

COBRA

Bas Spitters



COBRA
CONCORDIUM BLOCKCHAIN
RESEARCH CENTER AARHUS

Subjective history

Crisis in quality in blockchains (DAO, ...)

Tezos, Cardano start academic research centers INRIA, Edinburgh
focus on functional programming/formal methods and (of course) cryptography

2018: Lars Seier (founder of Saxobank) wants blockchain for business:
Need: quality, regulation readiness
Consultancy...

Feb'19 Opening of COBRA: Buus Nielsen, Dångard, Orlandi, Spitters

Concordium

Swiss Concordium foundation funds:

- Concordium AG
- COBRA center

Concordium foundation

Basic research on blockchain technology:

- P2P
- Distributed consensus
- Formal verification
- Smart contracts
- Zero knowledge
- Cryptographic engineering



COBRA
CONCORDIUM BLOCKCHAIN
RESEARCH CENTER AARHUS

People

Currently:

7 permanent staff involved

8 pd/PhD candidates/RA

'19-'22 ~80 publications



COBRA
CONCORDIUM BLOCKCHAIN
RESEARCH CENTER AARHUS

Cobra framework agreement

Free research:

- open source
- open access

Framework somewhat like DIREC with project agreements

Benefits to Concordium/AU (Continued...)

Co-funding:

IndustryFund (Blockchain Academy Network)

DIREC (Voting and blockchains, AU/ITU/Aix)

DIGIT (center between CS/ENG/math. WP on blockchains)

...tight collaboration on cryptographic engineering

CphFinTech



COBRA
CONCORDIUM BLOCKCHAIN
RESEARCH CENTER AARHUS

Benefits to Concordium, continued...

Recruitment:

- all researchers come from AU/ETH
- top developers come from AU

Basic research which can be quickly translated to production

Requires: researchers at the company!

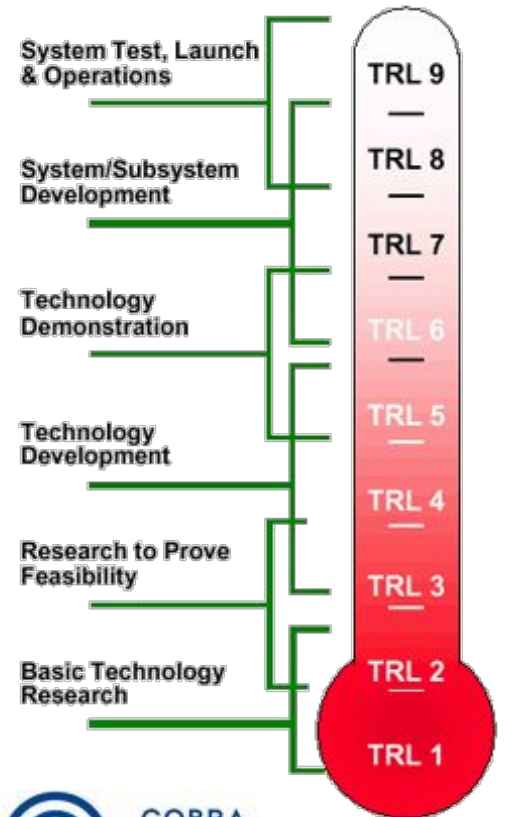
Knowledge pool at COBRA:

World leading in cryptography and PL&Verification

Advertising value: TPBC workshop, monthly newsletter, ...

Only pay a fraction:

other grants, student projects, other staff members, ...



COBRA
CONCORDIUM BLOCKCHAIN
RESEARCH CENTER AARHUS

Future

- PL design for smart contracts
- High assurance cryptographic software
- Provable security of protocols
- Consensus
- P2P
- Zero-Knowledge
- Voting
- Green transition
- Rust programming language: FM and cryptography
- ...

