



**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

Digital Trust Centre Research Grant Call

Professor LAM Kwok Yan
Executive Director, National Centre
for Research in Digital Trust

17 July 2023



PROGRAMME



3:00 pm

Welcome

3:05 pm

Overview on the DTC Research Grant Call

Professor Lam Kwok Yan, DTC Executive Director

3:25 pm

Q&A

4:00 pm

Light refreshments

4:30 pm

End of Programme



Overview of Digital Trust Centre (DTC)



INTRODUCTION

Digital Trust Centre is a national centre for research in trust technology, spearheading efforts to advance scientific research capabilities at the forefront of trust technology and to grow Singapore's trust technology industry and build a strong core of talent. Our work is funded by a \$50 million grant from IMDA and NRF for 5 years from 1 October 2022 to 30 September 2027.

1. Build up knowledge ecosystem

Identify needs and set strategic direction for research

- Harmonise capabilities across local research ecosystem and facilitate local and international research collaboration

Scale up local research capabilities

- Develop a strong local talent and indigenous capabilities in trust tech

2. Deliver industry impact

Strengthen translation of expertise to industry and accelerate innovation

- Develop sandbox for companies to experiment and prove value/ viability of trust tech
- Demonstrate real-world trust tech use cases through industry collaboration
- Provide research engineering support to co-develop solutions with early adopter companies

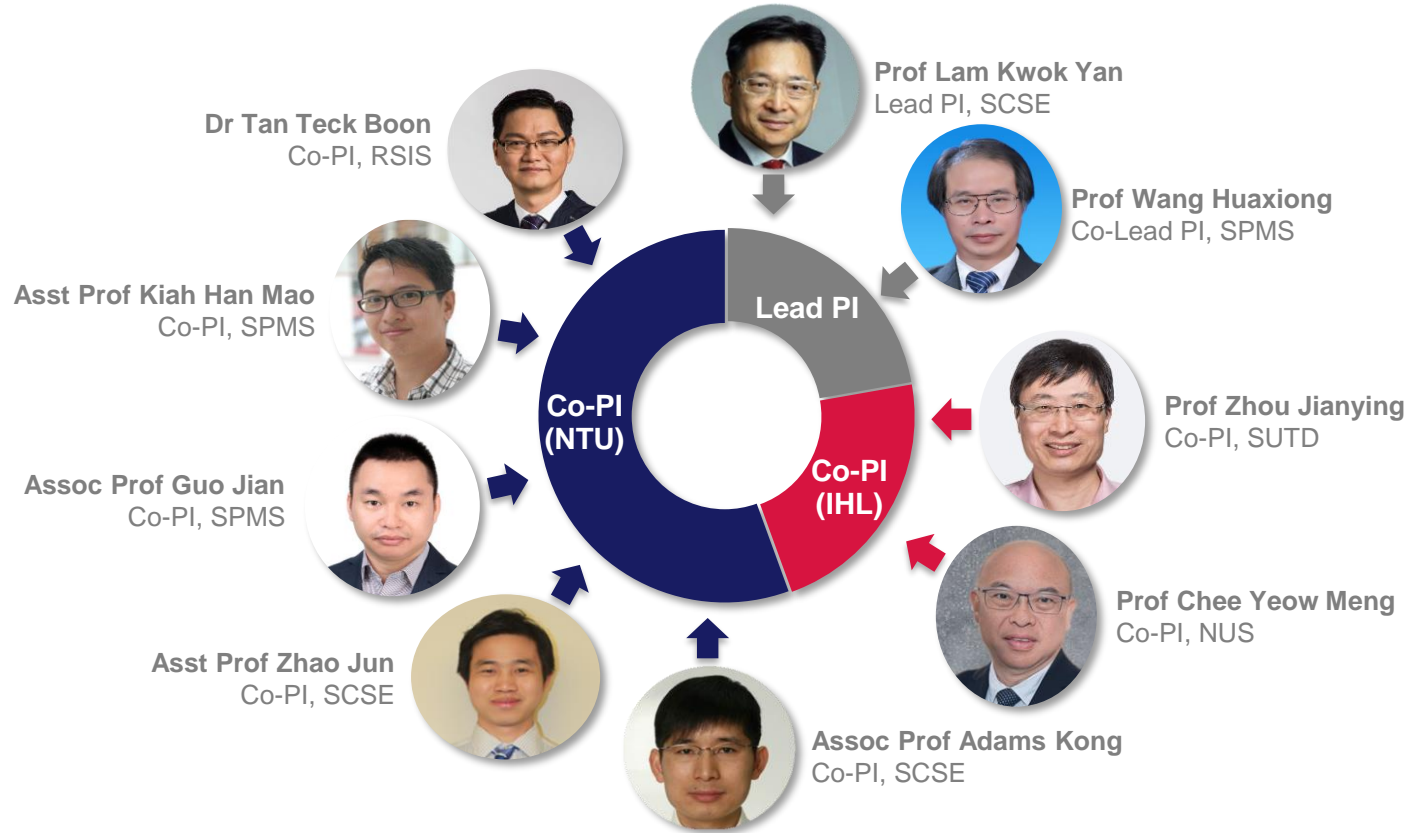
3. Position SG amongst global leaders

Reinforce SG's position as a Trusted Digital Hub

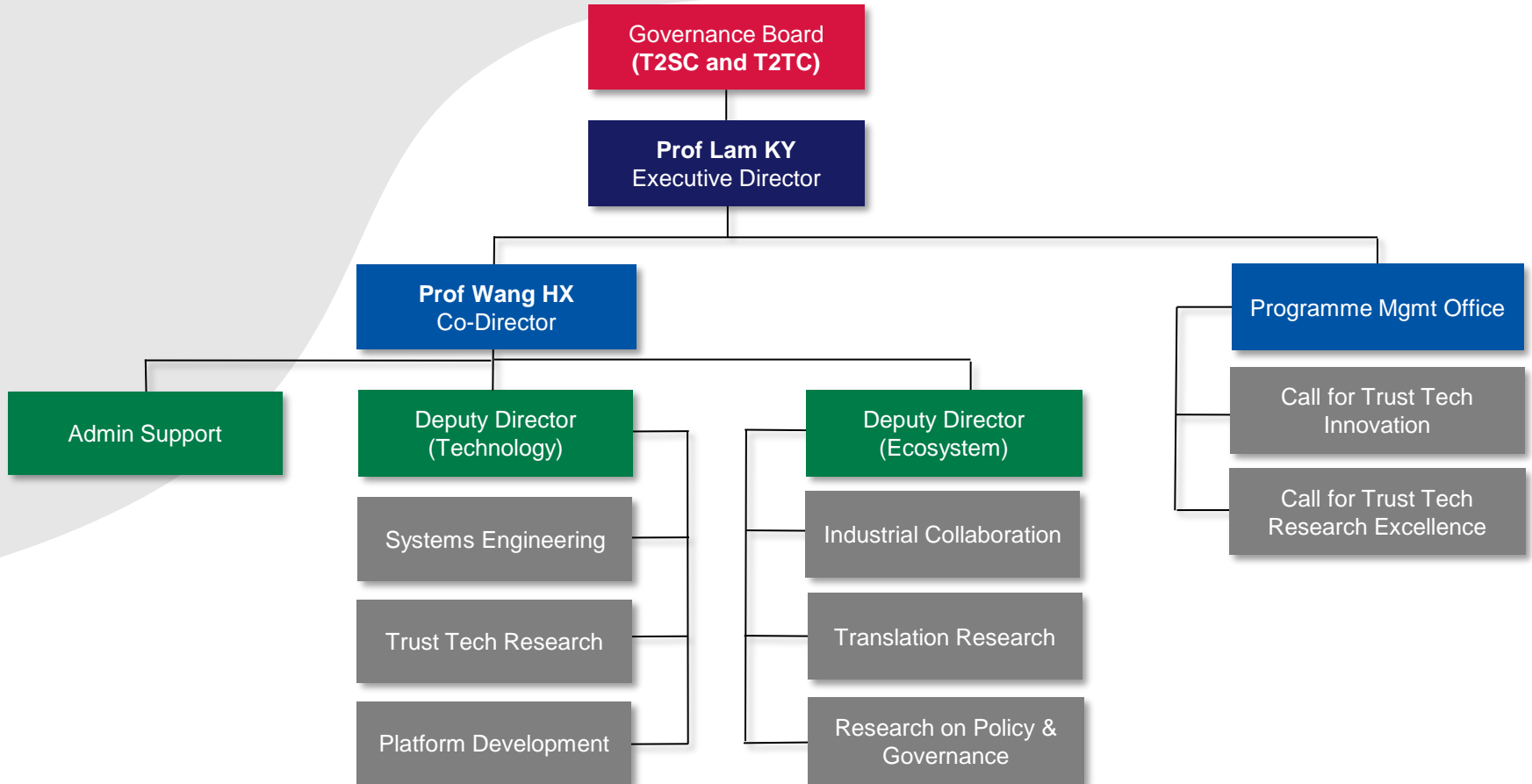
- Enhance testing tools and frameworks for AI governance to provide baseline level of trustworthiness that can be recognised internationally
- Build mindshare and shape global standards in digital trust through international partnerships and exchanges



PROJECT TEAM



ORGANISATIONAL STRUCTURE



CORE RESEARCH FOCUS

Areas of opportunity in trust tech

Trust Analysis

Derivation of insights while protecting and preserving privacy of data



Trusted Identity

Emerging trust areas in verifiability and authentication



Trusted Compute

In distributed architectures and heterogenous platforms



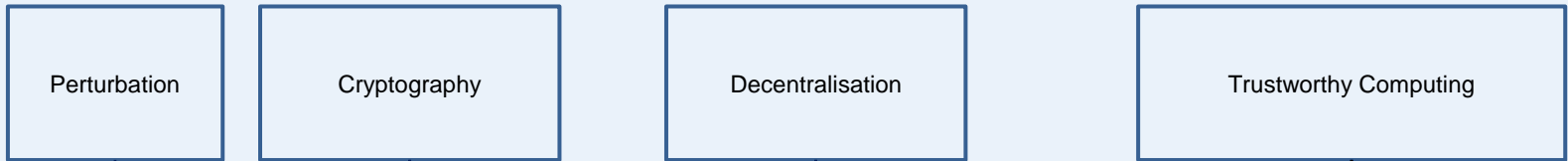
Trusted Accreditation

Technologies for testing & audit to accredit trustworthy products & services

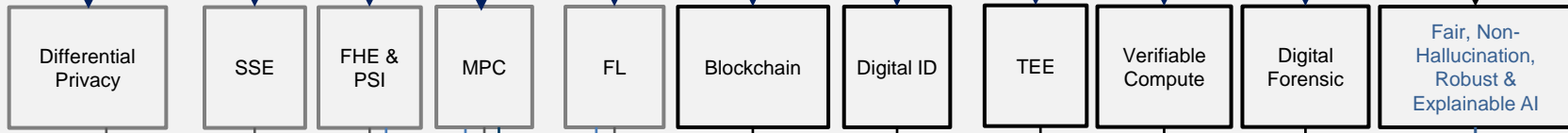


TRUST TECHNOLOGY STRATEGIC PLAN

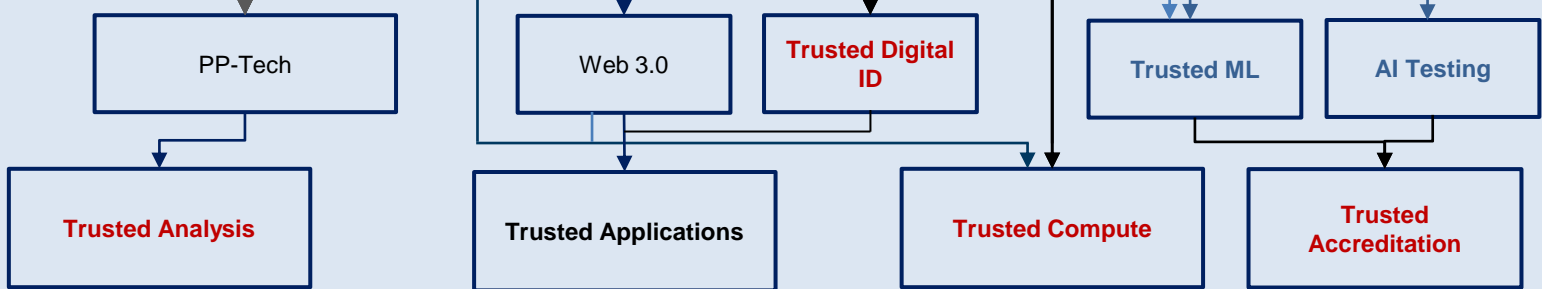
PARADIGM



FOUNDATIONAL RESEARCH



TRUST TECHNOLOGIES



Red Text: DTC main scope of TrustTech

Blue Text: emerging areas highly relevant to TrustTech but not covered by FRC Report

Trust Applications: objectives of Translational Research in different industry verticals

AI Testing: scientific methods for testing fairness, non-hallucination, robustness, explainability, etc. of AI models

SSE: Searchable Encryption; **FHE:** Fully Homomorphic Encryption; **PSI:** Private Set Intersection

MPC: Multi-party Computation; **FL:** Federated Learning; **TEE:** Trusted Execution Environment



Grant Call Overview



DTC RESEARCH GRANT CALL

- ✓ DTC research excellence grant call and innovation grant call seek to support the development of trust technologies and innovation that solve real world problems to create a digital world that is *safe, transparent and accountable*, while generating national benefits for Singapore.
- ✓ The DTC Call for Trust Tech Research Excellence (“DTC Research Grant Call”) is a **competitive research funding initiative designed to support research projects that advances the science of trust technologies** across Singapore-based Institutes of Higher Learning (IHLs) and Research Institutes (RIs).
- ✓ We encourage teams comprised of academics, researchers, scientists, engineers, domain experts, and other professionals to apply for the DTC Research Grant Call.



SCOPE 1: TRUSTED ANALYSIS



The focus will be on the sharing of sensitive data in artificial intelligence and machine learning. The emphasis will be on the trust tech enhanced computation without disclosing the actual raw data and/or the analytic model:

- a) **Searchable Symmetric Encryption (SSE):**
 - i. Leak user access / search patterns to servers, and
 - ii. Insufficient complex query expressiveness for search on encrypted data.
- b) **Full Homomorphic Encryption (FHE):**
 - i. Performance issues due to algorithm complexity and large ciphertext sizes which lead
 - ii. to high computational intensiveness and communication overhead and latency.
- c) **Private Set Intersection (PSI):**
 - i. Performance and scalability issues when the number of parties involved increases, and
 - ii. limited expressive queries and functionalities (e.g. lack of support for range, threshold, and conjunctive queries).
- d) **Multi-Party Computation (MPC):**
 - i. Practicability and scalability issues as protocols are communication and computationally intensive, particularly when dealing with a large number of parties or complex computations
- e) **Differential Privacy (DP):**
 - i. How to strike a balance between privacy and utility when applying DP.
- f) **Federated Learning (FL):**
 - i. How to develop mechanisms for collaborative model selection, model aggregation, and model update strategies in FL minimising impact on training accuracy.
- g) **Data Synthesis (DS):**
 - i. How to handle complex data types, capture spatio-temporal dependencies, and incorporate privacy-preserving mechanism in data synthesis process.

SCOPE 2: TRUSTED DIGITAL ID AND WEB 3.0



The focus will be on verifiable credentials/documents and transferable records in decentralised environments, track and trace in supply chain, digital identity, and analytics on decentralised finance:

- a) **Trusted Digital Identity Network** with emphasis on credentials and verification for digital ID, digital wallet and credential management, and digital ID network reference architecture.
- b) **Tokenisation** and token standards for digital assets to support security and auditing.
- c) **Biometric-assisted authentication** in Web 3.0.
- d) **Trust in Web 3.0 applications** through blockchain traceability and analytics, risk assessments and verification of smart contracts against legal contracts and the use of self-sovereign identity (SSI).



SCOPE 3: TRUSTED COMPUTE

The focus will be on how trusted execution environment (TEE) will impact to the design and analysis of trusted applications. Such impacts include the specialised knowledge and understanding of the security features and programming models offered by the given specific TEE platform. Furthermore, data provenance and evidence will be important to enhance the trust in the computation.

- a) Design and analysis of system environment for trusted compute based on applications of **TEE**.
- b) **Verifiable Computing (VC)** for the correctness in distributed, decentralised infrastructure for specific computation tasks, e.g. e-voting tally.
- c) **Digital Evidence:** An important part of digital trust is the ability to establish accountability and liability in case of fraud, transaction failure or abnormal behaviour. To achieve this, digital evidence borrows digital forensic concepts and techniques that are relevant in a holistic approach to digital trust.

SCOPE 4: TRUSTED ACCREDITATION



The focus will be on trusted AI model testing – (i) Research into scientific techniques for testing covering Fairness, Explainability, Robustness, Hallucination, (ii) For various AI / Machine Learning (ML) models, including supervised vs. unsupervised learning, and non-generative vs. generative AI, with respect to some of the following challenges

- a) **Hallucination** – Tackle factually inaccurate or fake outputs in Generative AI.
- b) **Fairness** – No unintended bias: AI system makes same decision even if an attribute changes, and data used to train model is representative.
- c) **Explainability** – Explain behaviour of AI models and/or multi-modal models to understand how the inner mechanics impact the generated output. Examples of problem include lack of transparency, non-deterministic outputs, high dimensionality, and overfitting.
- d) **Robustness** – Address issues relevant to robustness e.g., include non-adversarial robustness and privacy related attacks.

EVALUATION CRITERIA

Proposals should clearly state the following:

Alignment of proposal to DTC's objectives and direction.

Novelty of the research and the needle-moving research challenge that the proposal will solve.

Potential industry application or impact.

Benefit of the research to digital trust.


Relevance of the research to Singapore.



INTERIM REVIEW

MONTH 0
Research Start

MONTH 15
Interim Review

- 
- The performance and potential of the team's research project will be evaluated during an interim review.
 - Conducted by the Evaluation Committee, the interim review will be conducted 15 months into the project.
 - Teams will be required to give a presentation for the review.
 - Projects will be assessed on the progress of promised deliverables (KPIs) and quality of research outcomes.
- Continued funding support is unlocked for teams that passed the Interim Review.

NOTES

- DTC reserves the rights to terminate, after Interim Review or at any point in time, projects that do not meet the minimum expectations of progress and achievement, upon recommendation by the Evaluation Committee.
- The Evaluation Committee may also make recommendations to maximise the outcomes of funded projects (including adjustments to proposed durations and qualifying only certain components of a project to proceed to completion).



PROJECT DELIVERABLES AND OUTCOMES

Each project is expected to produce most, if not all, the following deliverables:



Publications in top 10% journals.



Industry R&D jobs.



PhDs & Masters trained.



Technologies deployed, including licences.

ELIGIBILITY

- The grant call is open to researchers from all Singapore-based IHLs and RI.
- PI and Co-PIs must hold full-time appointments in one of the above.
- Researchers from Medical Institutions, start-ups in Singapore, private sector and other entities are eligible to apply as Collaborators.
- Overseas collaborators and/or visiting experts may be invited to Singapore to assist with specific project tasks.
- Only research conducted in Singapore may be funded.
- Parallel submissions are not allowed.



PROJECT SUPPORT

DTC is equipped with common research-engineering capabilities to facilitate or support the Trust Tech community:

- Sandbox environment
- Industry contacts and matchmaking
- System engineering
- Fast prototyping
- Advice on opportunities for translational efforts

For more information, please contact DTC@ntu.edu.sg



Q&A



SUBMITTED QUESTIONS

1. Can a company be collaborator of the grant call?
 - Yes
2. Would the upcoming grant call include trust AI research (as part of trust computing)?
 - Yes
3. Are different RIs or IHLs encouraged to work together to jointly submit a proposal?
 - Yes, but not mandatory.
4. Can a person only be involved in one project?
 - For research staff, a person can be involved in more than one project and staff costs should be charged based on time commitment to the research. In terms of NRF guidelines, there are no restrictions on PI/Co-PI being involved in more than one project. Please refer to the below relevant clause.

8. All EOM related expenses shall be pro-rated taking reference from the project start date, except for lump-sum insurance claims, which shall be allowable as claimed. As a general principle, staff costs should be charged based on time commitment to the Research.



SUBMITTED QUESTIONS

5. Can you provide more clarity on what are the expectations with regard to industry collaborators? Is it mandatory?
 - Industry collaborators may provide one or more of these: use case scenarios, test data, in-kind contributions, etc. It is not mandatory but is an advantage.
6. What are the requirements for the letter of commitment from the company? Do you require the company to state how many people are participating the research and their time contribution to the project?
 - The company may specify their role/contribution to the project if awarded.
7. From the Research Project Performance Assessment section, it is noted that the project will be reviewed. If the team passes the interim review, then funding support will continue. May we know if there's a certain breakdown of how much will be funded for the first 15 months, and how much after the team passes the interim review? Or is the team supposed to budget for the entire 3 years, after which the project may be terminated and funding will be stopped if the team does not pass the interim review?
 - The budget needs to be reasonably distributed over the entire project period (e.g. entire 3 years).
8. Is having an industry partner a must for submission?
 - No.



SUBMITTED QUESTIONS

9. The faculty is interested in the topic - Trusted Accreditation, where there were 4 challenges listed (Hallucination, Fairness, Explainability and Robustness). Must the proposal cover all 4 challenges? Or can the team focus on just 1?
- No need to cover all. Can focus on just 1.
10. For the KPI section, it was indicated under the category of Research Excellence that only journal papers will be counted as a KPI for this category. May we know if conference papers will fall under this category as well?
- No, the grantee has to put up a Change Request to seek approval to amend the KPI definition to include top 10% conference and provide justification why each of the new conference is a respectable/worthy venue.
11. What is the maximum funding amount for each proposal?
- Up to \$2 million over three years, including 30% indirect cost.
12. Noted that the project commencement is from Dec 2023 onwards, can the project start date be at a later date (e.g. Apr 2024)?
- We don't expect PI to delay the commencement, but this can be considered on a case by case basis if there is strong justification.



SUBMITTED QUESTIONS

13. Under “Project Support and Facilitation” on common research-engineering capabilities that DTC may be able to support with, does it include access to cloud-based GPUs such as those hosted on Amazon, Azure etc.?
 - No. Proposal should include the cost of cloud services under OOE category of the budget.
14. Under “Project Deliverables and Outcomes”, technologies under TRL4-5 categories may not translate to industry jobs. May we understand how this will be reviewed in the proposal?
 - PI may propose whether to include industry jobs in the KPI.
15. Does the grant support research scholars? If does, does the portion for research scholars incur 30% IRC? Are research students who are holding a scholarship allowed to do paid internship or student helper work?
 - This grant call does not support research scholarship. For research students who are holding a scholarship, paid internship or student helper work are not claimable under the grant since they are existing scholarship holders.



SUBMITTED QUESTIONS

16. Must the industry partner be in Singapore or can it be counted if the industry partner is outside of Singapore?

- The industry partner can be overseas partner but the research and development activities must be conducted in Singapore. Please refer to the below relevant clause.

2.4 Other than expressly allowed under this Contract, the Funds or any part thereof shall not be channelled to Collaborators or to fund research and development activities overseas.



Thank you

