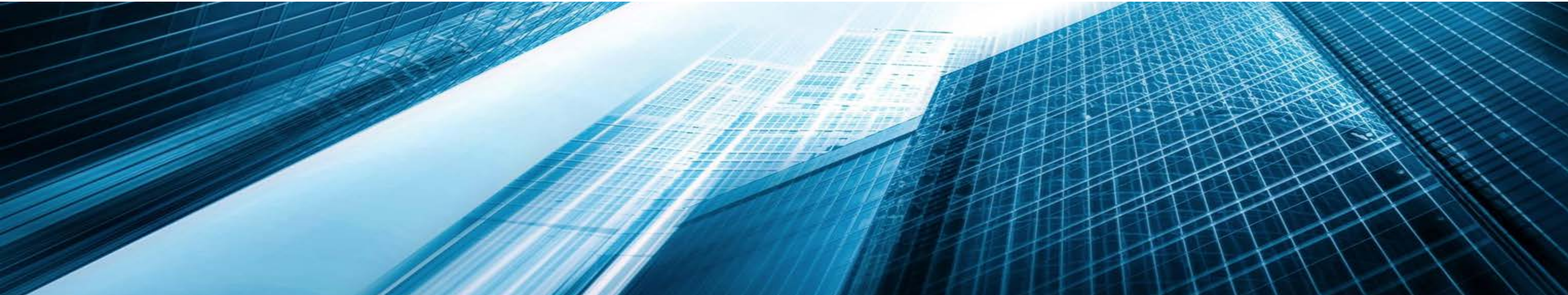
RISE FINANCIAL

TESTING OF DISTRIBUTED LEDGER SYSTEMS



INTRODUCTION

- CTO of RISE Financial Technologies

- London-based technology provider
- Bringing DLT infrastructure to the post-trade industry

- First product focused on issuance, settlement, and record keeping
- Past and current projects with SWIFT, CSDs, banks etc

RISE

FINANCIAL

SWIFT

Blockchain Startup 2016
Lifecycle of a bond on
the blockchain

IF YOU DON'T GET IT RIGHT...

- 2010 Bitcoin: Two critical validation bugs
  - Spend money from any account
  - Create unlimited money

IF YOU DON’T GET IT RIGHT...

- 2010 Bitcoin: Two critical validation bugs
  - Spend money from any account
  - Create unlimited money

- 2015 ShadowCash: Critical confidentiality bug
  - Revealed all originators of transactions
  - Lifted anonymity – of an anonymity-focused currency...

IF YOU DON’T GET IT RIGHT...

- 2010 Bitcoin: Two critical validation bugs
  - Spend money from any account
  - Create unlimited money

- 2015 ShadowCash: Critical confidentiality bug
  - Revealed all originators of transactions
  - Lifted anonymity – of an anonymity-focused currency...

- 2016 Ethereum DAO: Critical smart-contract bug
  - Lost $53M
  - Mistake made not by user but by creator of system

OVERVIEW

- Focus on:
  - Software testing
  - Challenges rather than established testing strategies

- Two main areas:
  - DLT system itself
  - Validation rules and smart contracts

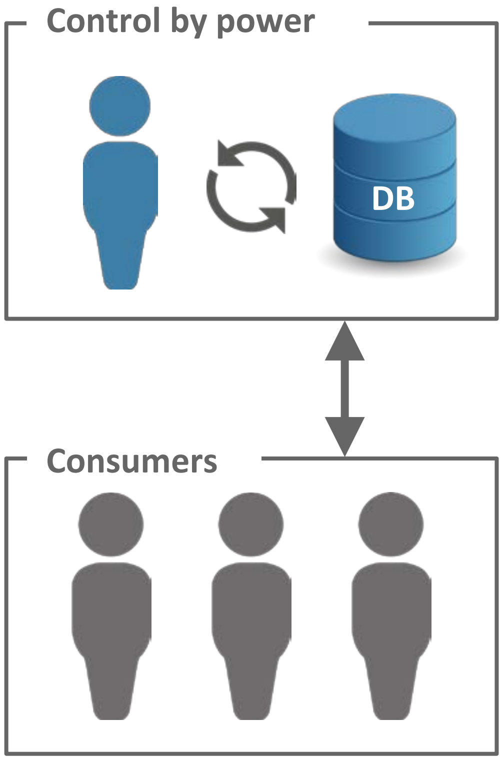
DLT? BLOCKCHAINS?

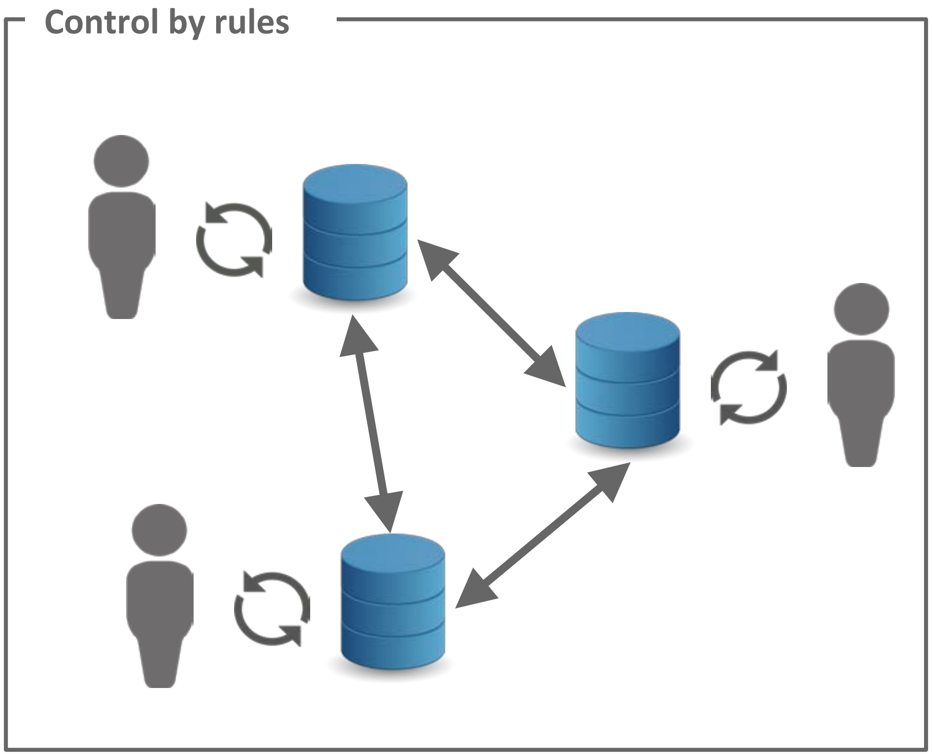
RISE
FINANCIAL

“Distributed ledgers are systems that enable parties who don’t fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts”

- Blockchain is essentially a distributed database with **shared control**
- What’s new is that this can now be done with **limited trust**
- Participants agree on validity of changes to the system according to a set of rules (*consensus*)

SHARED CONTROL





DLT SYSTEM

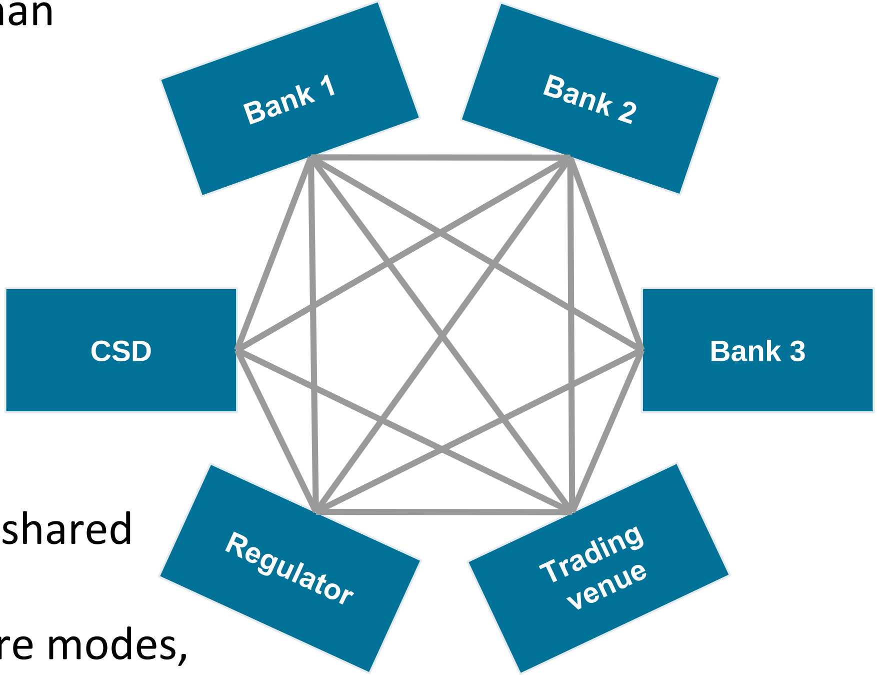
IT'S A DISTRIBUTED SYSTEM!

Distributed systems are a **great deal harder** than conventional tx processing systems.

Testing of distributed systems is **notoriously difficult**.

Analogous to a massively inter-connected banking system:

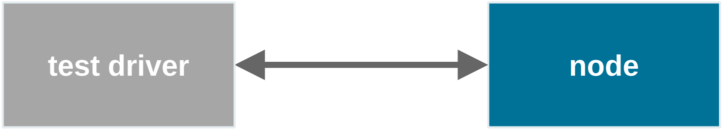
- Delays, frequent lags, connection losses, shared but diverging data
- Concurrent execution, independent failure modes, no global time



DS TEST STRATEGIES

- Isolate
- Make it deterministic
- Inject faults

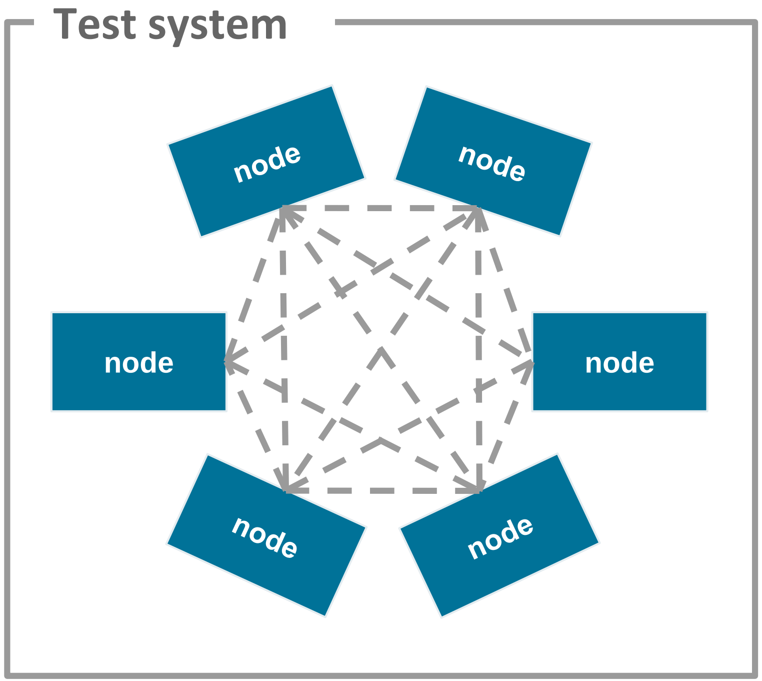
1) Test each component in isolation



DS TEST STRATEGIES

- Isolate
- Make it deterministic
- Inject faults

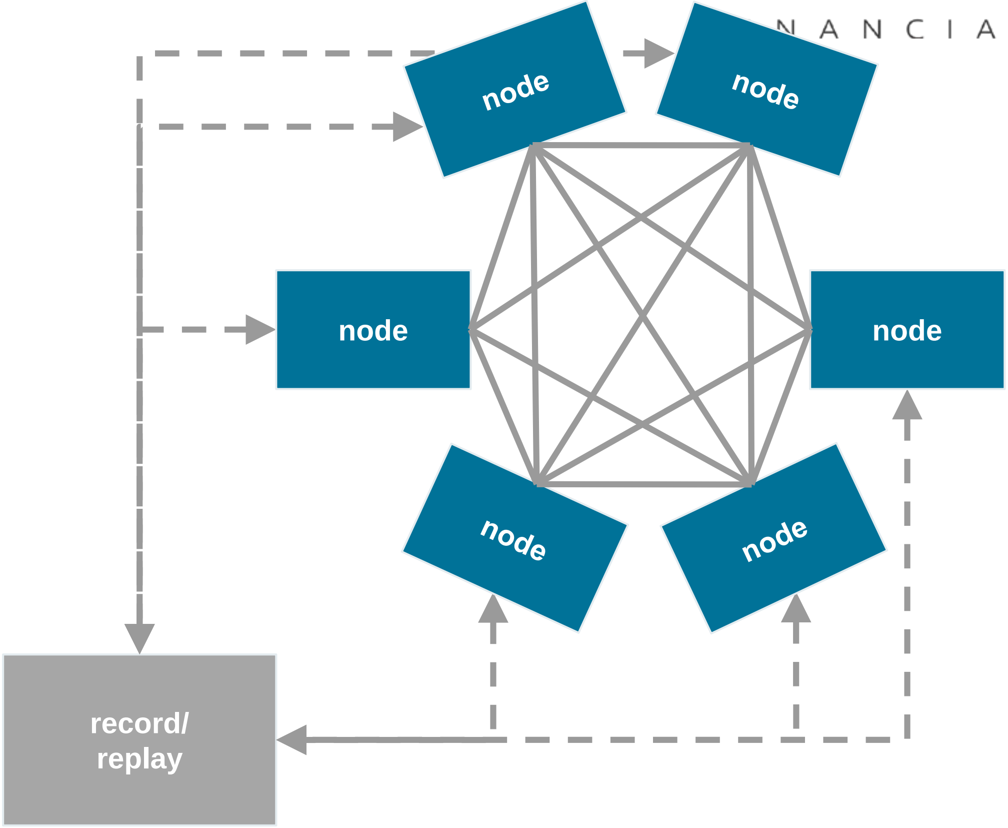
1) Test each component in isolation
2) Test system in a tightly controlled environment



DS TEST STRATEGIES

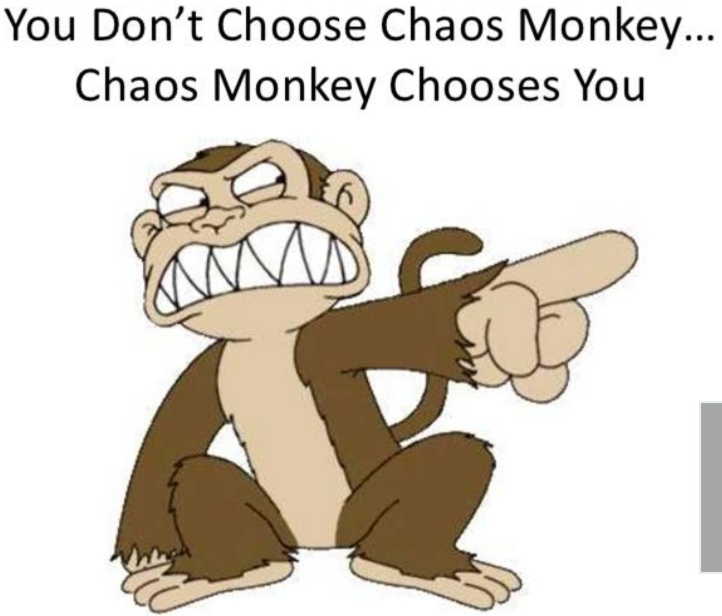
- Isolate
- Make it deterministic
- Inject faults

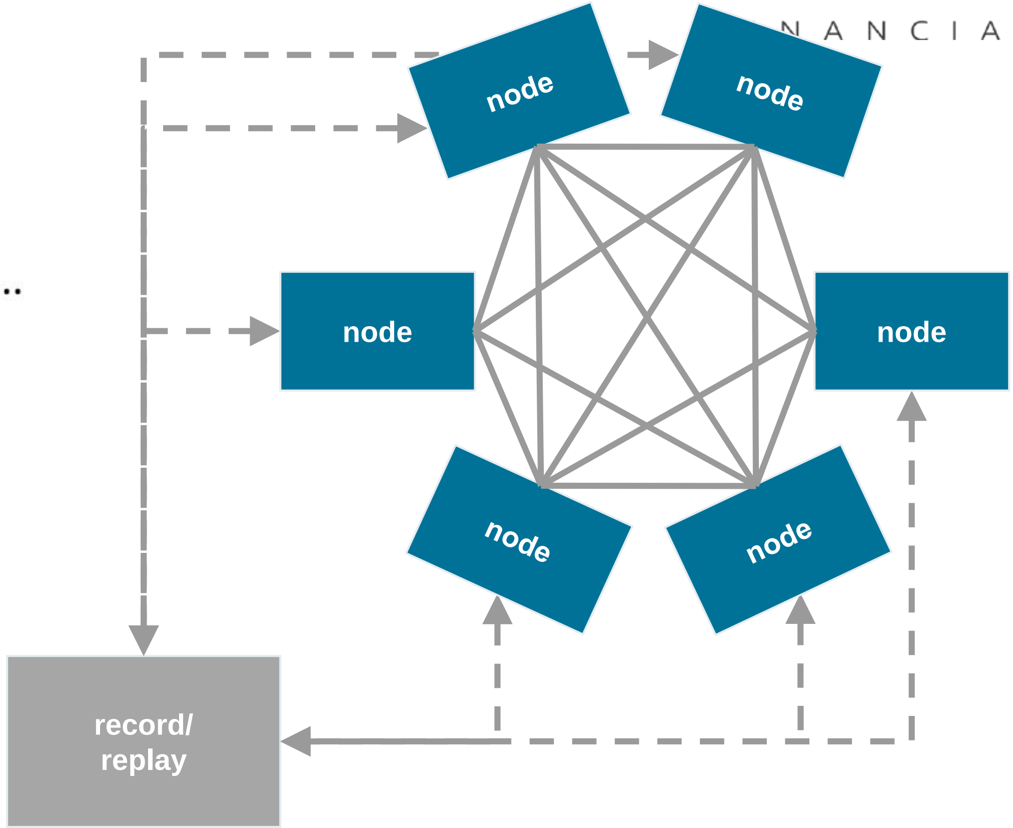
1) Test each component in isolation
2) Test system in a tightly controlled environment
3) Deal with non-determinism



DS TEST STRATEGIES

- Inject **random** faults!





FURTHER CHALLENGES

- Adversarial environments
  - DLT systems intended for networks with limited trust
- Non-functional testing
  - Ensuring non-functional requirements is hard in a distributed system
- Security testing
  - A DLT is essentially a cryptographic system
- Version and change management
  - Backwards compatibility

VALIDATION RULES

VALIDATION RULES

- Network participants agree on what’s valid and what’s not valid
- They follow a set of shared rules, the **validation rules**
- Rules can be hard-coded or ad-hoc (“smart contracts”)

- Tradeoffs between complexity, flexibility and security
  - Complexity is caused by flexibility
  - Simplicity favors security
- Heavily influences testability and QA

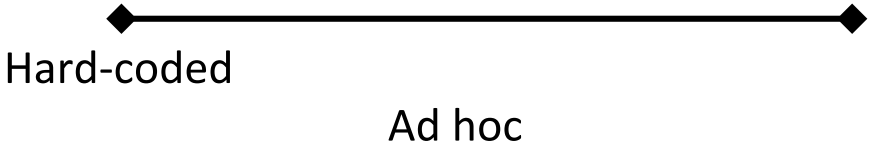
VALIDATION RULES

- Challenges:
  - Make absolutely consistent across diverse systems/architectures
  - The more complex the rules, the larger the state space

- Can be tackled with the usual testing/QA methods
  - Model/black-box testing
  - Unit testing, regression testing, etc

- Some tips:
  - Keep it simple
  - Keep it self-contained
  - Keep it stateless

HARD-CODED VS. AD HOC

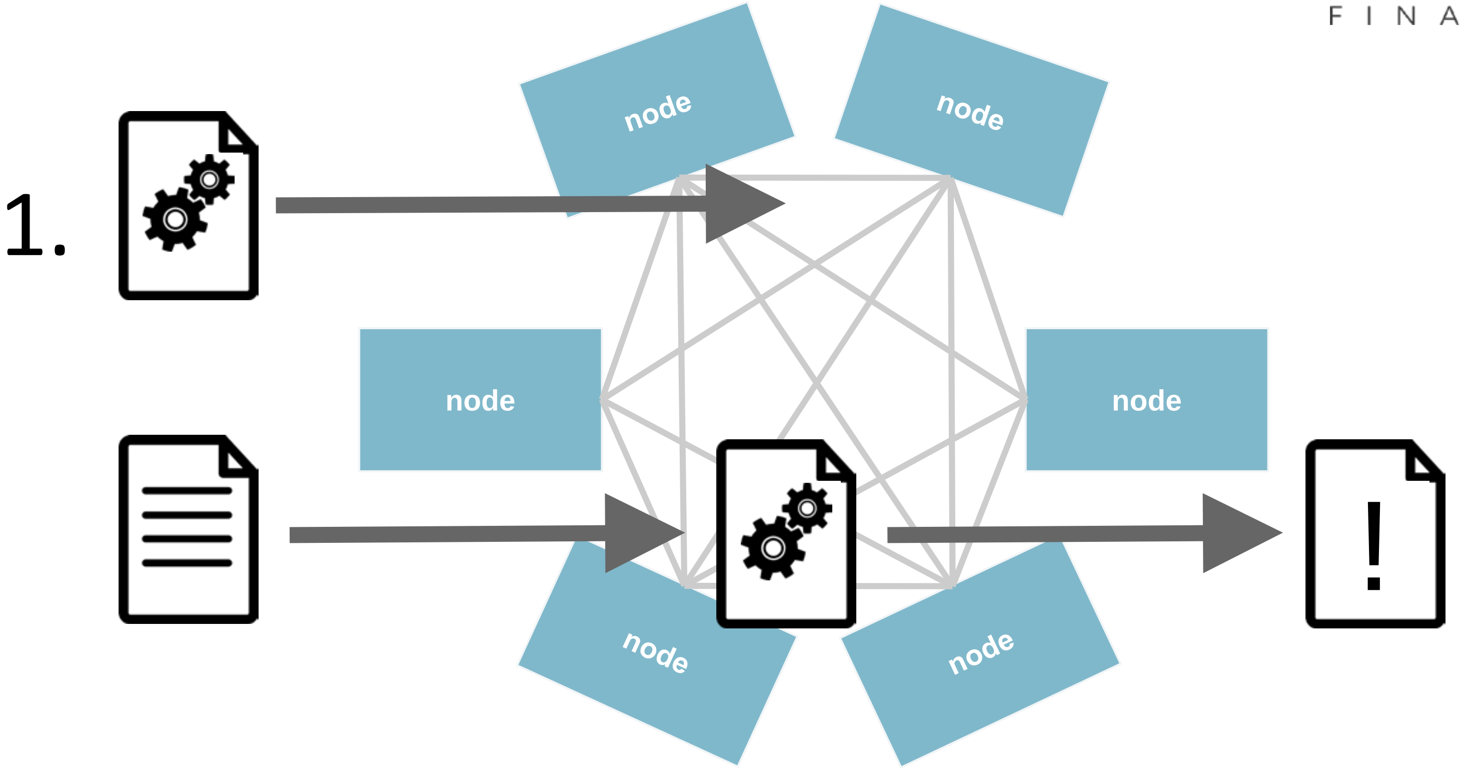


- Encode validation rules in blockchain engine
  - Tight control on rule implementation
  - Thoroughly reviewed and tested

- More flexible are extensions using scripting languages
  - Bitcoin uses a very limited stack-based language

- Smart contracts

SMART CONTRACTS



SMART CONTRACTS

- Smart contracts **transfer risk** from the DLT provider to the DLT user
  - User has to do testing and QA

- Most smart contract languages are Turing complete
  - High complexity
  - Infinite state space

- Additional complexity from interactions between smart contracts
  - These might be from different providers

SMART CONTRACTS

From the user’s perspective:

- Testing/QA of a (Turing complete) program...
  - ...that potentially interacts with other programs
  - ...in a distributed, non-deterministic system
  - ...on a dynamically changing and expanding network
  - ...using evolving rules and features

SUMMARY

TESTING CHALLENGES

- Distributed systems are really hard to test
  - DLT systems are even harder

- Testing/QA of validation rules is crucial
  - Complexity makes testing hard

- Smart contracts testing is unsolved
  - Risk lies with the user

RECOMMENDATIONS

RISE FINANCIAL

Stay focused:

- Limit scope, chose the right use-case

Test components:

- Isolate, inject faults!

Test non-deterministically:

- Record/replay
- Unleash the Chaos Monkey

Arne Brutschy, PhD
arne@rise-technologies.com
www.rise-technologies.com

DISCLAIMER

This Document (the Document) has been prepared by RISE Financial Technologies Ltd (RISE) for the purpose of setting out certain confidential information in respect of RISE's business activities and products. References to the "Document" includes any information which has been or may be supplied in writing or orally in connection with the Document or in connection with any further inquiries in respect of the Document. This Document is for the exclusive use of the recipients to whom it is addressed.

This Document and the information contained herein is confidential. In addition to the terms of any confidentiality undertaking that a recipient may have entered into with RISE, by its acceptance of the Document, each recipient agrees that it will not, and it will procure that each of its agents, representatives, advisors, directors or employees (collectively, Representatives), will not, and will not permit any third party to, copy, reproduce or distribute to others this Document, in whole or in part, at any time without the prior written consent of RISE, and that it will keep confidential all information contained herein not already in the public domain and will use this Document for the sole purpose of familiarising itself with certain limited background information concerning RISE and / or its business activities and products. This Document is not intended to serve as basis for any investment or contractual decision. If a recipient has signed a confidentiality undertaking with RISE, this Document also constitutes Confidential Information for the purposes of such undertaking.

While the information contained in this Document is believed to be accurate, RISE have not conducted any investigation with respect to such information. RISE expressly disclaim any and all liability for representations or warranties, expressed or implied, contained in, or for omissions from, this Document or any other written or oral communication transmitted to any interested party in connection with this Document so far as is permitted by law. In particular, but without limitation, no representation or warranty is given as to the achievement or reasonableness of, and no reliance should be placed on, any projections, estimates, forecasts, analyses or forward looking statements contained in this Document (if any) which involve by their nature a number of risks, uncertainties or assumptions that could cause actual results or events to differ materially from those expressed or implied in this Document. Only those particular representations and warranties which may be made in a definitive written agreement, when and if one is executed, and subject to such limitations and restrictions as may be specified in such agreement, shall have any legal effect. By its acceptance hereof, each recipient agrees that none of RISE nor any of their respective Representatives shall be liable for any direct, indirect or consequential loss or damages suffered by any person as a result of relying on any statement in or omission from this Document, along with other information furnished in connection therewith, and any such liability is expressly disclaimed.

Except to the extent otherwise indicated, this Document presents information as of the date hereof. The delivery of this Document shall not, under any circumstances, create any implication that there will be no change in the affairs of RISE or the products described herein after the date hereof. In furnishing this Document, RISE reserve the right to amend or replace this Document at any time and undertake no obligation to update any of the information contained in the Document or to correct any inaccuracies that may become apparent.

This Document shall remain the property of RISE. RISE may, at any time, request any recipient, or its Representatives, shall promptly deliver to RISE or, if directed in writing by RISE, destroy all confidential information relating to this Document received in written, electronic or other tangible form whatsoever, including without limitation all copies, reproductions, computer diskettes or written materials which contain such confidential information. At such time, all other notes, analyses or compilations constituting or containing confidential information in the recipient's, or their Representatives', possession shall be destroyed. Such destruction shall be certified to RISE by the recipient in writing.

Neither the dissemination of this Document nor any part of its contents is to be taken as any form of commitment on the part of RISE or any of their respective affiliates to enter any contract or otherwise create any legally binding obligation or commitment. RISE expressly reserve the right, in their absolute discretion, without prior notice and without any liability to any recipient to terminate discussions with any recipient or any other parties.