smart contracts

- toepasbaarheid internetregelgeving
  - vertrouwen in personen
    - leverancier
    - TTP automatische gelijkstelling elektr met schriftelijk
    - gecentraliseerd
  - vs vertrouwen in code
    - smart contract
    - geen TTP
    - gedecentraliseerd
  - hoe vertrouwen in code vergroten?
- toepasbaarheid vermogensrecht
  - juridisch
    - opschorting
    - nakoming
    - schadevergoeding
    - ontbinding
    - vernietiging
  - feitelijk
    - adres wederpartij
    - voor verhaal vatbare vermogensbestanddelen
  - hoe remedies juridisch en feitelijk uitoefenen?
- smart contract deel
  - maken
    - programmeer smart contract in Solidity
    - programmeer contract account in smart contract
    - compileer contract source in EVM bytecode
    - deploy EVM bytecode op de blockchain
  - uitvoeren
    - spel start pas als één van de deelnemers Ether overmaakt van EOA naar contract account
    - smart contract voert zichzelf gedecentraliseerd uit
    - Ether van beiden wordt aan winnaar overgemaakt zodra minimaal 51% nodes eens
    - code = law
  - **code bepaalt betaling**
  - **centraliseren van vertrouwen, en wel in code**
  - vergelijk
    - abstracte bankgarantie betaalbaar op eerste verzoek
    - wissel / cheque
- cryptocurrency deel
  - Externally Owned Account (EOA)
  - openen
    - key file
      - publieke sleutel
      - private sleutel = versleuteld
    - paswoord
      - gekozen bij aanmaken EOA
      - ontsleutelt private sleutel
    - accountnr = laatste 20 bytes publieke sleutel
  - overmaken
    - Ether wordt overgemaakt zodra minimaal 51% nodes eens
    - transactiekosten betalen aan nodes
  - beschikken over EOA
    - iets dat je hebt (key file)
    - iets dat je weet (paswoord)
    - = 2-factor
  - gedecentraliseerd grootboek dat gedecentraliseerd wordt bijgewerkt
    - transacties
    - actuele status
  - **mens bepaalt betaling**
  - vergelijk bankrekening
- voorbeeld
  - raad getal onder de 10 spel
  - klassiek
    - vertrouwen dat iedere deelnemer inlegt en internetbedrijf uitbetaalt
    - transactiekosten door speler aan internetbedrijf en internetbedrijf aan PSP
    - internetbedrijf en PSP zijn SPOF
  - Ethereum smart contract
- bronnen
  - Ri elektronische handel 2000/31
    - 6:227a vormvereiste = schriftelijke ovk
    - 6:267 elektr ontbinding elektr ovk
    - KS 28197
    - Stb 2004, 210
    - sinds 30 juni 2004
  - Ri consumentenrechten 2011/83
    - samenvoeging en vervanging minharmonisatierichtlijnen
      - colportage 85/577
      - verkoop op afstand 97/7
    - hoog niveau van consbesch
    - KS 33520
    - Stb 2014, 140
    - X Implementatiewet van toepassing op alle ovken gesloten na 13 juni 2014
  - Wet elektr rechtsverkeer
    - 7:932 elektr polis
    - 1:88-3 elektr toestemming echtgenoot
    - 156a Rv elektr onderhandse akte
    - KS 31358
    - Stb 2010, 222
    - sinds 1 juli 2010
  - eIDAS Vo 910/2014
    - 25-2 eIDAS Vo gelijkstelling gekwalificeerde elektr handtekening met schr handtekening
    - 3:15a gelijkstelling geavanceerde en gewone elektr handtekening met schr handtekening als aan bepaalde voorwaarden voldaan
    - KS 34413
    - Stb 2017, 13
    - sinds 10 maart 2017
- definitie
  - smart contracts
    - little programs that
    - execute 'if this happens then do that'
  - smart contracts on the blockchain
    - softwareprogramma's
    - die zonder tussenpersoon gedecentraliseerd op nodes draaien die met elkaar in een netwerk verbonden zijn
    - die uit zichzelf 'if this then that' commando's uitvoeren
    - die waarde verschuiven zodra de nodes met minimaal 51% consensus bereiken
    - waarvan de transacties op alle nodes worden vastgelegd, openbaar zijn en niet kunnen worden gewijzigd
- historische ontwikkeling
  - Electronic Data Interchange (EDI)
    - one-to-one
    - interchange agreements
  - e-commerce via internet
    - one-to-many
    - website terms & conditions
    - intermediation
      - AirBNB
      - Uber
  - blockchain
    - one-to-one / one-to-many
    - code = law
    - disintermediation
- internetregelgeving
  - vertrouwen in leverancier versterken
    - infoverplichtingen
      - 3:15d adres, KvK etc
      - 6:227b hoe wordt ovk gesloten
      - 6:230m kenmerken producten/ diensten, prijs, ontbindingsrecht
      - 6:230v bevestiging info op duurzame gegevensdrager
    - contracteerproces
      - 6:227c-1 herstel invoerfouten
      - 6:230v-3 knop bestelling met betalingsverplichting
    - bescherming consument
      - 6:230o 14 dagen ontbindingsrecht
    - achterstand tov brick-and-mortar wegnemen
  - gelijkstelling elektr met schr
    - 6:227a als schriftelijkheidsvereiste voor geldigheid ovk dan ook elektr
    - 25-2 eIDAS Vo TTP vereist voor automatische gelijkstelling gekwalificeerde elektr handtekening met schr handtekening
    - 156 Rv
      - ondertekend 25-2 eIDAS Vo en 3:15a
      - geschrift 156a Rv
      - bestemd om tot bewijs te dienen
  - **centraliseren van vertrouwen, en wel in personen**
    - persoon leverancier
    - persoon TTP