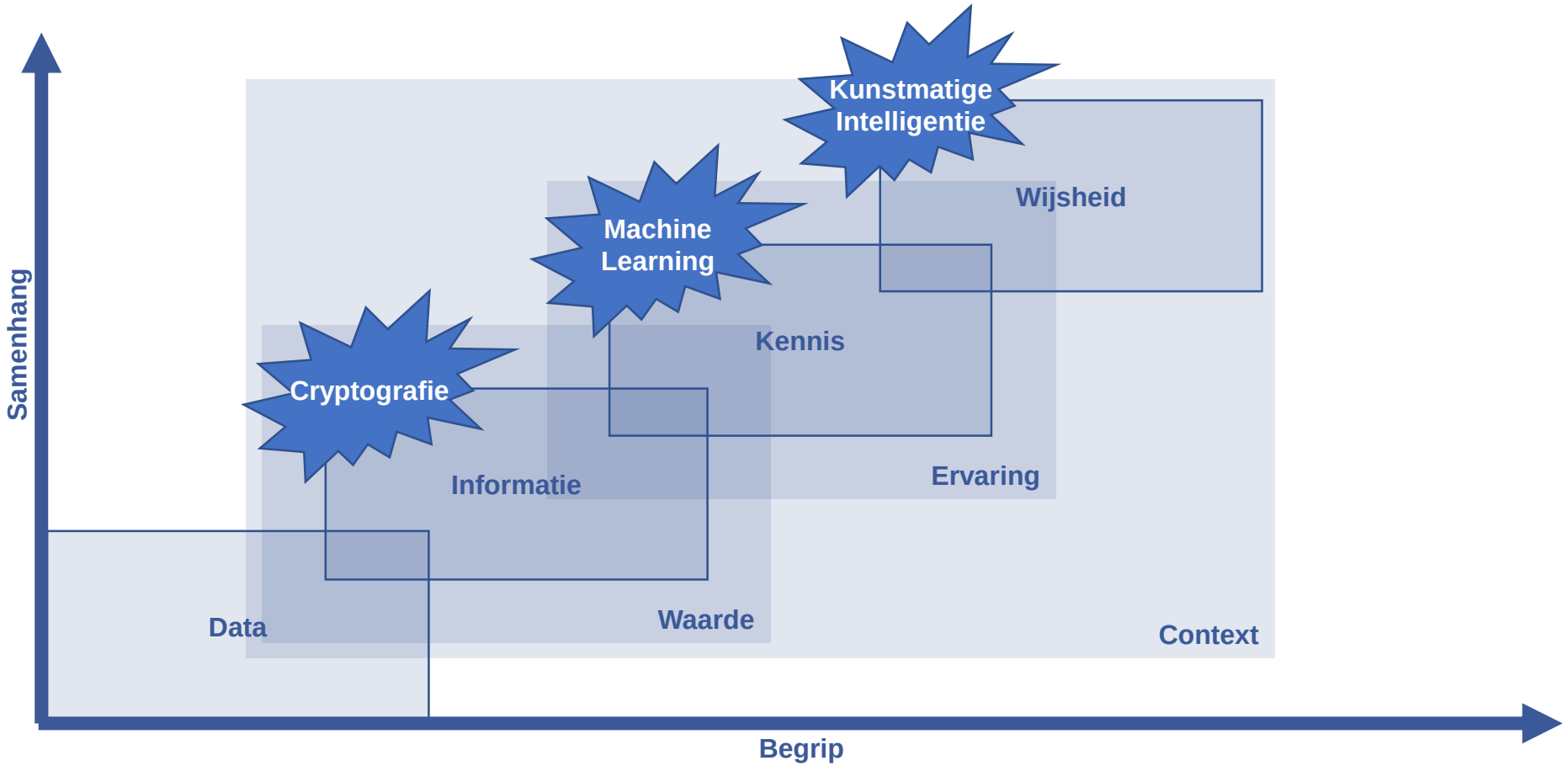
door een sterke informatiepositie


New Scientist
WEEKLY 30 June 2018
SEA CHANGE
An entire Arctic ecosystem is vanishing
ASTEROID ARRIVAL
Space mining probe homes in on target
MOVE OVER NAVY SEALS
Why dolphins are the US military's best friend
How to think about...
Life / The multiverse / Time /
Truth / Entropy / Consciousness /
Gender / Logic / Particles /
Schrödinger's cat / Genes /
The blockchain / Black holes /
the most mind-bending concepts in science
No3184 £4.50 US/CAN$6.99
PLUS CANNABIS OIL / ELECTRIC PLANES / MAGNETIC MOTHS

Waar gaan we het over hebben?



Digitalisering van Waarde



Waarde in het onderwijs

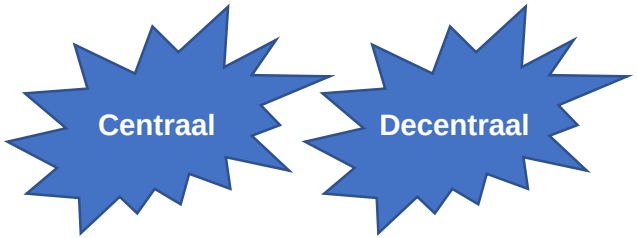
1. **Waarde heeft te maken met onze doelen ➔**
   Zelfstandige betrokken burgers die een beroep kunnen uitoefenen.
2. **Waarde concretiseren ➔ In beton beitelen van**
   Cijfers, leerprestaties, presentie, examens, vaardigheden, competenties, diploma.

Is alleen het digitaliseren van deze informatie voldoende?

Nu en straks?

Digitalisering van Waarde

1. **Digitaliseren van informatie ➔**
   Scannen of registreren van analoge informatie.
2. **Waarmerken van informatie ➔**
   Unieke vingerafdruk vastleggen = aantoonbare originaliteit.
3. **Ondertekenen van informatie ➔**
   Verbinden met de bron = aantoonbare afkomst.
4. **Tijdstempelen van informatie ➔**
   Datum en tijdstip transactie vastleggen = aantoonbare creatie.
5. **Verankeren van de waarde ➔**
   Vastleggen afkomst, waarmerk, tijdstempel ...
   Op een andere plek dan de informatie zelf!



Rol van Cryptografie

- **Klutsen ➔**
  - Iets onleesbaar maken met je privé sleutel.
  - Iets leesbaar maken met je publieke sleutel.
- **Waarmerken ➔**
  Hashen, data omzetten in unieke onleesbare code van vaste lengte.
- **Ondertekenen ➔**
  - Zender berekent waarmerk van informatie.
  - Zender klutst het waarmerk met privésleutel.
  - Zender geeft informatie + geklutst waarmerk aan ontvanger.
  - Ontvanger ontklutst het waarmerk met publieke sleutel.
  - Ontvanger berekent zelf waarmerk en vergelijkt deze.
  - Waarmerk klopt? Dan EN afzender correct EN origineel correct.

Even voorstellen …

Fred is onze bestuurder

Hoeveel handtekeningen per dag zet hij? ➔

1?

10?

100?

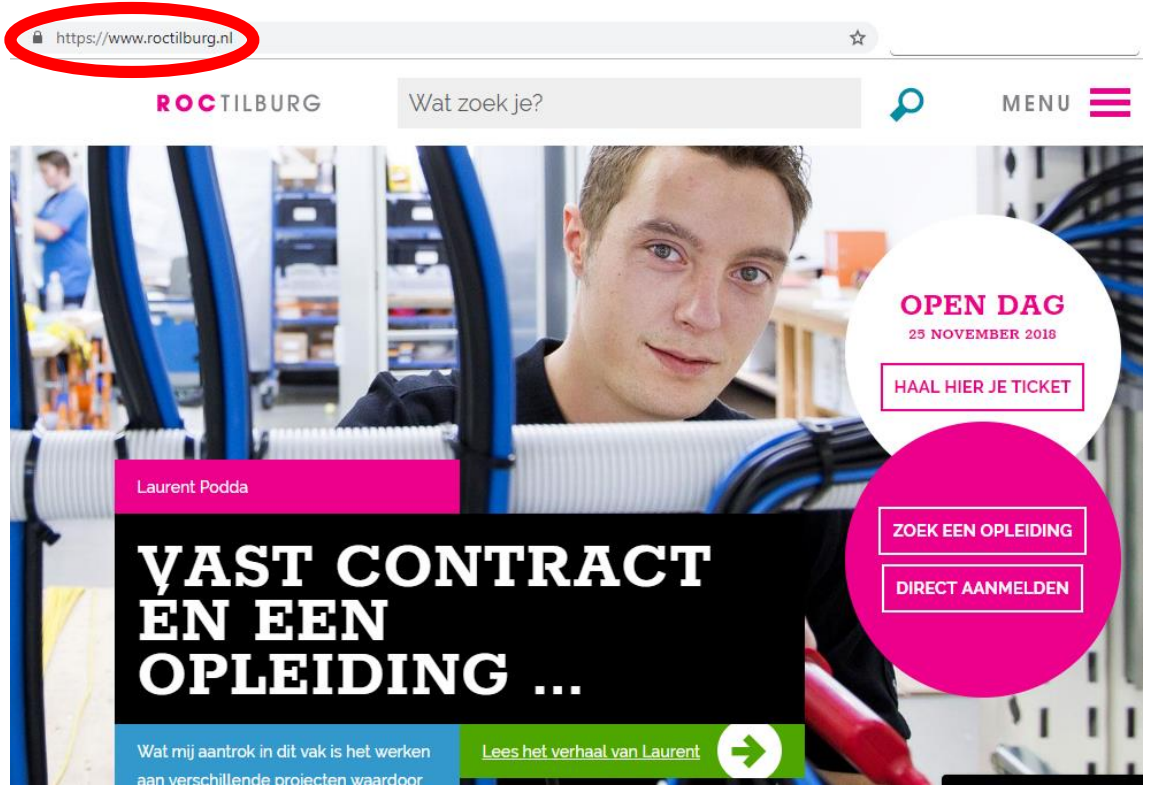
1000?

10000?

100000?

Verankeren = Keten van vertrouwen

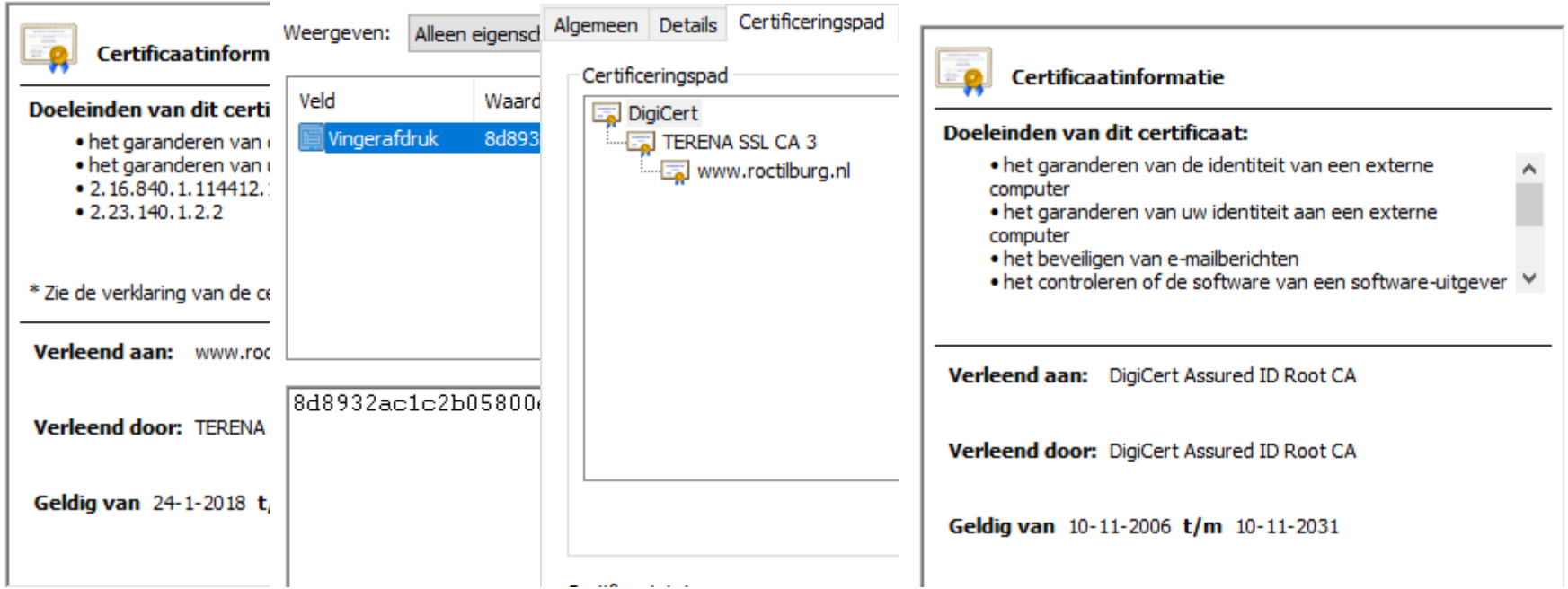
1. **Vertrouwen in het domein door certificaat ➔**
   Website is van ons!



Verankeren = Keten van vertrouwen

2. Vertrouwen in het certificaat-uitgever door controle ➔

Dit certificaat komt van een heuse certificaat-uitgever! (TTP)



Verankeren = Keten van vertrouwen

3. **Vertrouwen in controle door toezicht ➔**
   Deze certificatiedienstverlener is onder toezicht van het Agentschap Telecom.
4. **Vertrouwen in Fred door identificatie met paspoort ➔**
   Deze persoon in wiens naam de instelling het certificaat gebruikt is de enige echte!
5. **Vertrouwen in paspoort door ….**

Conclusie:
We zetten al op grote schaal digitale handtekeningen door onze Public Key Infrastructure voor sites.

Centraal versus Decentraal

- **Centraal ➔**
  Selecte partijen waarop de overheid toezicht houdt en die certificaten mogen uitdelen.
  Registers met uitgereikte en ingetrokken certificaten + looptijden.
- **Decentraal ➔**
  Iedereen kan een ‘certificaat’ of sleutelpaar aanmaken.
  Grootste implementatie: BlockChain van het Bitcoin netwerk.

Toepassen op waarde in onderwijs

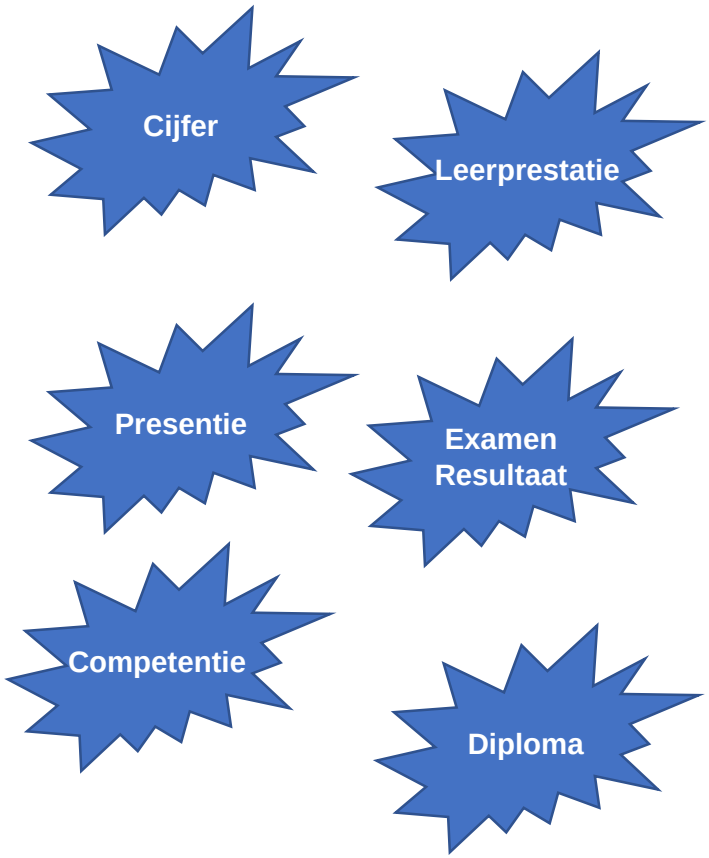
Hypothetisch voorbeeld:

1. Een beoordelaar geeft een 8 voor een gemaakt examen.
2. De student ontvangt de beoordeling.
3. De school vernietigt het gemaakte werkt.
4. De school vernietigt de cijferlijst.
5. De school wist het dossier van de student.
6. De school houdt op te bestaan
7. De student claimt een 8 te hebben.

Zou jij hem geloven?

Ja, mits ondertekend … mits het certificaat nog bekend is.

Standaard voor Claims



Verifiable Claims

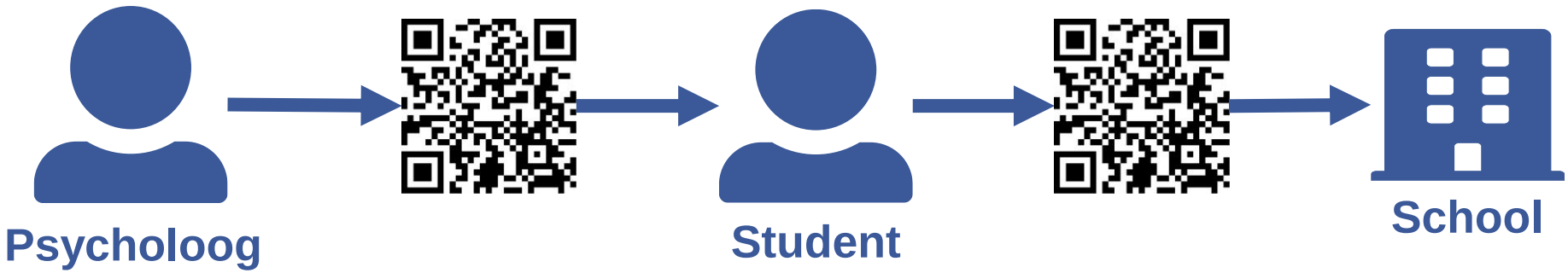
- Identiteit van Ontvanger
- Claims over Ontvanger
- Metadata over Claims
- Handtekening van Uitreiker

Portfolio …

- **Eigenaarschap ➔**
  Student
- **Inhoud ➔**
  Verzameling bewijslast om kennis, vaardigheden en competenties aan te tonen.
- **Portfolio 1.0 ➔**
  Bewijslast op papier + natte handtekening
- **Portfolio 2.0 ➔**
  Bewijslast in bestanden volgens ePortfolio standaard.
- **Portfolio 3.0 ➔**
  Bewijslast in bestanden volgens ePortfolio + digitaal ondertekend.

Kunnen bewijzen dat je bewijslast voor competenties authentiek is.

Hypothetisch voorbeeld ADHD Diagnose



Wat maakt dit mogelijk?

Bevrijding van informatie!

- **Informatie kan elders voortleven ➔**
  Gegevens zijn authentiek ook al komen ze niet meer uit een systeem van ons.
  Gegevens zijn authentiek ook al komen ze niet meer uit een systeem gekoppeld met ons.
- **Regievoering door de ontvanger zelf ➔**
  Student kan zelf regie voeren over … wie zijn gegevens mogen zien.

Zoektocht naar generieke oplossing ….
Niet alleen student, ook burger, patiënt, verzekerde etc.

Ontwikkeling in Privacy

- **Wetgeving ➔ AVG / GDPR**
  Grote impact en invloed.
- **(Social) Media, FG ➔ Bewustwording**
  Berichten over datalekken, mishandel in data (= nieuwe olie?)
- **Rechten van betrokkenen + Toestemming ➔ Student in zn kracht**
  Inzage, Rectificatie, Vergetelheid, Beperking, Overdraagbaarheid, Bezwaar.
- **Overzicht bewerkingen ➔ Transparantie**
  Dataregisters en melding datalek.
- **PIA ➔**
  Risico's van te voren inschatten en maatregelen nemen
- **Indicatie ➔ Heb je als instelling**
  Meer gegevens dan de student?
  Betere gegevens dan de student?

Is BlockChain disruptief voor studentinformatiesystemen?

Zwakte van Blockchain

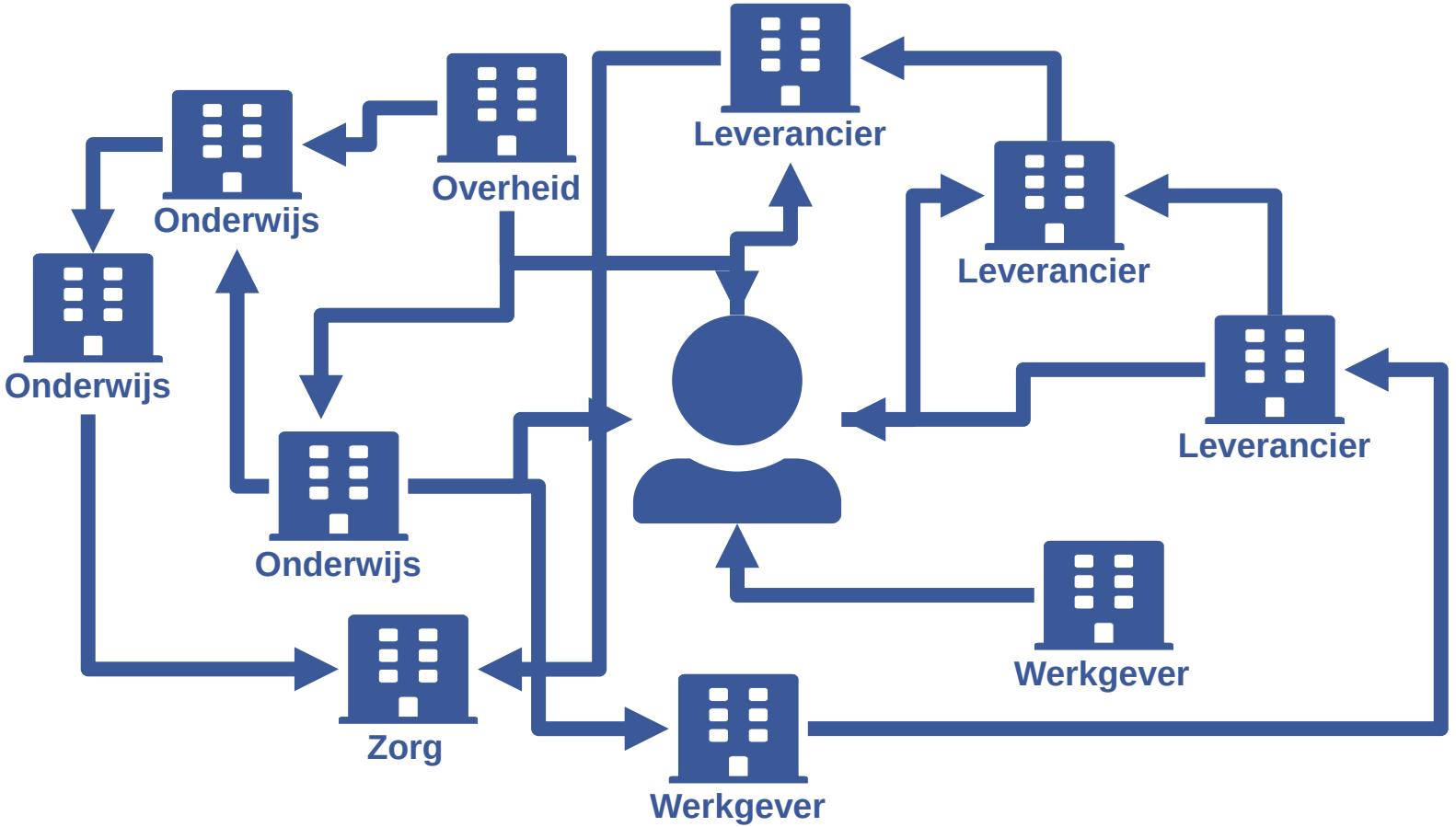
- **Niet kunnen muteren ➔**
  In strijd met de AVG en het recht van betrokkene.
- **Noodzaak bewerkersovereenkomsten ➔**
  Moeilijk te realiseren als de database bij veel knooppunten opgeslagen is. Dit geldt vooral voor een open blockchain.
- **Energiegebruik ➔**
  Hoog bij het huidige consensusmodel (BitCoin Netwerk).

Wat dan wel ipv openbare BlockChain? ➔
Verifiable Claims …

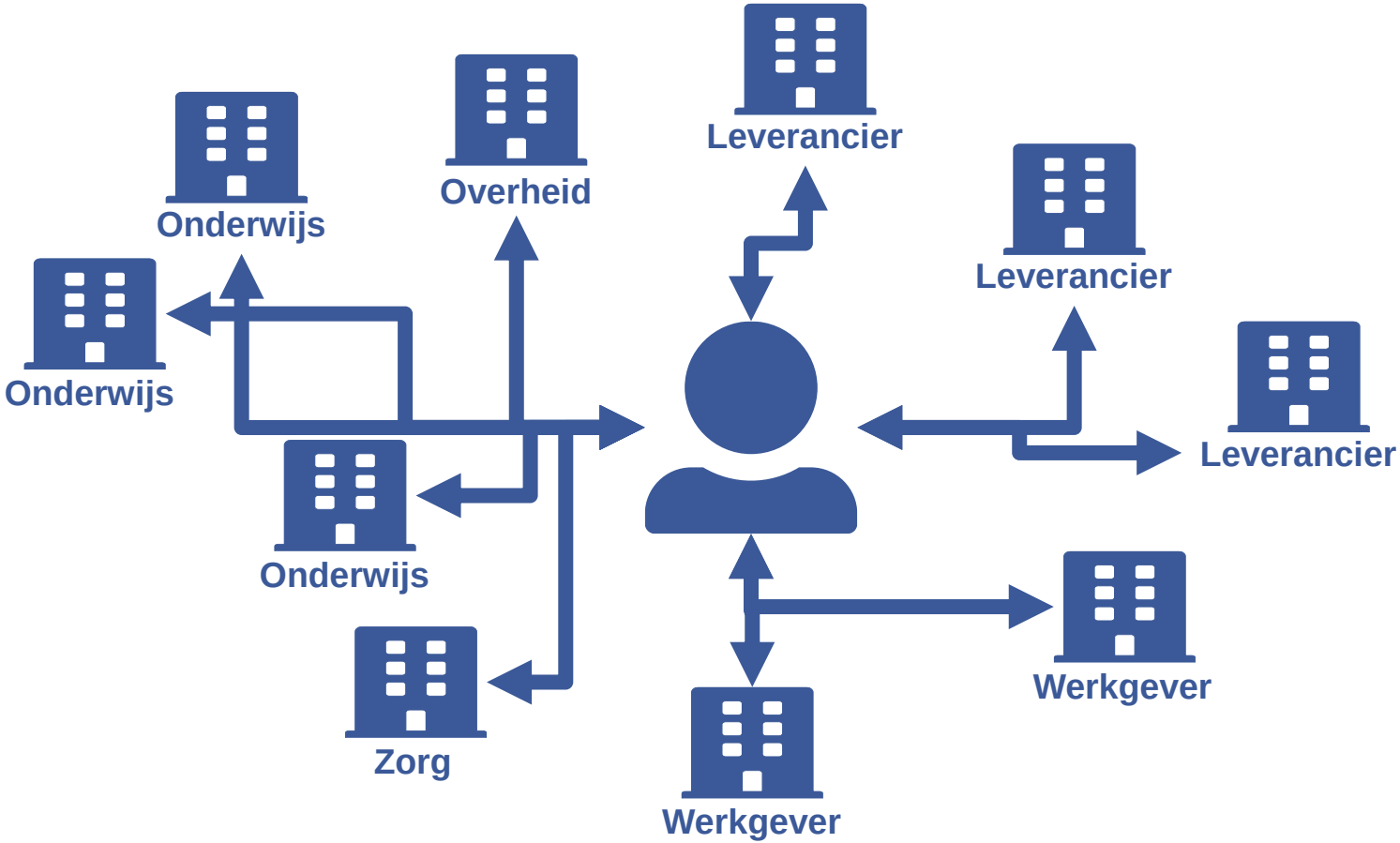
Kansen voor systemen

- **Studentadministratie ➔**
  “Status Student”, POK, OOK, Examenresultaten als ‘Verifiable Claims’?
- **ELO ➔**
  Leerprestaties, vaardigheden en competenties als ‘Verifiable Claims’?
- **AAR ➔**
  Presentie, bewijs van deelname als ‘Verifiable Claims’?
- **Portfolio ➔**
  Alles verzamelt in persoonlijke Wallet / Vault **BIJ** de student?
- **Toestemming ➔**
  Functionaliteit voor Consentmanagement.
  Auditbare registratie van toestemming, gebruik ervan en eventueel intrekken.

Zwakke informatiepositie



Sterke informatiepositie



Beleidsmatige Verankering

- **Aanwezig in Onderwijsvisie? ➔**
  Flexibilisering, co-creatie bedrijven, kleinere onderwijseenheden?
- **Opnemen in beleid voor privacy ➔**
  Doelen of principes voor zelfsoevereiniteit.
- **Opnemen in informatiestrategie ➔**
  Doelen of principes voor een sterke informatiepositie.
  Ambitieniveau automatisering/digitalisering?
- **Opnemen in technologiebeleid ➔**
  Standaarden voor koppelingen met ‘Wallets’, Micro-Credentials, OpenBadges.
- **Opnemen in beleid voor mediawijsheid ➔**
  Zelf verantwoordelijk voor je data en het bewaren en backup.
- Student Centraal = Actief betrekken bij zijn gegevens.

Concrete uitwerkingen

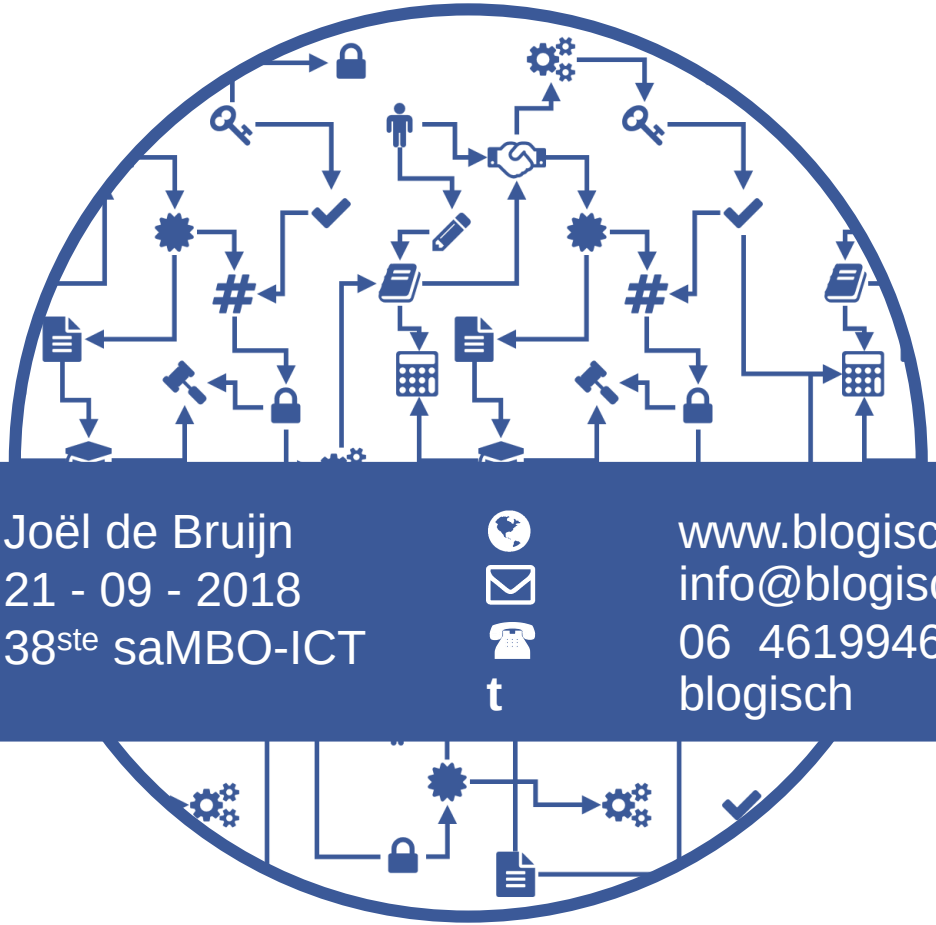
- **Disclaimer ➔**
  Geen aandelen, geen ervaring mee, jonge technologie, geen voorkeur van saMBO-ICT.
- **Identity Mixer ➔ Ontwikkelt door IBM**
  Cryptografisch algoritme om alleen datgene te tonen wat echt noodzakelijk is.
- **IRMA ➔ I Reveal My Attributes**
  App + koppelingen door NL stichting ‘Privacy by Design’.
- **Studybits ➔ Project ihkv BlockChain Fieldlab**
  Onderzoek naar o.a. Sovrin
- **Learning Machine ➔ Digitale Diploma’s**
  MIT met zogenaamde ‘BlockCerts’ standaard.

Colofon

- **Sessie ➔**
  38ste saMBO-ICT conferentie
- **Plaats ➔**
  ROC Twente, De Gieterij, Hengelo
- **Datum ➔**
  20-09-2018
- **Trefwoorden ➔**
  Cryptografie, Waarde, Vertrouwen, BlockChain, Zelfsoevereiniteit, AVG

Bronnen

- **New Scientist, Juli 2018➔**
  https://www.newscientist.com/issue/3184
- **Eigenschappen van informatie, John de Koning➔**
  https://www.slideshare.net/JohndKoning/out-smart-your-business-stappenplan-informatiestrategie
- **Certificatiedienstverleners Toezicht ➔**
  https://data.overheid.nl/data/dataset/certificatiedienstverleners
- **Verifiable Claims ➔**
  https://www.w3.org/TR/verifiable-claims-data-model/
- **Wikiwijs IBP in het MBO ➔**
  https://maken.wikiwijs.nl/104332/AANPAK_IBP_IN_HET_MBO
- **Identitymixer ➔**
  https://www.zurich.ibm.com/identity_mixer/
- **IRMA ➔**
  https://privacybydesign.foundation/



Presentator	Joël de Bruijn		www.blogisch.nl
Datum	21 - 09 - 2018		info@blogisch.nl
Event	38ste saMBO-ICT	☎	06 46199466
		t	blogisch