



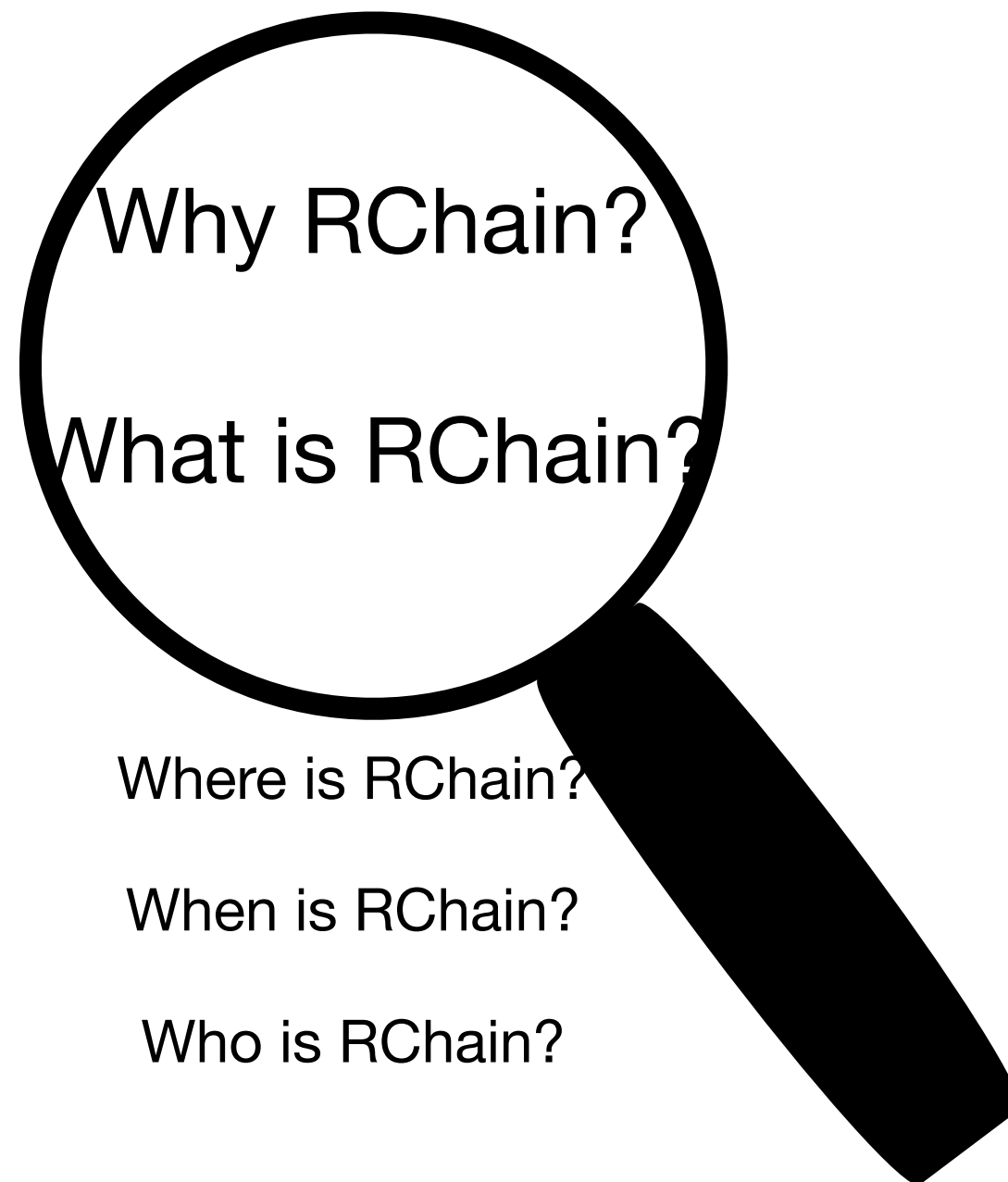
RChain
COOPERATIVE

An introduction

Lucius Gregory Meredith

An introduction

Who, What, Where, Why, When?





An introduction

Who, What, Where, Why, When?

Where is RChain?



When is RChain?

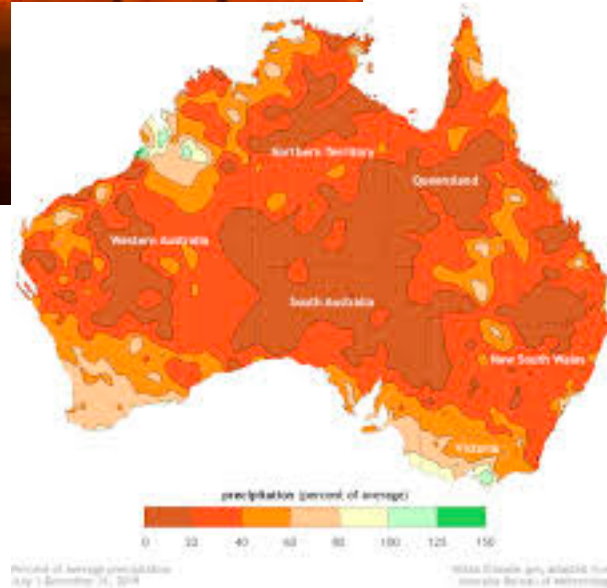


Who is RChain?

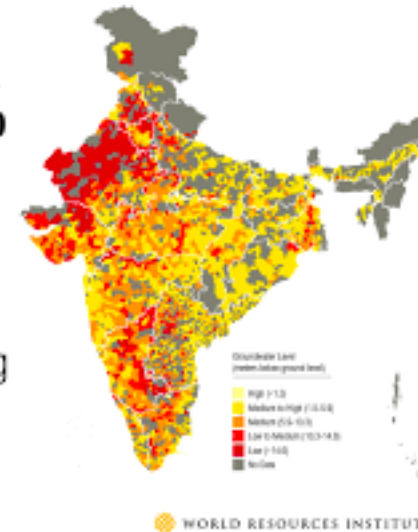


Why RChain?

To address climate change and other existential threats we need a global coordination technology



54%
of India's
Ground-
water
Wells Are
Decreasing



Covid-19: Almost 3,000 lorries stuck in Kent as UK and France aim to restart freight

© 22 December 2020

Coronavirus pandemic

In the case of climate change, governments and corporations are moving too slow

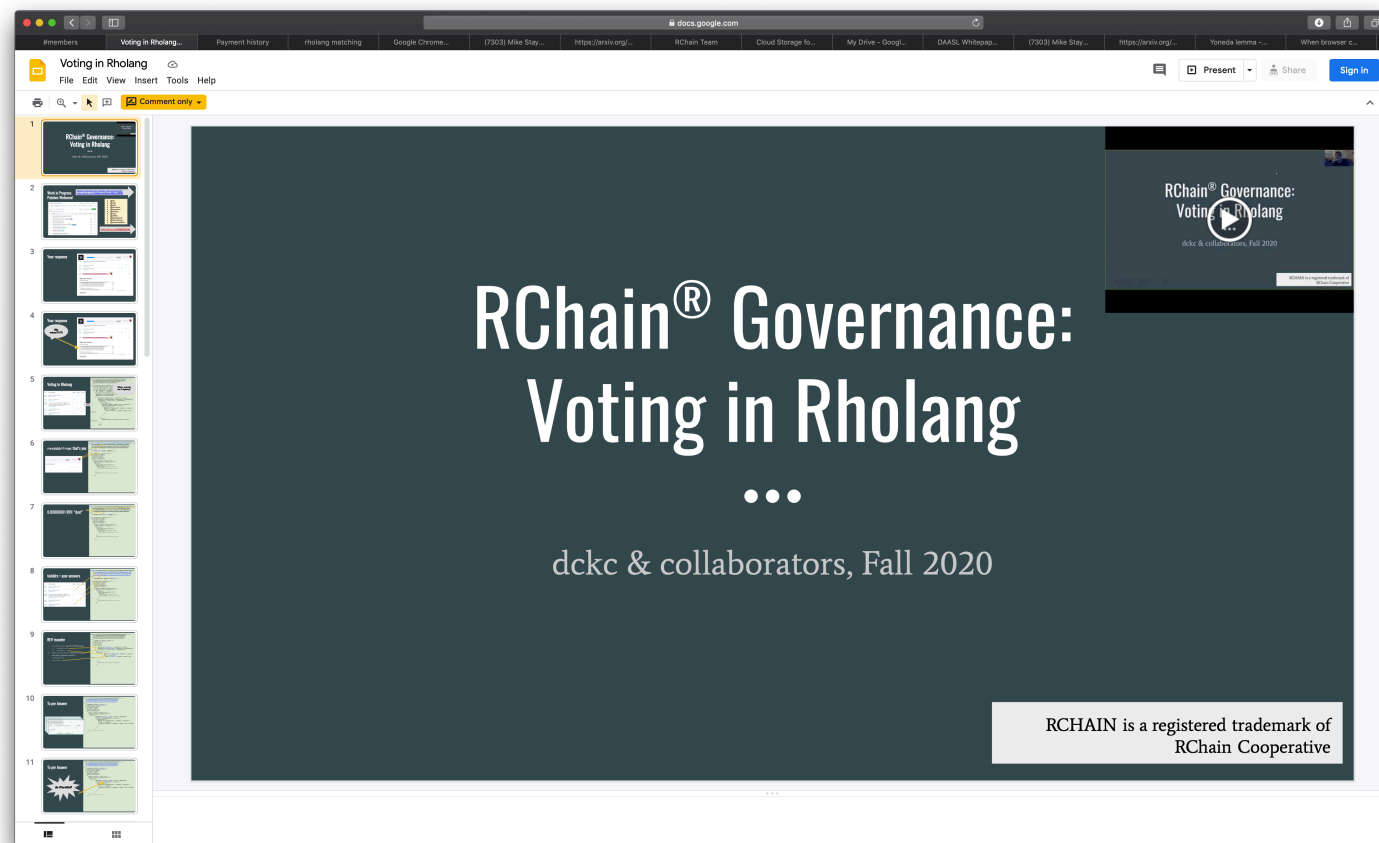
Greta Thunberg: 'We are speeding in the wrong direction' on climate crisis

Exclusive: Climate striker speaks before UN event marking five years since the Paris accord



Why RChain?

Hypothesis: with appropriate coordination technology we will see more and more instances of self-organization



The *RChain Community* built a cryptographically secure on-chain voting mechanism.

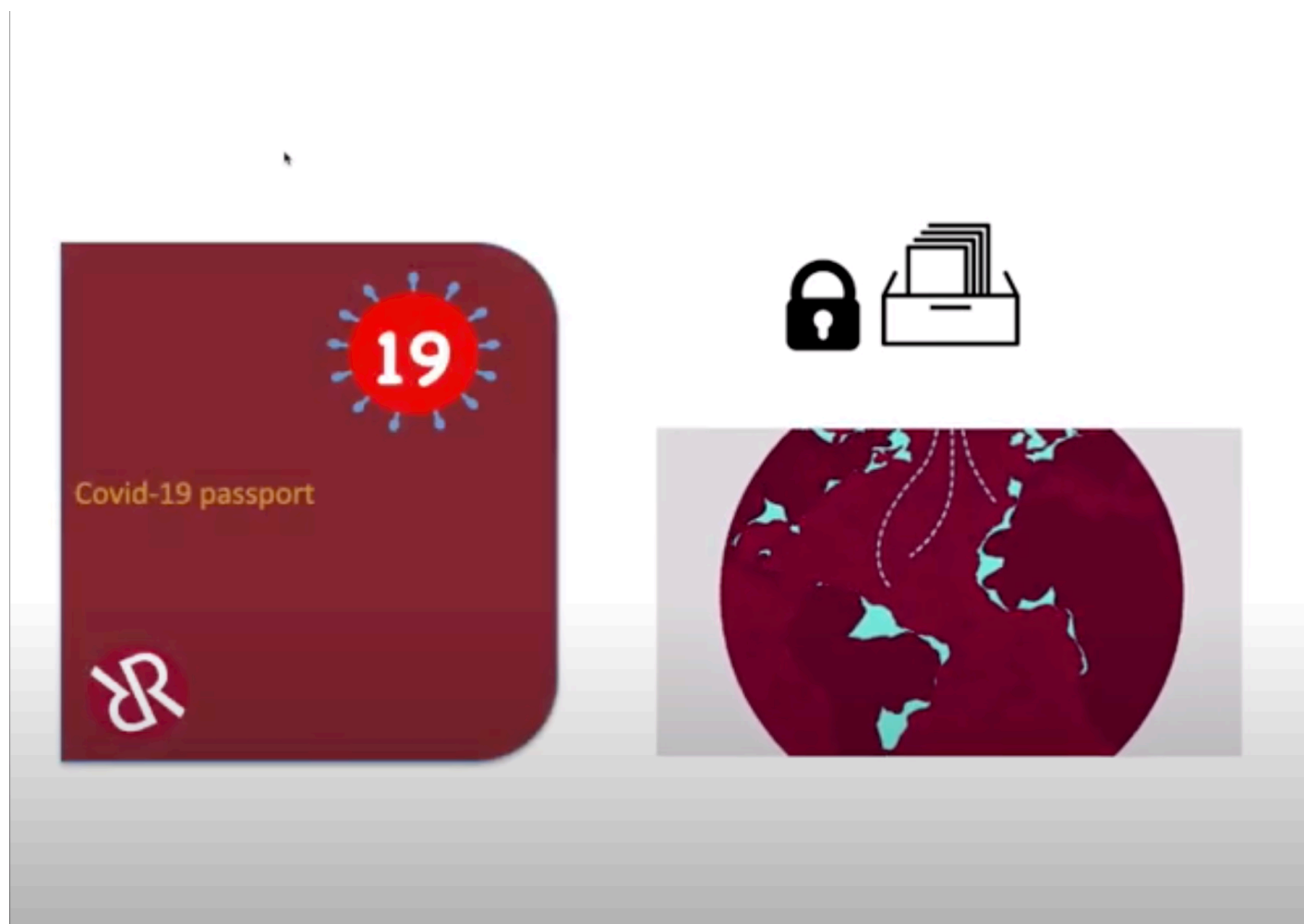
Members from around the globe voted from the safety of their home.

They could check the results of the election themselves without fear that other members would know their vote.



Why RChain?

Hypothesis: with appropriate coordination technology we will see more and more instances of self-organization



The *RChain Community* built a cryptographically secure on-chain COVID-19 passport.

People can store encrypted proof of vaccination and test results on-chain.

Their data is not situated behind the firewall of a private company.



What is RChain?

RChain the organization

Like many utility and financial service companies around the globe, RChain is a cooperative.

One member, one vote.

RChain's membership spans the globe, with members in China, Croatia, Russia, UK, US, and ...

The function of the cooperative is to facilitate governance of the protocol.





What is RChain?

RChain the technology

RChain revises the blockchain proposal in the following ways.

At the heart of every blockchain worthy of the name is an ***economically secured, leaderless distributed consensus algorithm.***

With such an algorithm autonomous programs can agree on a locally stored value.



Bitcoin nodes store a ledger.

Ethereum nodes store the state of a virtual machine.



RChain changes the proof-of-work algorithm to pure proof-of-stake.

RChain nodes stores the state of a *concurrent* virtual machine.

The machine is realized in terms of a new kind of Tuple Space.



RChain Research



What is RChain?

Why is concurrency so important?

An 8 lane freeway with negligible lane crossing gets roughly
8x
the throughput of a 1 lane freeway



What happens if all those lanes must be funneled down to 1 lane?





What is RChain?

Why is concurrency so important?

Someone buying empanadas from a street vendor in Santiago is almost certainly using different resources than someone else buying grilled tofu from a street vendor in Shanghai



Ethereum must serialize these transactions





What is RChain?

Why is concurrency so important?

This is true of all computational resources, and not just tokens





What is RChain?

What other aspects of models of computation are relevant?

	Completeness	Compositionality	Concurrency	Complexity	Reflection	Behavioral Types
Regular expressions	✗	✓	✗	✗	✗	✗
Turing machines	✓	✗	✗	✓	✗	✗
Lambda calculus	✓	✓	✗	✗	✗	✗
CCS	✓	✓	✓	✗	✗	✗
Petri nets	✓	✗	✓	✓	✗	✗
π -calculus	✓	✓	✓	✓	✗	✓
ambient calculus	✓	✓	✓	✓	✗	✗
join calculus	✓	✓	✓	✓	✗	✗
rho calculus	✓	✓	✓	✓	✓	✓



What is RChain?

Today's market requirements of the model of computation

$$P, Q ::= 0 \mid \text{for}(y \leftarrow x)P \mid x!(P) \mid P|Q \mid *x$$
$$x, y ::= @P$$

\equiv is the smallest equivalence
including α -equivalence making
 $P, 0$ is a commutative monoid

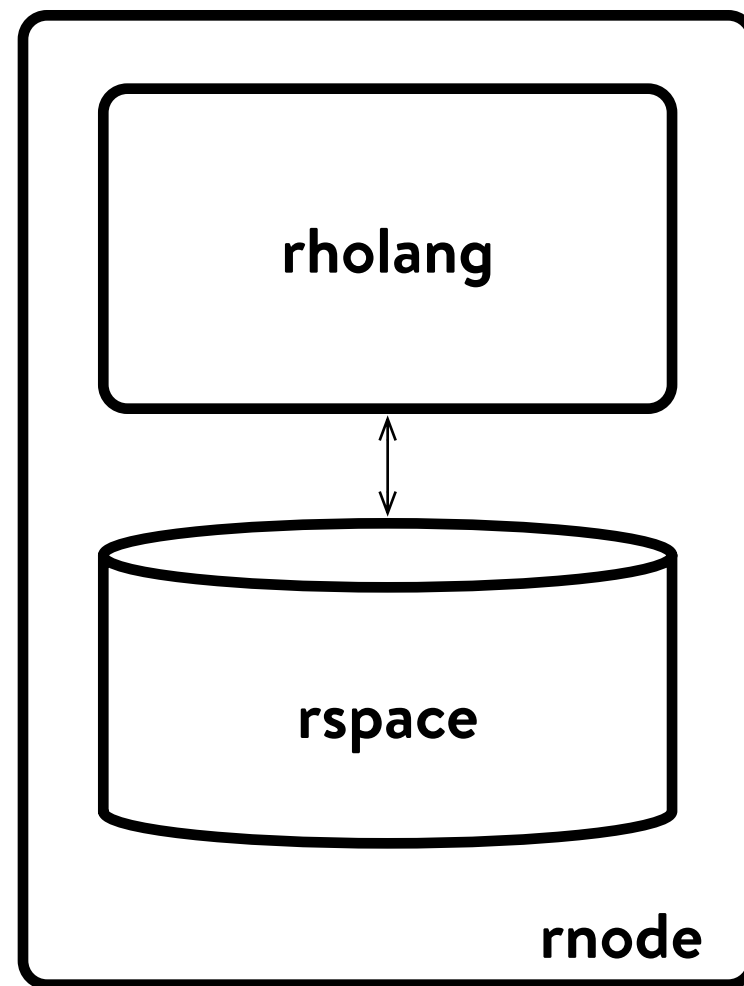
$$\text{for}(y \leftarrow x)P \mid x!(Q) \rightarrow P\{ @Q / y \}$$
$$P \rightarrow P' \Rightarrow P|Q \rightarrow P'|Q$$
$$P \equiv P', P' \rightarrow Q', Q' \equiv Q \Rightarrow P \rightarrow Q$$


No byte code injection
attacks!

Perfect correlation
between language
and execution
and storage

What is RChain?

Correctness is also an aspect of scalability



```
P, Q ::= 0 | for( y <- x ) P | x!( Q ) | P | Q | *x
x, y ::= @P
```

```
for( y <- x ) P | x!( Q ) -> P{@Q/y}
```

The semantics of rholang
is isomorphic to the semantics
of rspace

```
RSpace.consume( x, λy. P )
RSpace.produce( x, Q )
```



What is RChain?

Today's market requirements of the model of computation



```
for( amt1 <- shanghaiAccount )P( amt1 ) | wallet( shanghaiAccount )  
| for( amt2 <- santiagoAccount )P( amt2) | wallet( santiagoAccount )
```



What is RChain?

Today's market requirements of the model of computation

Rholang

To the rho-calculus rholang 1.0 adds

new names

pattern matching

joins

recursive definitions

while rholang 1.1 adds

synchronous i/o

let statements

RChain Research



What is RChain?

Today's market requirements of the model of computation

Transactional semantics

$\text{for}(\text{ptrn} \leftarrow x) P \mid x!(Q) \rightarrow P\{ @Q / y \}$

+ pattern matching reconciles SQL and NoSQL

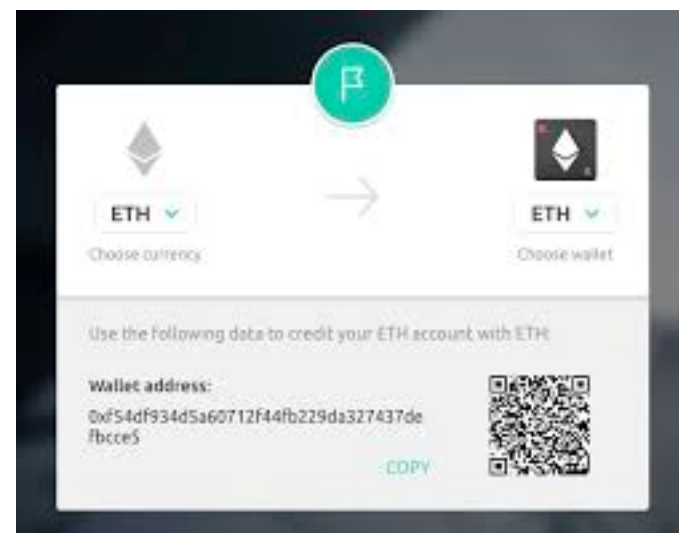
Making RChain a database as well as a smart contracting platform

What is RChain?

Namespaces



URLs inhabit namespaces



Blockchain addresses
inhabit namespaces



Even phone numbers
inhabit namespaces



What is RChain?

Namespaces

Rholang

$$P, Q ::= 0 \mid \text{for}(y \leftarrow x)P \mid x!(P) \mid P|Q \mid *x$$
$$x, y ::= @P$$

The original namespace gives names the structure of programs

Subnamespaces are mapped to

URIs

addresses

phone numbers

...

This structure is also used to detect conflict and support other static analysis, such as leaking secrets



What is RChain?

Consensus

Jump to radical fault tolerance in rholang

What is RChain?

OSLF in a nutshell

$$M, N ::= e \mid g \mid M * N$$
$$e * m = m = m * e,$$
$$(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$$
$$S, T ::= \text{true} \mid S \& T \mid \sim S$$
$$e \mid g \mid S * T$$
$$\langle m \rangle S$$
$$\sim e \& \sim(\sim e * \sim e)$$



What is RChain?

OSLF in a nutshell

$$M, N ::= e \mid g \mid M * N$$
$$e * m = m = m * e,$$
$$(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$$
$$S, T ::= \text{true} \mid S \& T \mid \sim S$$
$$e \mid g \mid S * T$$
$$\langle m \rangle S$$
$$\sim e \ \& \ \sim(\sim e * \sim e)$$
$$\text{Th} \dashrightarrow^y \text{Cat}(\text{Th}^{\text{op}}, \text{Set}) \dashrightarrow^{\text{Sub}} \text{Pos}$$
$$f_{\text{sub}} \circ y$$

What is RChain?

OSLF in a nutshell

$M, N ::= e \mid g \mid M * N$

$e * m = m = m * e,$
 $(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$

$S, T ::= \text{true} \mid S \& T \mid \sim S$
 $e \mid g \mid S * T$
 $\langle m \rangle S$

$\sim e \ \& \ \sim(\sim e * \sim e)$

$\text{Th} \dashrightarrow^y \text{Cat}(\text{Th}^{\text{op}}, \text{Set}) \dashrightarrow^{\text{Sub}} \text{Pos}$

$\int_{\text{sub}} \circ y$

What is RChain?

OSLF in a nutshell

$M, N ::= e \mid g \mid M * N$

$e * m = m = m * e,$
 $(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$

$S, T ::= \text{true} \mid S \& T \mid \sim S$

$e \mid g \mid S * T$
 $\langle m \rangle S$

$\sim e \ \& \ \sim(\sim e * \sim e)$

$\text{Th} \dashv\!\!\dashv y \dashv\!\!\dashv \text{Cat}(\text{Th}^{\text{op}}, \text{Set}) \dashv\!\!\dashv \text{Sub} \dashv\!\!\dashv \text{Pos}$

$\int_{\text{sub}} \circ y$

What is RChain?

OSLF in a nutshell

$M, N ::= e \mid g \mid M * N$

$e * m = m = m * e,$
 $(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$

$S, T ::= \text{true} \mid S \& T \mid \sim S$
 $e \mid g \mid S * T$
 $\langle m \rangle S$

$\sim e \ \& \ \sim(\sim e * \sim e)$

Add to Th the theory of graphs with
src of a rewrite being the redex
and trgt of a rewrite being the reduced term

$\text{Th} \dashv\!\!\rightarrow \text{Cat}(\text{Th}^{\text{op}}, \text{Set}) \dashv\!\!\text{Sub} \rightarrow \text{Pos}$

What is RChain?

OSLF in a nutshell

$M, N ::= e \mid g \mid M * N$

$e * m = m = m * e,$

$(m_1 * m_2) * m_3 = m_1 * (m_2 * m_3)$

$S, T ::= \text{top} \mid \text{bot} \mid 0 \mid 1 \mid \sim S \mid S * T \mid S \# T \mid S \& T \mid S + T$
 $e \mid g \mid S^* \mid$
 $\langle m \rangle S$

Th

— V-y-> V-Cat(Th^{op}, V) --Sub-> Pos

$\int_{\text{sub}} \circ V\text{-y}$

V = Girard quantale

V = Traced monoidal category with UDC



What is RChain?

Consensus

Open questions

Verification vs replay

Extension and
Implementation of OSLF

RChain Research