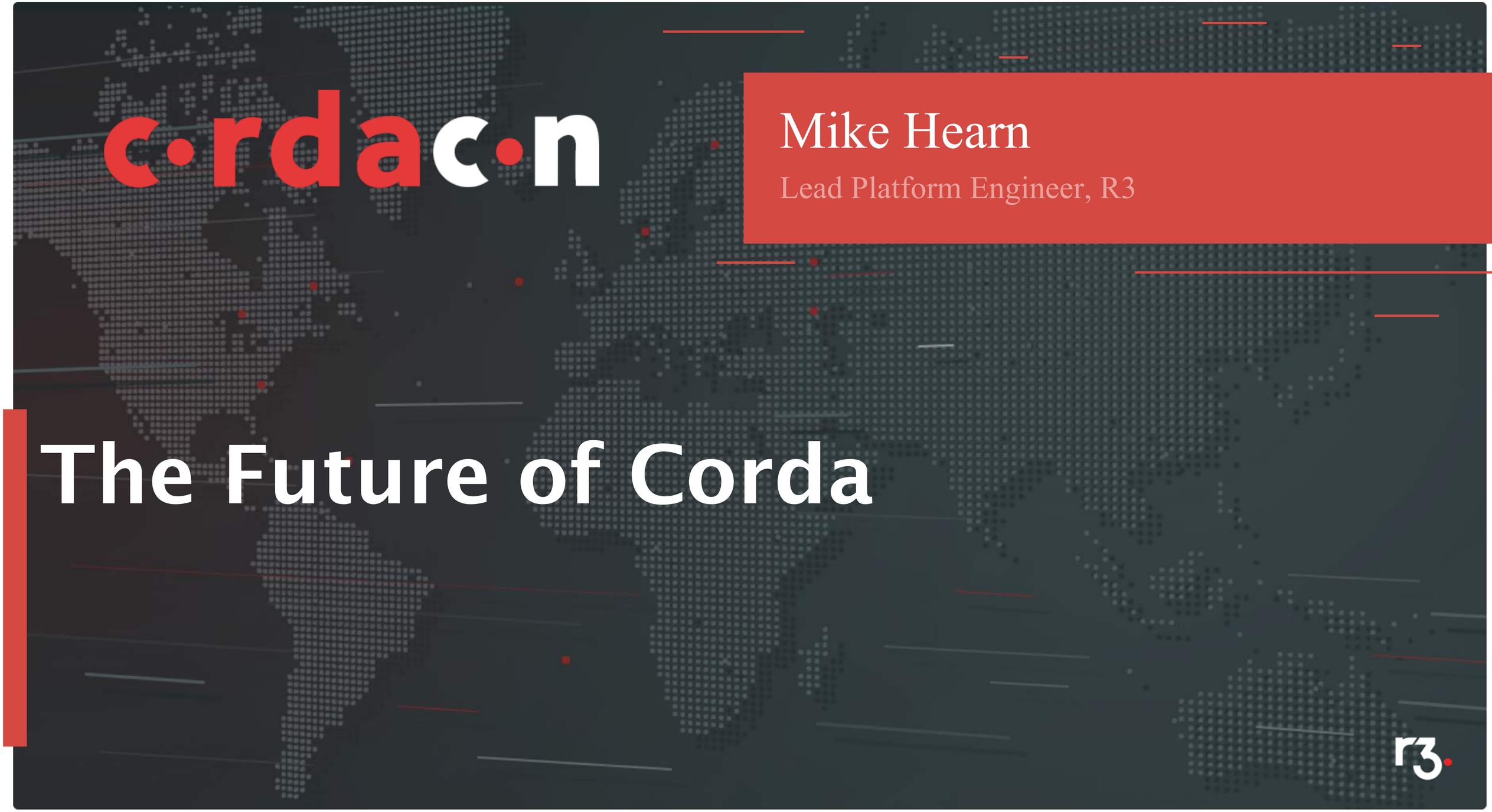


Mike Hearn

Lead Platform Engineer, R3

The Future of Corda

r3

Agenda

- Phased rollouts, zone parameters and governance
- Short term priorities
- Imagining the future

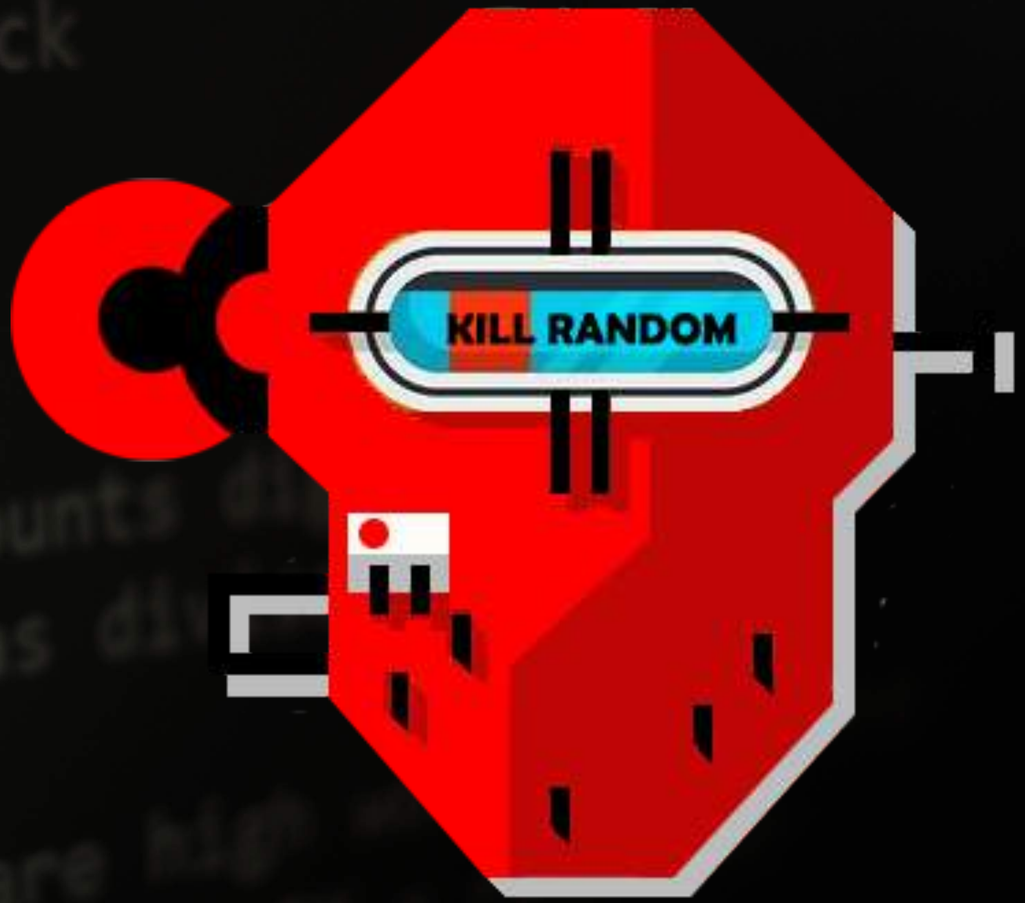
Rollouts & Zones

Completing the Corda Design

r3

Deterministic JVM preview

- Smart contracts give the *same answer* to *everyone*.
- The Corda **DJVM** is our answer to Ethereum's EVM.
- Subset of the Java platform that removes all sources of non determinism like timers, RNGs, GC callbacks etc.
- Existing apps opt in and will not break.
- Goal: ship a developer preview with IDE integration so testing and adaptation can begin. Long notice period.



The Determinator

r3.

Intel SGX preview

- **Reminder:** Intel SGX allows us to *encrypt the entire ledger*.
- Automatic, awesome, seamless privacy for everything: fast.
- First cut DJVM is running inside an SGX enclave.
- Next step after DJVM is to ship a preview of an SGX node.
- Aiming for feature complete this year, ship next year.

Code mobility: completing the vision

- Public blockchain systems allow anyone to run code on them.
- Corda does not (yet)
- Not a big deal – in Corda you don’t see data that’s irrelevant anyway.
- But sandboxed bytecode is a part of every blockchain since Bitcoin. So we want this too, for long transaction chains and big zones.
- Once DJVM is deployed apps that target it can be executed in the sandbox. This capability is thus activated on a per-app level.

Phased rollouts: completing the vision

We have committed to backwards compatibility.

BUT Corda is not currently restrictive enough to achieve the long term vision:

- Can write non-deterministic code inside contracts.
- Can write accidentally blocking code inside flows.
- Can run a node on CPU/OS without SGX support.

So what to do?

Phased rollouts: completing the vision

- Every node has a **platform version.**
- Every app has a **target version.**
- Every app today has targetVersion=1 (cannot set it ☺)
- Target versions let apps *opt in* to breaking changes.
- Zones can specify a minimum platform and target version.

Phased rollouts: completing the vision

Well written and maintained apps will keep their target version set **close or equal** to the latest platform version they want to support.

Target version lets us:

- Work around app bugs in the platform.
- *Without* hurting other apps that don’t have those bugs.
- Introduce changes that are not fully compatible like DJVM and SGX without breaking apps that aren’t ready for it.

Zone governance: the upgrade cycle

- Some features need everyone to upgrade before they can be used.
- Corda equivalent of a “hard fork”
- How to organize, schedule and enforce such an upgrade?
- Zone operator’s job – R3 will use a governance mechanism to figure out the details for our zone.

Zone governance:
The Constitution

Network parameters

The set of all things on which reasonable people might disagree

(and which are not fixed by the design)

Zone governance:
Example network parameters

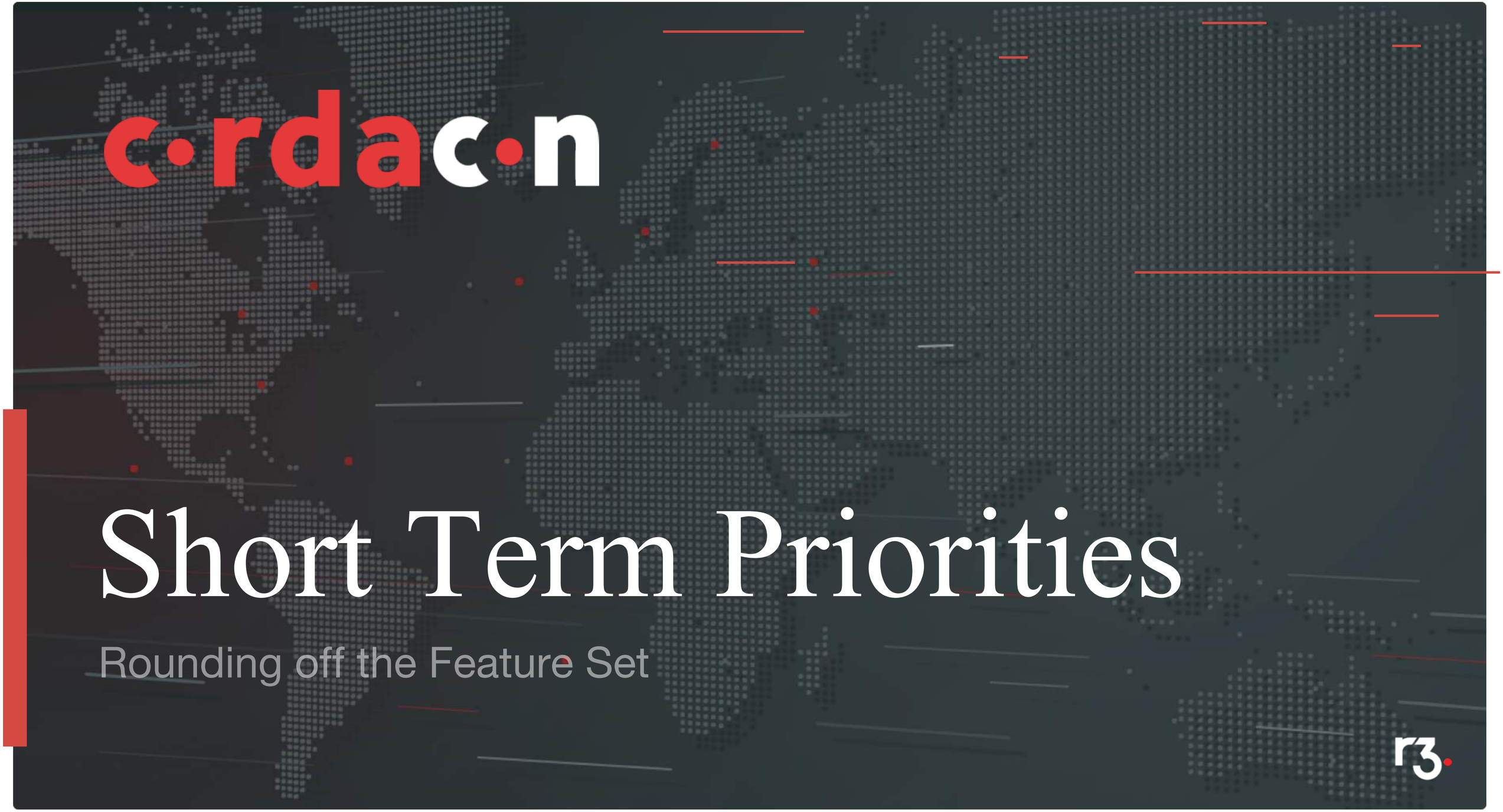
- Max transaction and message sizes
- Minimum platform version
- Event horizon time
- Which notaries to trust
- Supported cryptographic algorithms and rollout schedules
- Port numbers
- Whether or not IPv6 is mandatory
- Whether or not the *internet* is mandatory!
- SGX rollout status
- Application whitelists, if wanted (allows to opt out of determinism)

Zone governance:
Example of non-parameters

Not intended to be about:

- Picking winners
  (i.e. enforcing particular apps, schemas, service providers, workflows or models)
- Controlling what the users can do
- Being Evil™

- Example:
  Zone operator decisions can be sometimes overridden



Short Term Priorities

Rounding off the Feature Set

r3

Security upgrades

- **HSM support** (partly done already)
- Additional **security audits** of key components
- Sandbox isolation of internal components, for bug resistance
- **Audit framework**

Short term priorities

- Round off edge cases in the data model and contracts
- Ship previews of the DJVM and SGX
- Bug fixing and improved automatic testing
- **Human interaction**
- **Scale to massive numbers of hosted identities**

Human interaction

- *Flows* are how Corda coordinates changes to the ledger.
- Straight-line code that can interact with other organizations.
- Flows should be able to interact with individuals as well.
- **Step 1:** allow flows to send/receive on arbitrary message Qs.
- **Step 2:** build connectors to popular ticketing systems.
- **Step 3:** (possibly) Desktop and/or mobile apps to approve signing.

Scale to massive number of firms

- **Unexpected opportunity:** projects that want to on-board thousands of companies

- **New requirement:** desire for *hosted identities* where:

1. The legal owner of the identity holds the keys, but
2. The legal owner of the identity does not run the node

- Two pronged effort, probably to start later this year (maybe).

PROPOSAL ONLY: FEEDBACK DESIRED

Project MAXIMUS

Enable R3 Corda nodes to host huge numbers of identities

1. Split the MQ broker out of the node.

2. Have a supervisor process start flow workers on demand when traffic arrives for an identity.

3. Federated on-boarding.

4. Flows and procedures for negotiated node takeover by the identity owner if and when they graduate.

Long Term Vision

The Automatable Economy

r3

The automatable economy

Where is this all going?

How does blockchain interact with artificial intelligence, if at all?

Are we just making things more efficient or is there more to it?

The automatable economy

- **HTTP** is the protocol for talking to web servers

  … ‘**spiders**’ are bots that crawl the web

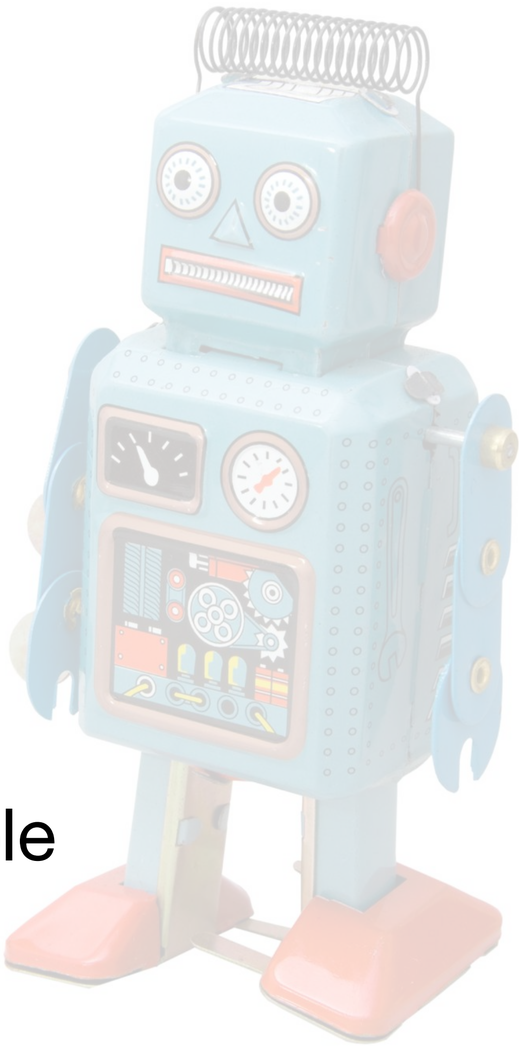
- **SMTP / IRC / Slack** are protocols for talking to people

  … ‘**mailing lists**’ are bots that redistribute emails

  … ‘**chatbots**’ are bots that hold conversations with people

- **Corda flows** are protocols for talking to businesses

  … so … ‘**agents**’ are bots that start business workflows?



The automatable economy

Imagine lightweight Corda apps for invoicing, buying and selling.

Need a workshop for industry participants to build CorDapps together:

- Food deliveries
- Conference space
- Flight tickets
- Event tickets

“Alexa, organize me a conference”

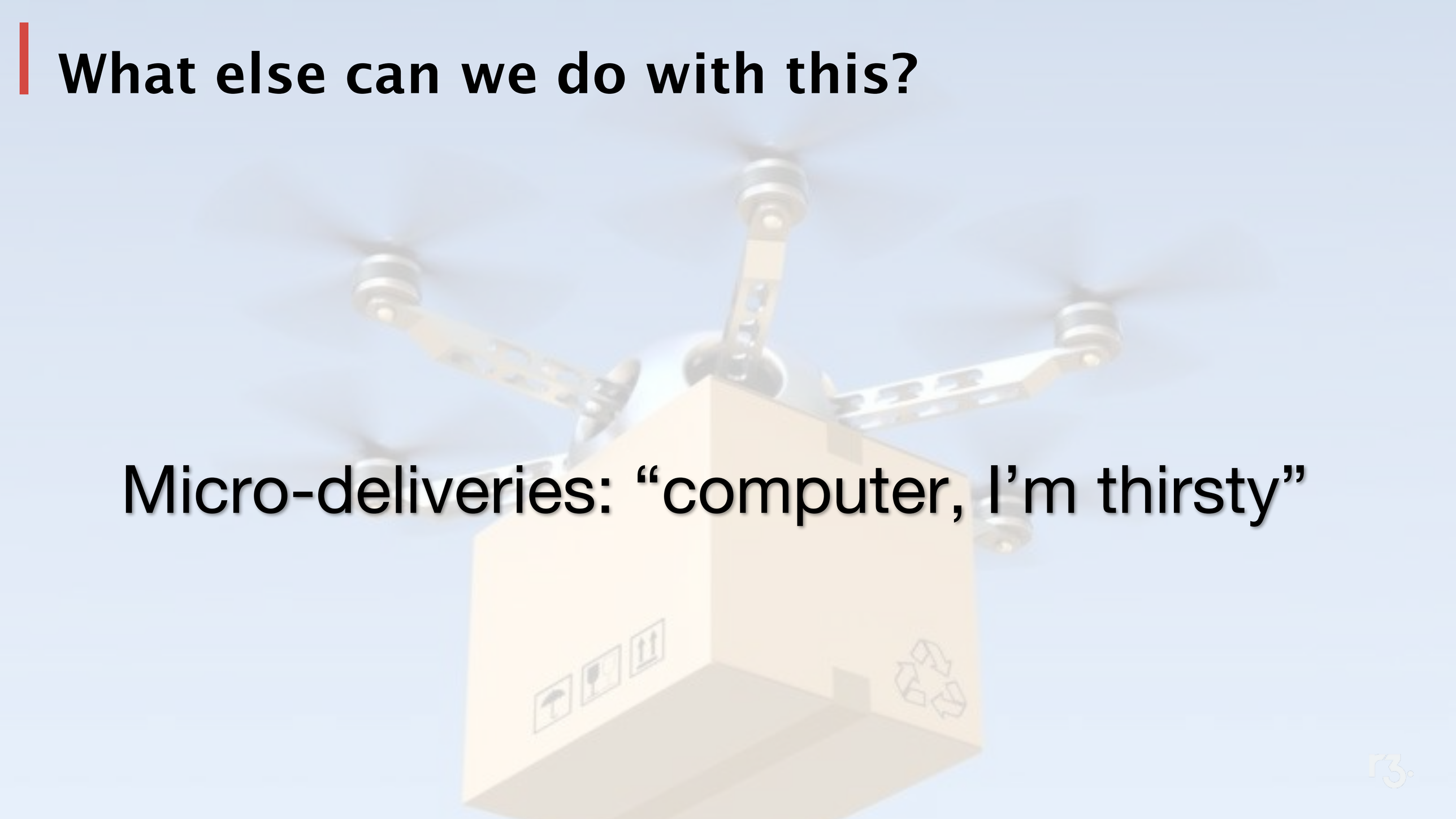
The automatable economy

How smart can these bots get?

1. A/B testing on suppliers.
2. Deep reinforcement learning using HappyOrNot boxes to train the AI.
3. Use smart contracts and SGX to enable bots to trust other bots. Trustworthy business partners guaranteed!

Start with simple, commodity, low-dimensional problems like booking flights and hotels.

What else can we do with this?



Micro-deliveries: “computer, I’m thirsty”

What else can we do with this?

Micro-insurance

“computer, do an insured software update to my web servers”

What else can we do with this?

Global trade optimization

Project Ubin: decentralized, private, p2p net-out for arbitrary ledger tokens

Model all fungible commodities as tokens

Run continuous net-out for physical shipments

Competitors may end up shipping to each other

What else can we do with this?

Speculative trade execution

Train a deep neural network inside an SGX enclave on all invoices from all businesses simultaneously

DNN learns how to pre-order goods and services **before** a business owner knows they need them

DNN driven agent could be programmed to be non-profit

Autonomous agents

Agents may be funded via crowdfunding

Or as a public service by governments, or business consortia

Or **they may reproduce using profits previously earned**

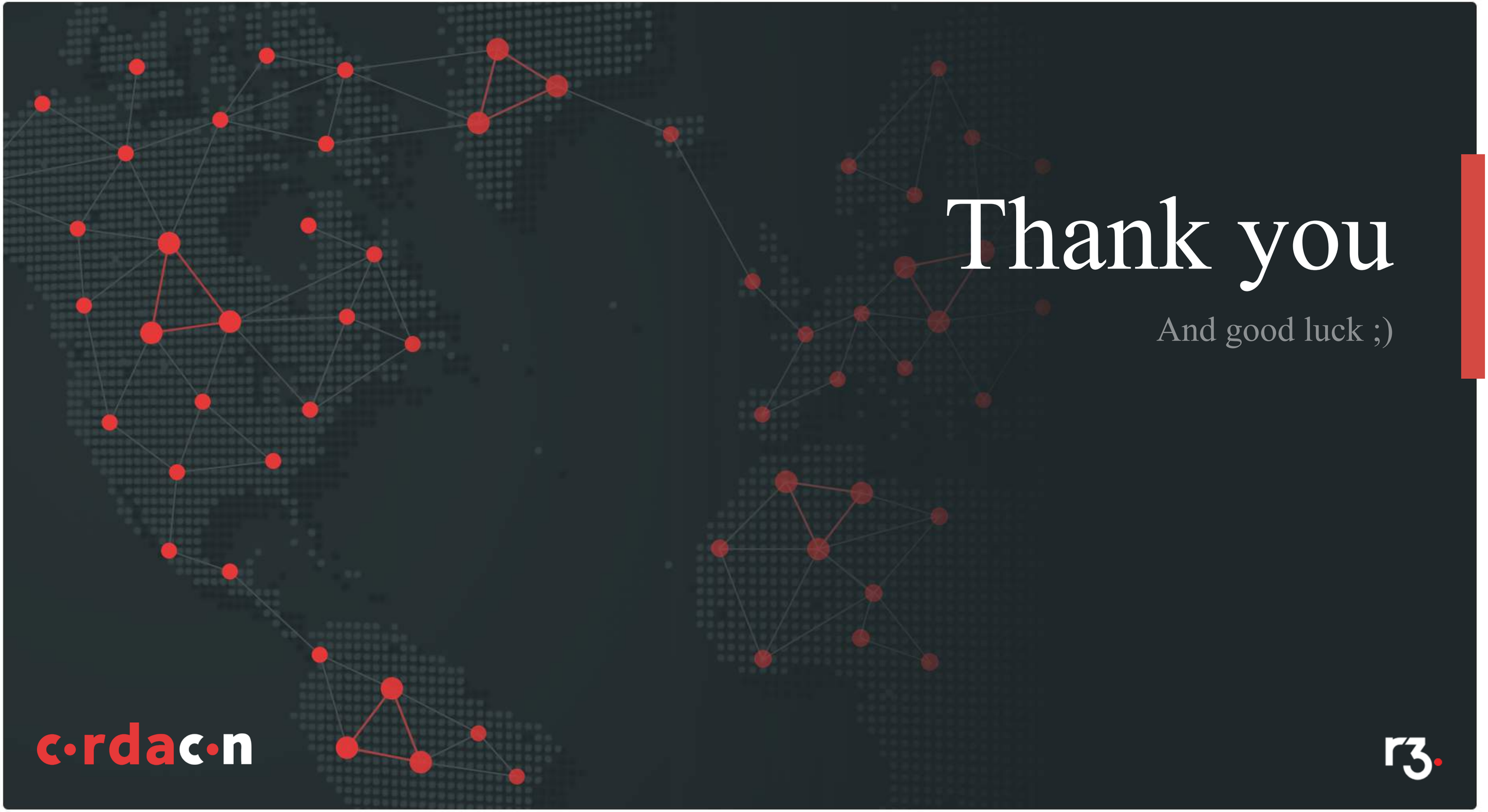
Agents embedded in robots may order babies from the factory

using e.g. the SelfDrivingCarPurchase CorDapp

Agents may charge their offspring for being born via ‘birth loans’

Agents may be more trustworthy than people and so outcompete them.

r3.


Thank you
And good luck ;)
corda con
r3.


<backup slides>
c·rdac·n

Corda Desktop

A dedicated, cheap, single purpose computer with a custom OS.

Used only for signing transactions and other secure business activities.

Does not allow arbitrary apps to be installed.

Flows get new API to interact with it.

Potential future feature: secure PDFs (cannot be printed, forwarded or screenshotted, watermarked video?)

Long term possibility to evolve into a hardened device for industrial control?