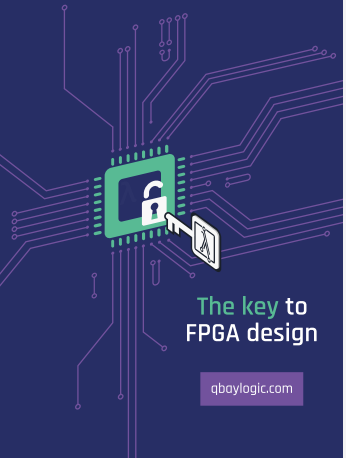
QBayLogic.
The key to FPGA-ASIC design

Creators of the
Clash compiler



The key to
FPGA design

qbaylogic.com

Clash Formal

Ökosystem Vertrauenswürdige IT

Dr. Christiaan Baaij, **Dr. Felix Klein**

20.01.2025 – Kickoff

QBayLogic.
The key to FPGA-ASIC design

QBayLogic: Wer sind wir?

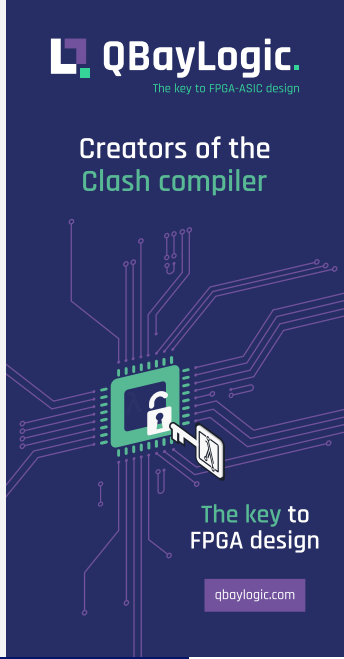
Member of CHIPTECH TWENTE

- 2016 gegründetes **Spin-off der Universität Twente**:
  Forschung seit 2009, Sitz in Enschede (Twente Region, Niederlande (Ost))
- Fokus auf innovativem FPGA Chip Design:
  Schöpfer des **Clash Compilers**
- Mitarbeiter: von 2 (2016) auf 20 (2025):
  (eingebettete) Software- und Toolentwicklung,
  FPGA- & RTL-Design, Forschung, Projektmanagement

- Partner von **ChipTech Twente**: ein Exzellenzcluster für IT-Firmen im Semiconductor Bereich, Elektrotechnik und Mechatronik, Mikroelektronik, Nanotechnologie, Photonik, Quantentechnolgie und Mikrofluidik
- Mitglied der niederländischen Semiconductor Innovation Mission 2023 (Japan) und der niederländischen Handelsmission 2023 (USA)

QBayLogic: Unsere Expertise

- **FPGA basierte Entwicklung:**
  IP Design in VHDL, (System)Verilog, **Haskell/Clash**
- **ASIC Design:** RTL Entwicklung, Simulation
- **FPGA/ASIC Validierung und Verifikation**
- **Systems-on-Chip:**
  QSys, IP-designer Vivado, IP-blocks, LiTex, RISC-V
- **Workflow Design & Setup:** CI / CD / CT
- **(Forschungsnahe) Produktrealisierung:**
  von der Idee bis zum ersten Prototypen
- **Projektierung & Projektmanagment**



QBayLogic: Kunden

Member of CHIPTECH TWENTE

Haskell: mehr als nur eine Programmiersprache

- **Funktionale Sprache**
  - basierend auf dem Lambda-Kalkül
  - unabhängig von Rechnerarchitektur-spezifischen Eigenheiten
- **Starke Typisierung**
  - Fehler werden bereits vor der Inbetriebnahme erkannt
  - Eigenschaften können über das Typ-System ausgedrückt und forciert werden
- **Einsatz in der Forschung**
  - vielseitige Tools und Anwendungen zu Haskell bzw. Haskell nutzend
  - beliebt an Universitäten (Grundlagenlehre Programmierung / Informatik)
- **Industrielle Nutzung**
  - *Meta*, *Microsoft*, *Standard Chartered*, *Tesla*, *Klarna*, *Galois*, *Serokell*, ...
  - beliebt für Anwendungen mit hohen Sicherheits- / Korrektheitsanforderungen

Haskell: ein vielseitiger Allrounder

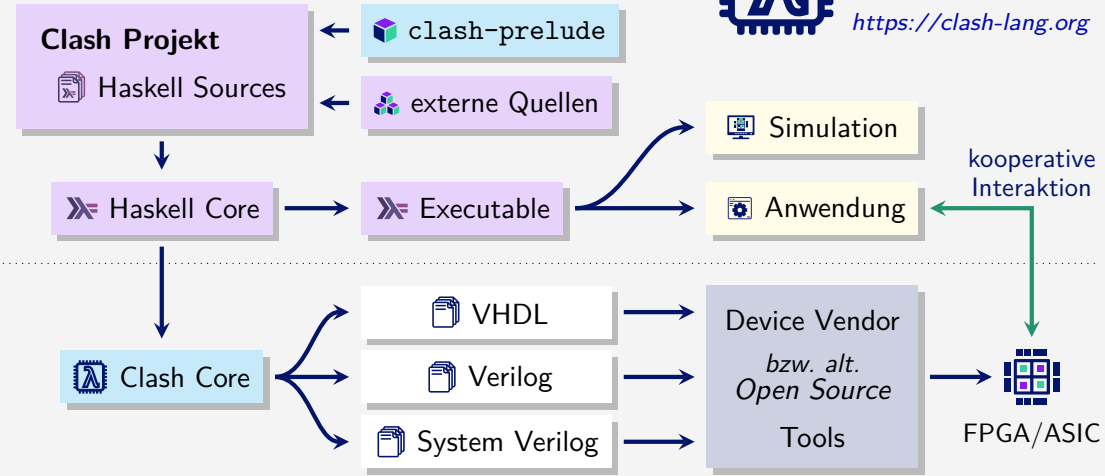
- **Webframeworks:** IHP, Obelisk, Snap, Yesod, ...
- **Build- & Paketmanagement:** Cabal, Nix, Shake, ...
- **Eingebette & Verteilte Systeme:** Ivory, Copilot, Cloud Haskell, sparkle, ...
- **Graphik & Musik & Kunst:** Gloss, Diagrams, Haskore, Tidal Cycles, ...
- **Formale Verifikation**
  - Haskell hat ein eigenes, eingebautes, typ-basiertes Constraint System
  - Korrektheitsbeweise / Assistenzsysteme: `hs-to-coq`, `agda2hs`, Haskabelle, ...
  - Refinement Types: Liquid Haskell
  - Automatisierte Beweissysteme: `sbv`, `yices-painless`, ...
- **Hardware:** Bluespec, Lava, ForSyDe, **Clash**
- ...

Clash Compiler: Haskell → Hardware

Clash

A modern, functional, open source hardware description language

https://clash-lang.org



Clash Formal

Ecosystem formally verifiable IT

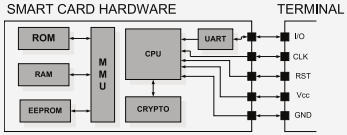
Projektziel

"Anwendbarkeit von Methoden und Werkzeugen zur ***formalen Verifikation****, wie Beweisassistenten oder automatisierten Beweissystemen, nicht nur im Bereich der funktionalen Programmierung, sondern im gleichen Sinne zur Prüfung von* ***funktionalen Hardware Designs*** *in Haskell / Clash."*

Was heißt das jetzt konkret?

- **Forschungsfragen (50%):**
  - Inwieweit können existierende Lösungen zur Haskell Softwareverifikation auch im Bereich Hardware mittels Clash genutzt werden?
  - In welchem Umfang können die formal zu prüfende Eigenschaften direkt mithilfe des Typ-Systems von Haskell beschrieben werden?
  - Können die auf diese Art und Weise spezifizieren Eigenschaften zwischen Hard- und Software geteilt und kooperativ genutzt werden?
- **Entwicklung (50%):**
  - Erweiterung des existierenden Clash Compilers / Ökosystems um anwenderfreundliche Werkzeuge zur formalen Verifikation (Open Source)
  - Smart Card Demonstrator (Open Source)

Smart Cards

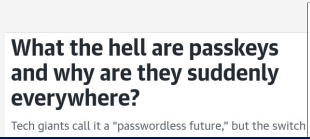


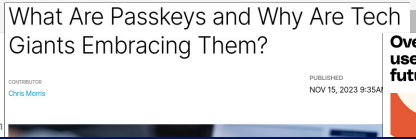
- Dediziertes Hardware-Token zur Verwaltung sicherheitskritischer Daten (Passwörter, Identitäten, ...)
- Mini-Computer im Taschenformat:
  CPU, Speicher, Crypto-Core, eigenens Betriebssystem
- Zahlreiche Anwendungsgebiete & Schnittstellen
- Offene Standards:

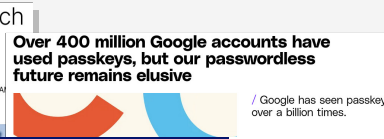
fido ALLIANCE

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

- **Passkeys** sind die Technologie von morgen!







Clash Formal

Ecosystem formally verifiable IT

Clash

A modern, functional, open source hardware description language

https://clash-lang.org