



Smart Contracts and REA Contracts

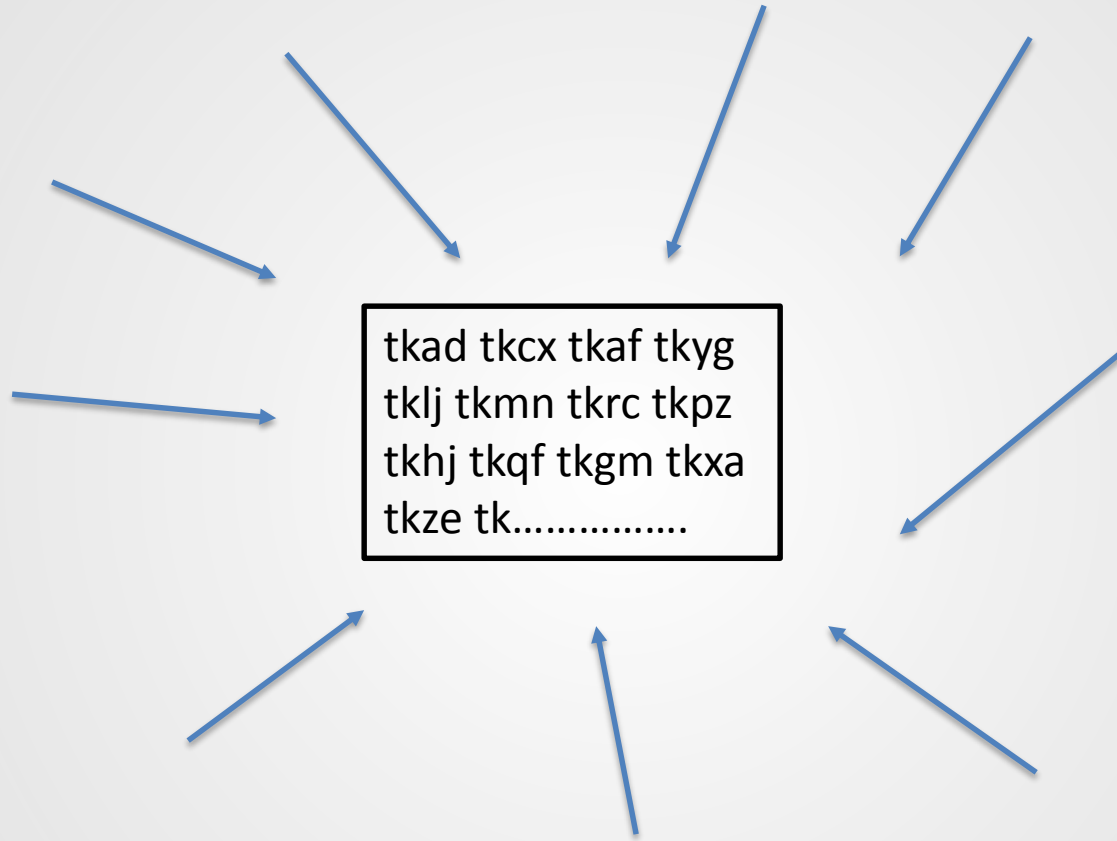
Dr. Graham Gal

Isenberg School of Management

What I will talk about

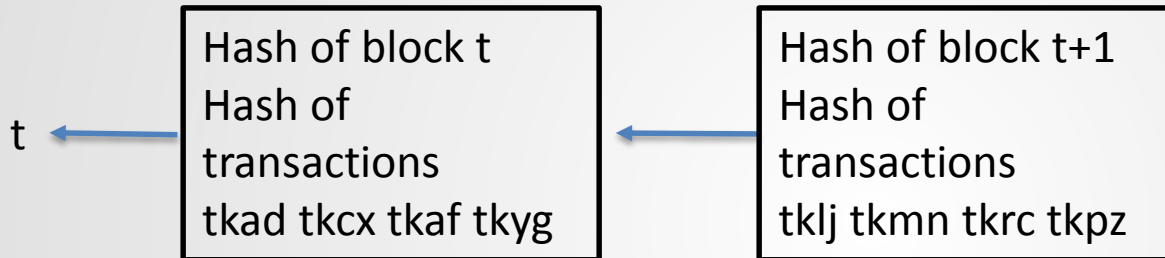
- Blockchain basics
- Trading Partner and Independent Views
- Contracts in these two views
- Tokenization
 - Universal Identifier
 - Tokenization of Rs, Es, and As

Getting Rid of Intermediaries – I trust No One



Creating a Trusted Time Ordered Sequence

tkad tkcx tkaf tkyg
tklj tkmn tkrc tkpz
tkhj tkqf tkgm tkxa
tkze tk.....



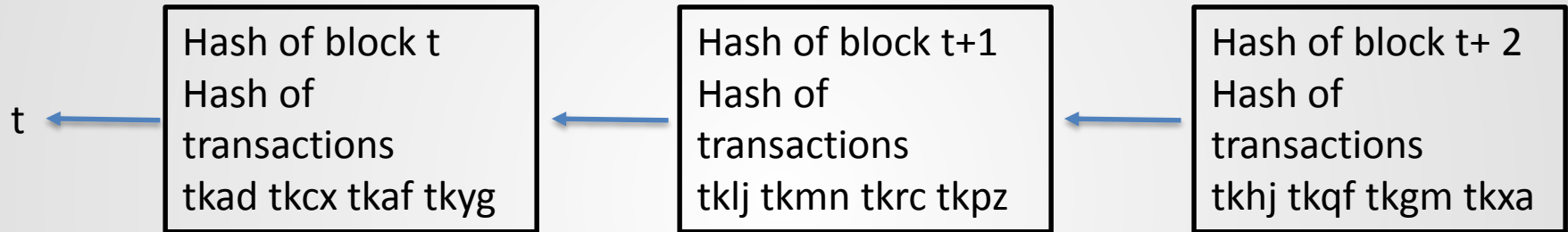
Now h wants to add a transaction to j

- 1) Signs on with private key (token)
- 2) Creates the transaction tkhj and attempts to add to the chain
- 3) Members of chain validate transaction

After sufficient number of validated transactions have been collected they are “Mined” into a new block and added to chain

Creating a Trusted Time Ordered Sequence

tkad tkcx tkaf tkyg
tklj tkmn tkrc tkpz
tkhj tkqf tkgm tkxa
tkze tk.....



Now h wants to add a transaction to j

- 1) Signs on with private key (token)
- 2) Creates the transaction tkhj and attempts to add to the chain
- 3) Members of chain validate transaction

After sufficient number of validated transactions have been collected they are “Mined” into a new block and added to chain

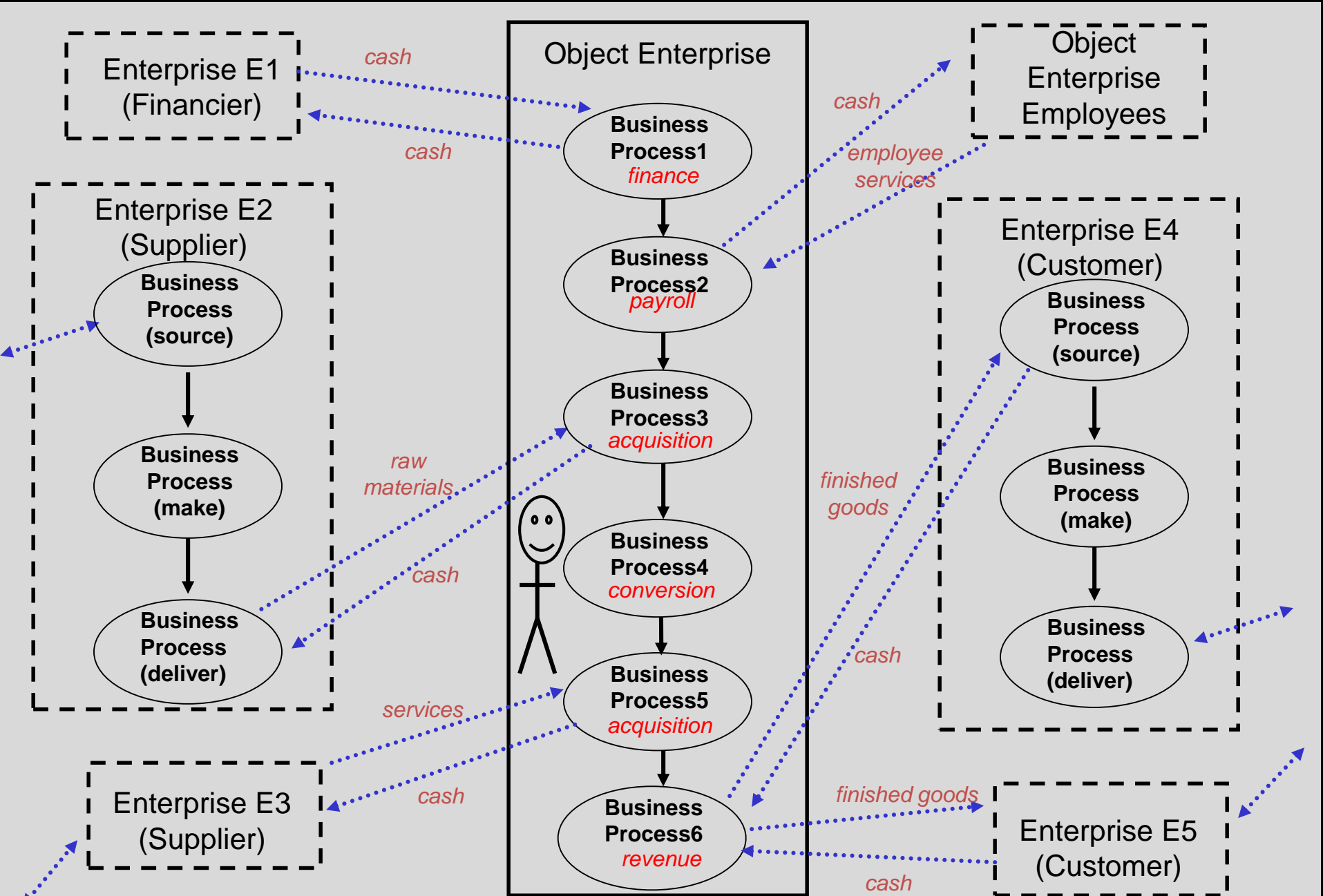
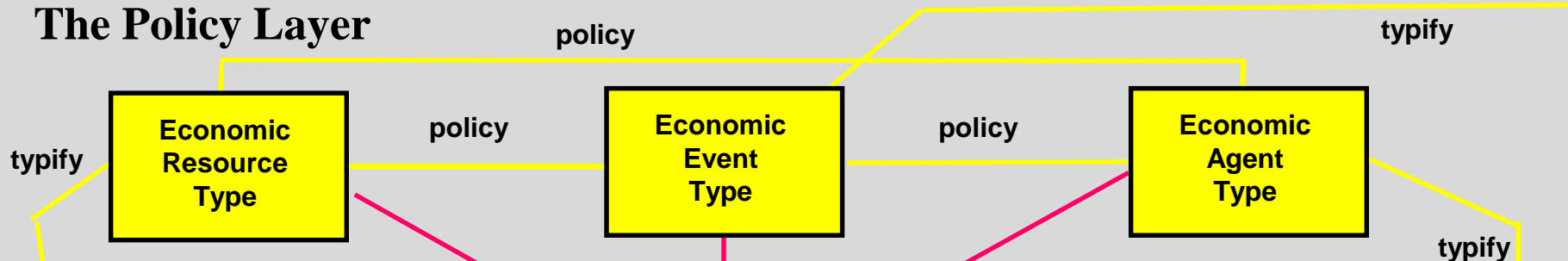


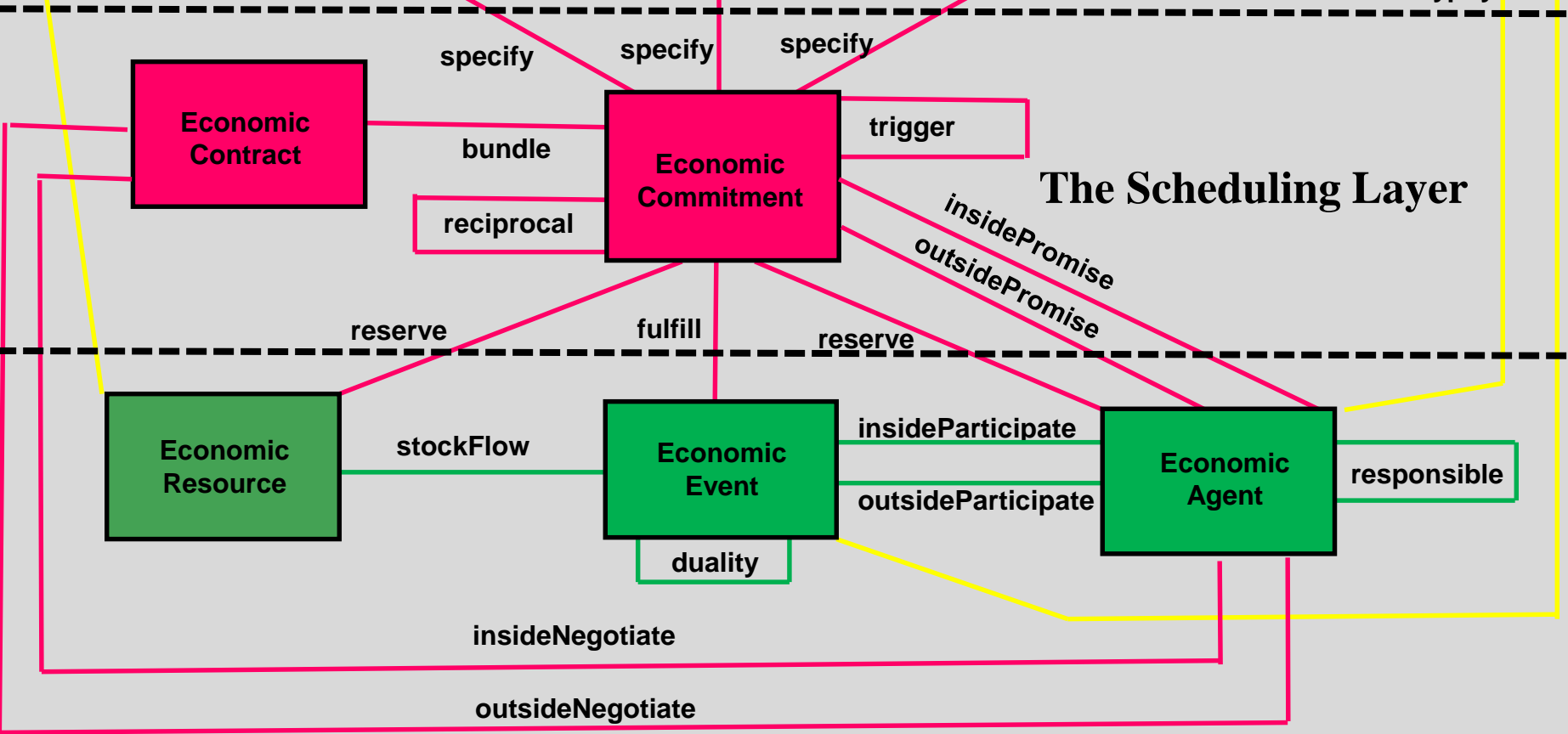
Figure 5-3

REA Modeling at the Value Network level -- Trading Partner View

The Policy Layer



The Scheduling Layer



The Accountability Layer

The REA Metamodel (Trading Partner View)

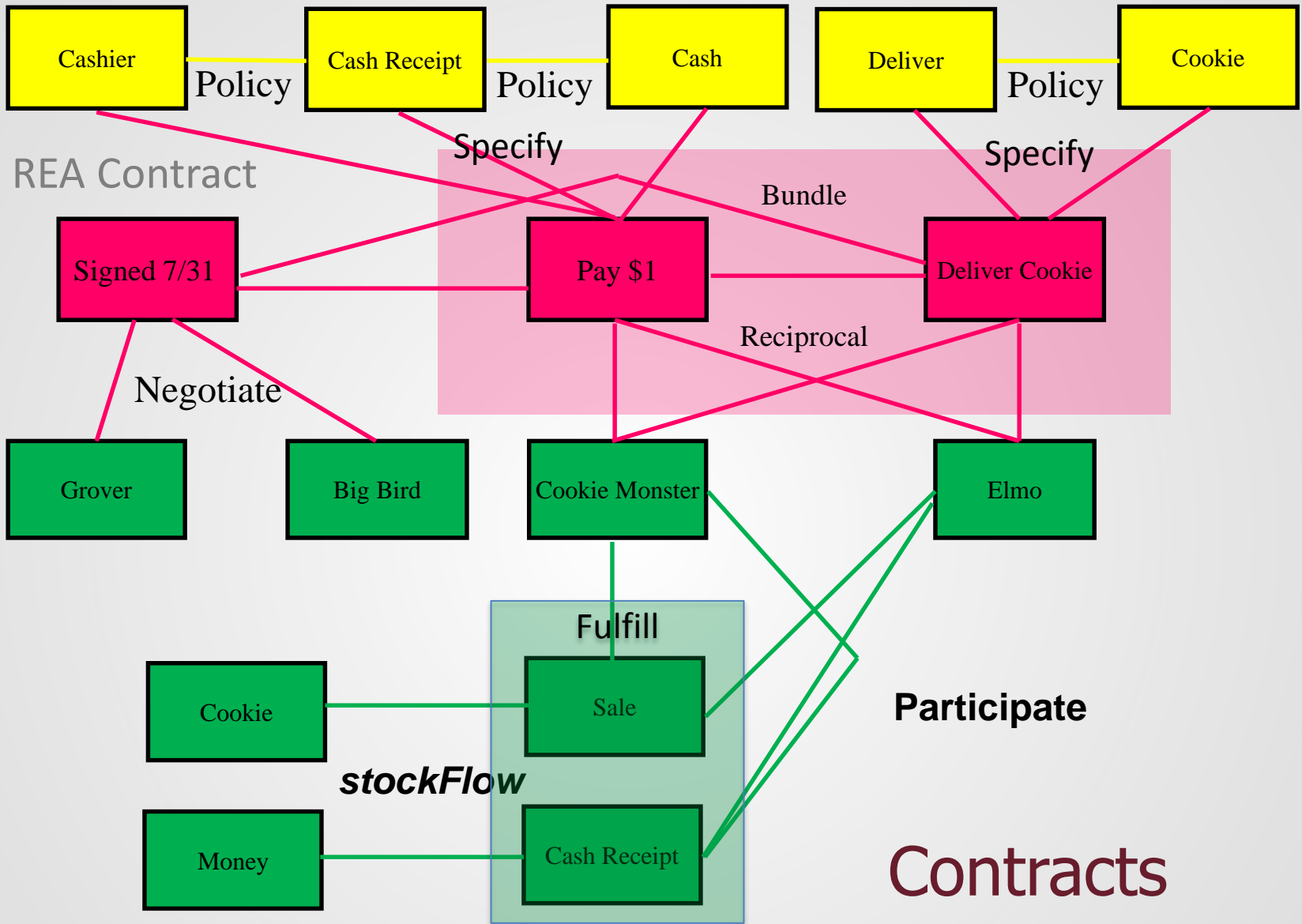
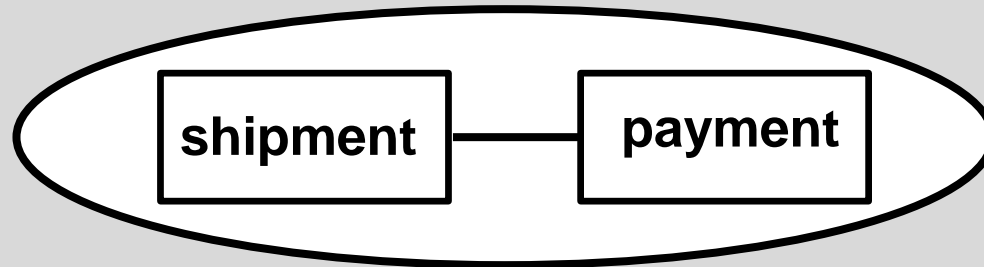


Figure 5-2

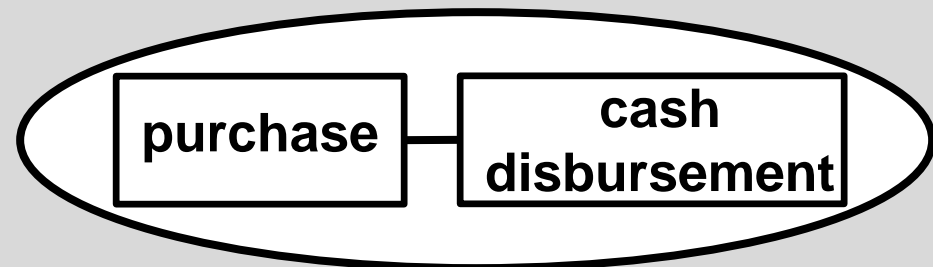
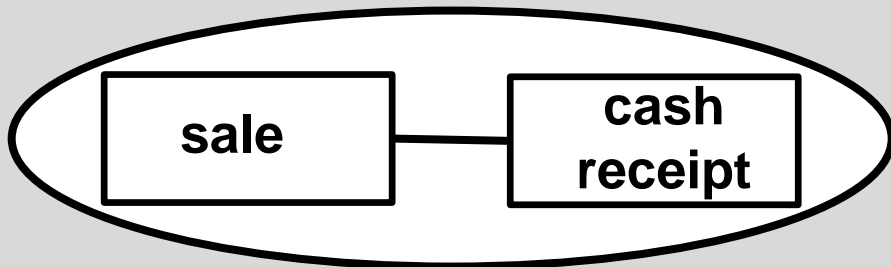


collaboration space viewed independently of the trading partners



value chain view (revenue process)
of the selling trading partner

value chain view (acquisition process)
of the buying trading partner



seller



buyer

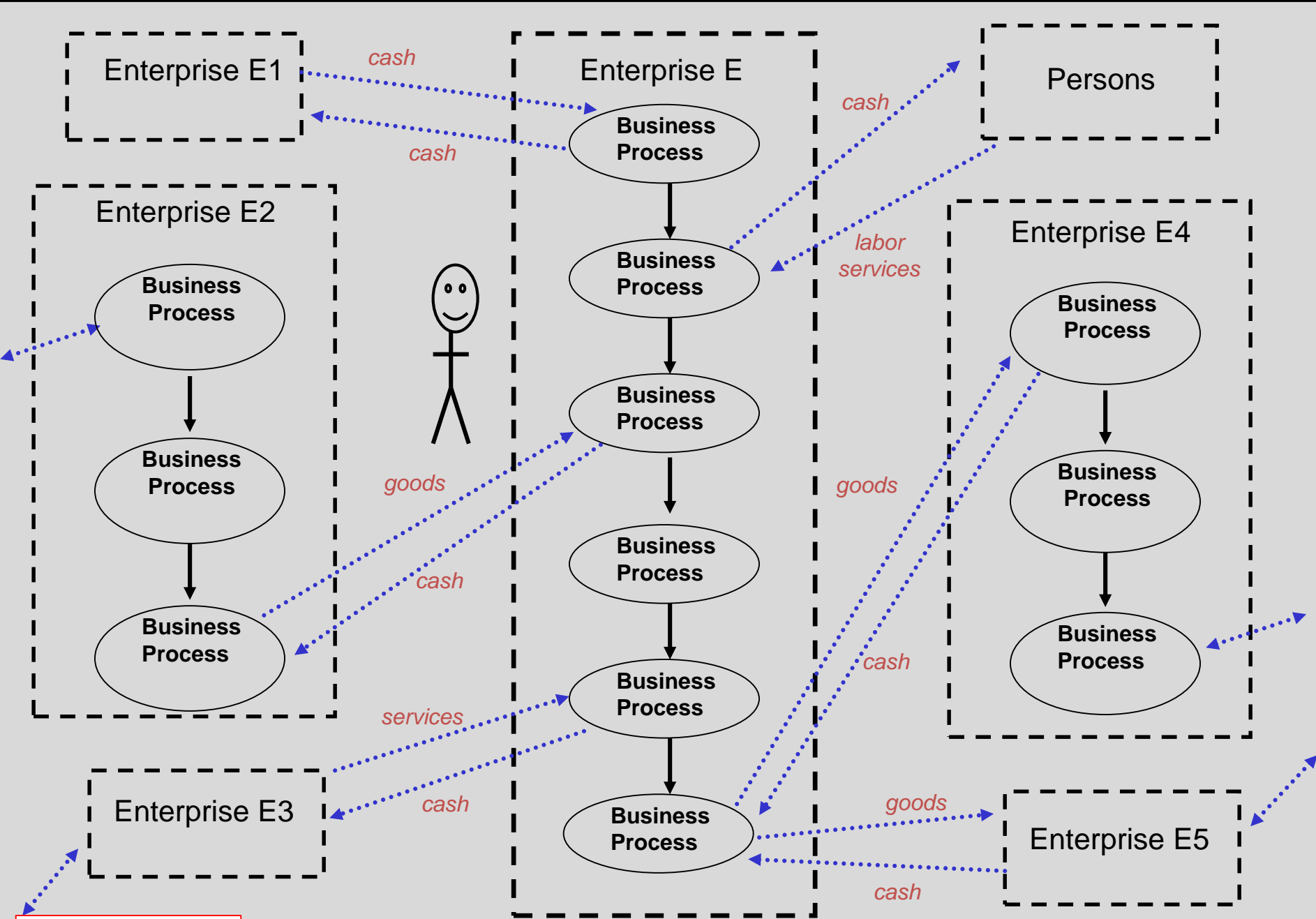
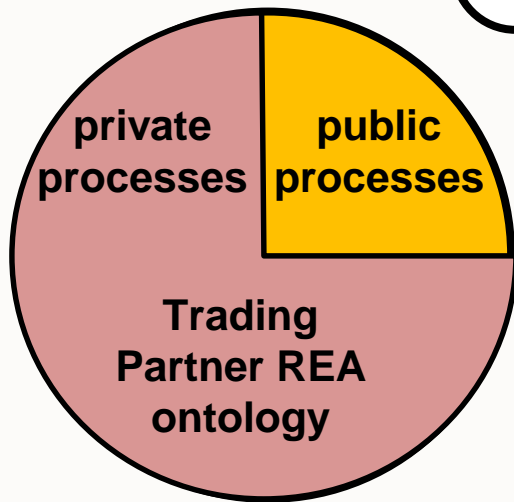


Figure 5-6

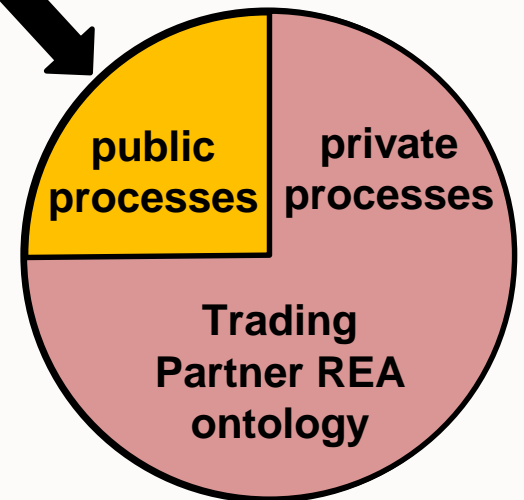
Modeling at the Value Network level -- Independent View

Distributed Business Transaction Repository

(Independent REA view of ontological categories
and their states in collaboration space)



firm-a



firm-b

Figure 5-9

A Value Chain (a script for creating value)

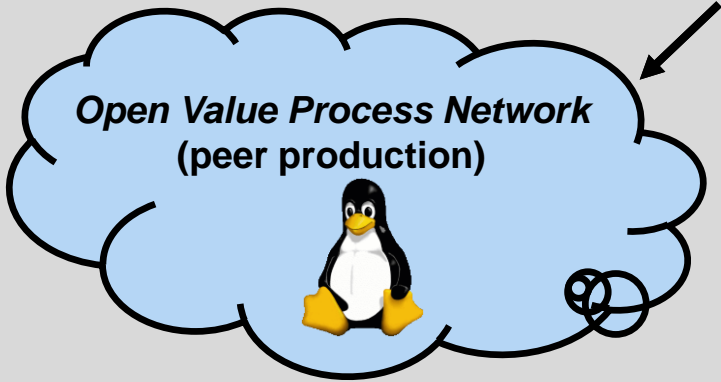
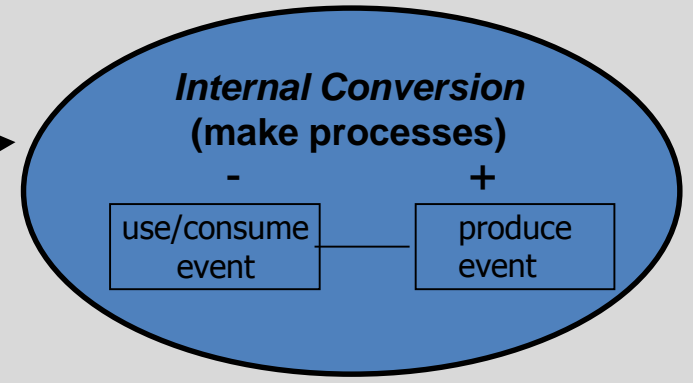
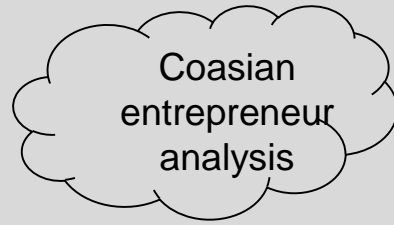
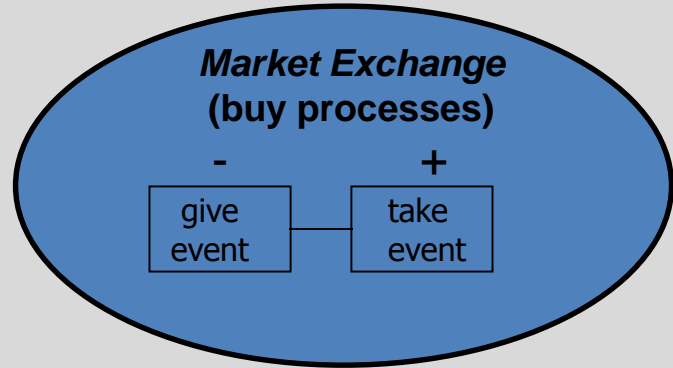
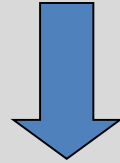
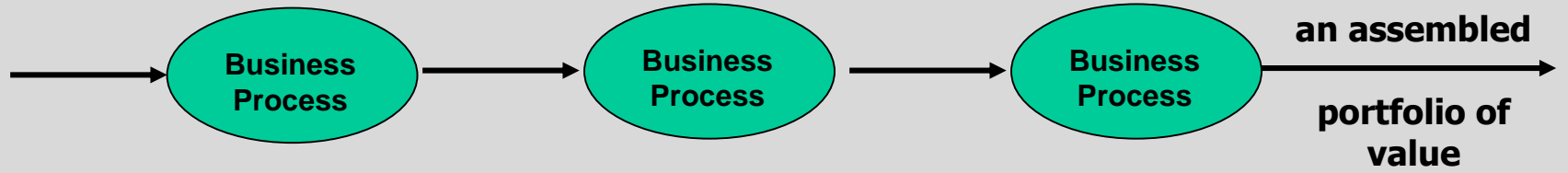
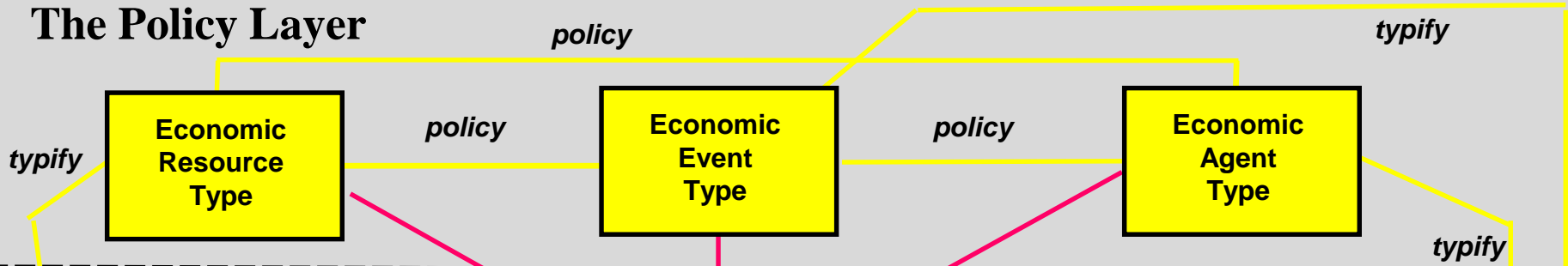
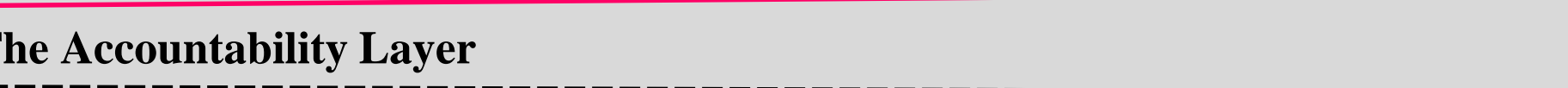
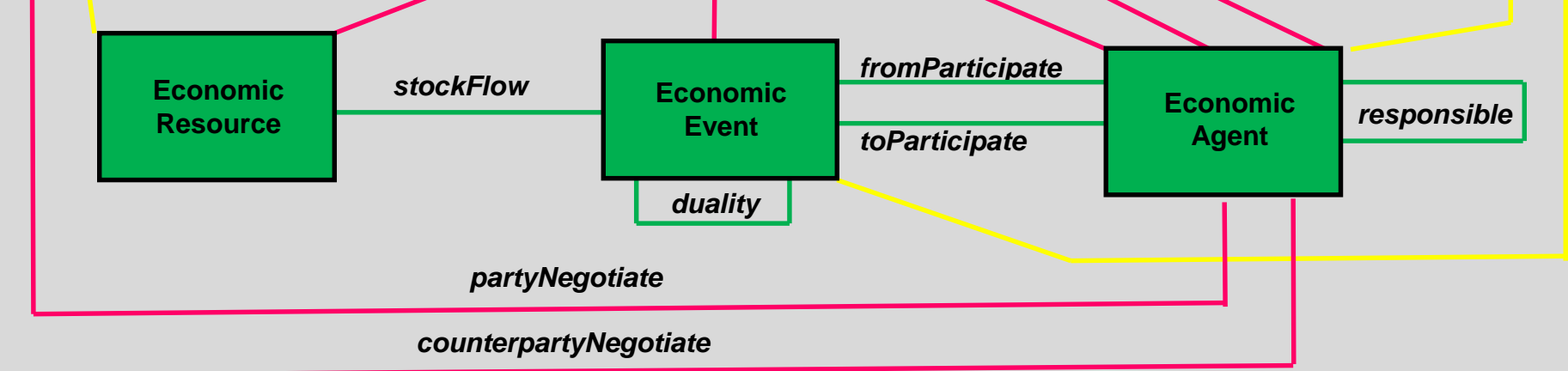
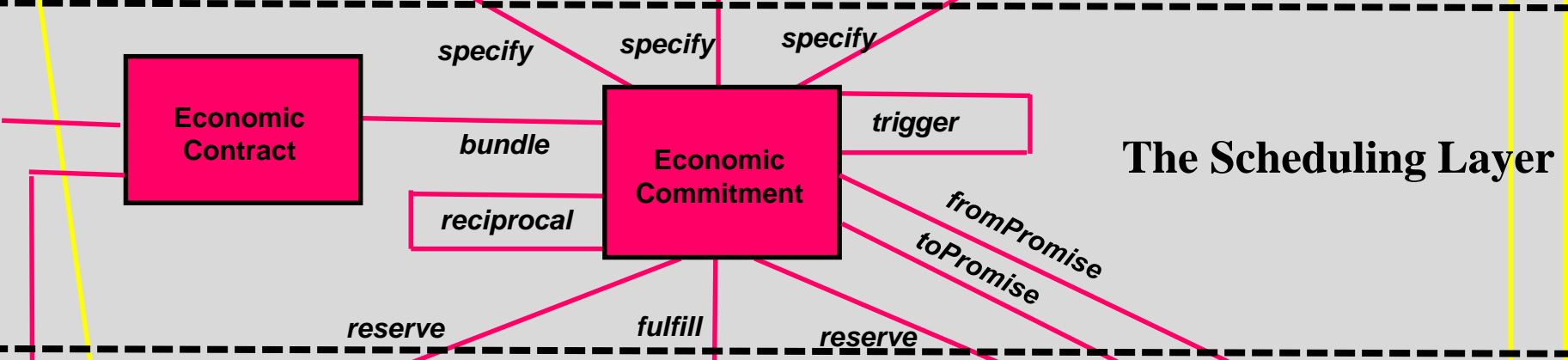


Figure 5-11

The Policy Layer



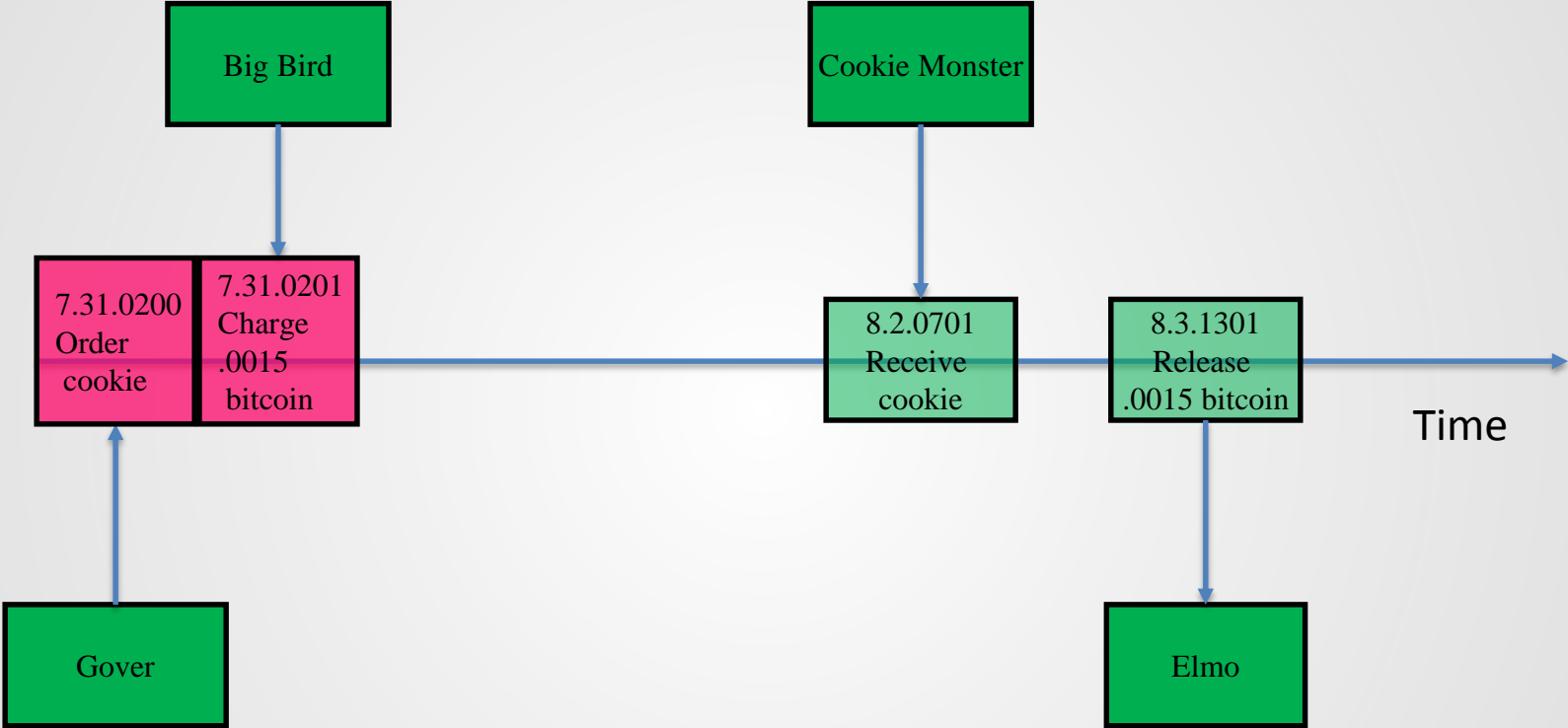
The Scheduling Layer



The Accountability Layer

Contracts

- Smart Contracts



Watching the Blockchain

- With Just Crypto Currencies on Blockchain
 - January 30, 2017 transaction for 1.25 bitcoin between party A and party B
- Adding Other resources
 - January 30, 2017 transaction for 1.25 bitcoin between party A and party B
 - January 31, 2017 transaction for token #32324afe342223
- Questions
 - Was this a contract between A and B?
 - Was #32324afe342223 delivered?
 - Did B have the right to deliver resource #32324afe342223?
 - What is resource #32324afe342223?

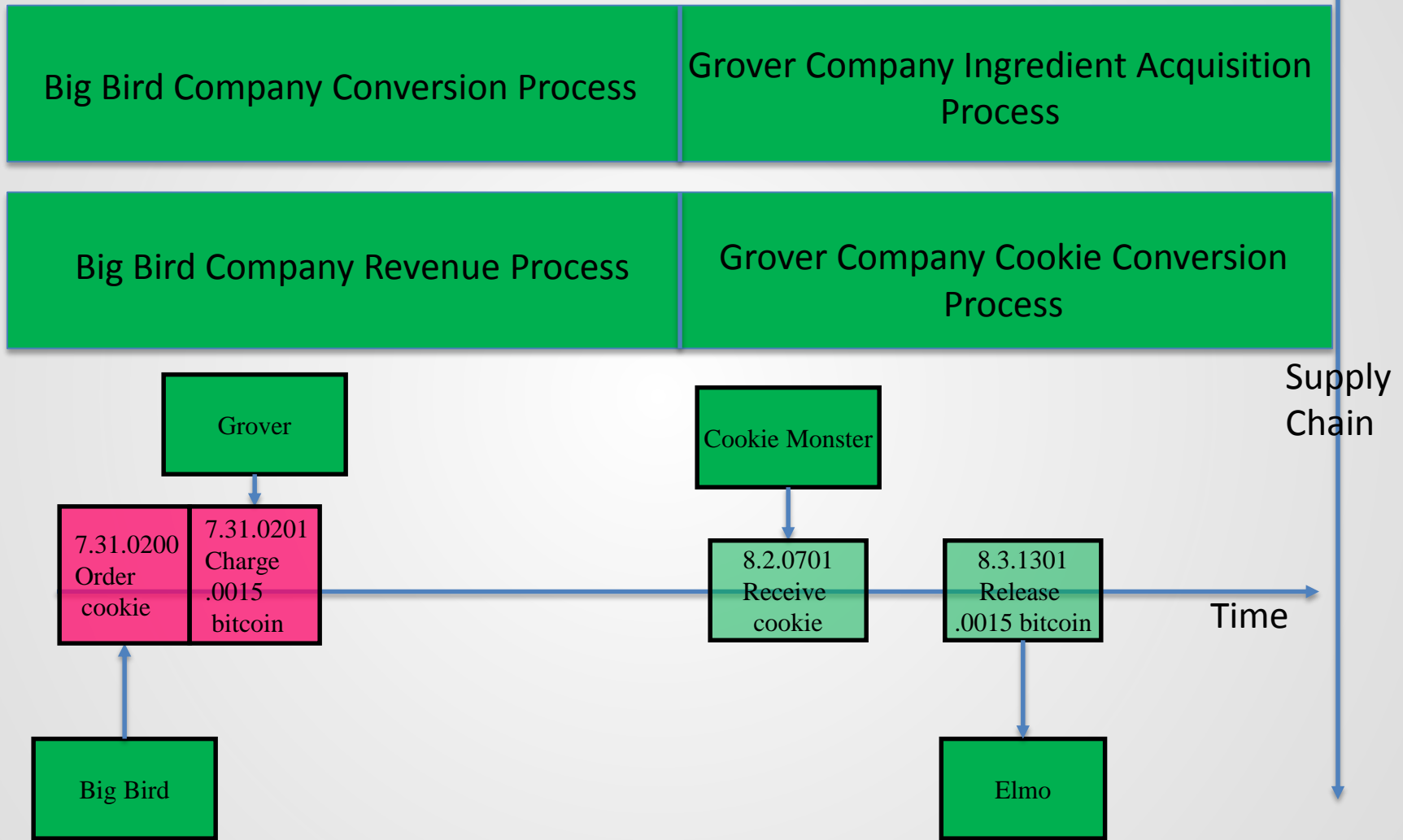
Facilitating Contracting on the Blockchain

- Contract added to the blockchain
 - Contract ID #2afe3280 added to blockchain on February 20, 2017
 - Includes
 - commitment #11afde by Agent #12afbae334 to deliver 3000 gallons of gasoline(trigger)
 - commitment #212321 by Agent #fec54aff27 to deliver 54,000 USD (reciprocal)
 - Economic events added to blockchain
 - Event #121ededff by Agent #12afbae334 resource #ec23ff49af quantity 3000 in fulfillment of commitment #11afde on 2017-03-04
 - Event #93efcb34 by Agent #fec54aff27 resource #23223de quantity 54,000 in fulfillment of commitment #212321 on 2017-03-04

Duality

Contracts

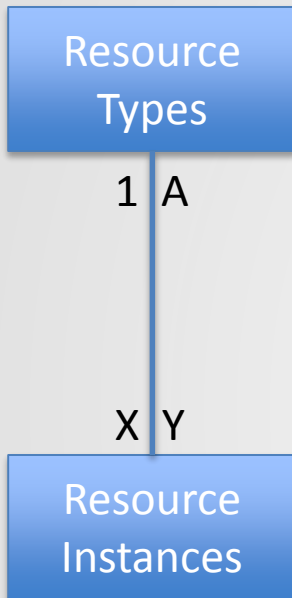
REA Contracts up the Supply Chain



Tokenization

- Need Universal IDs
 - What should be in an ID
- Need Universal Assurance
 - What can we assure
- What Should Not be Revealed
 - Supply Chain might reveal process inputs

Tokenization of Resources



Function Calls:

Token_Type(_token) would return its type

Token_units(Token_type_quantity(_token) return units
(gallons, barrels)

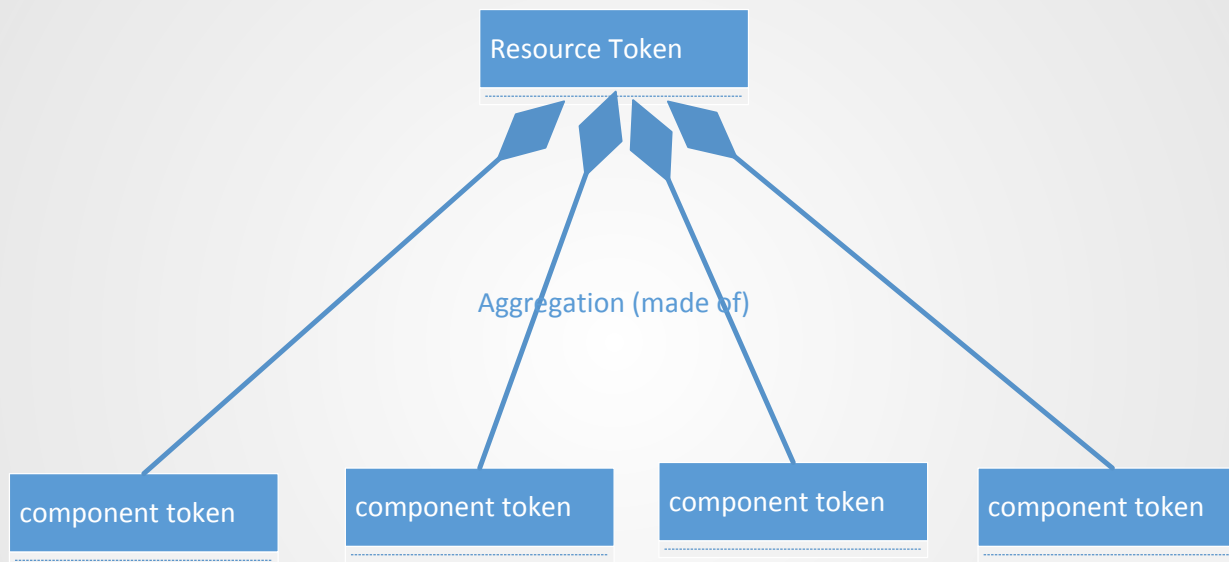
Token_Quantity(_token) would call Token_type_quan and
return 3000 gallons

And

Token_name(_token) could return fuel.gasoline

Tokenization of Resources with Components

Supply Chain Information



Who made the engine in car with vin #...?

What paint was used on car with vin # ?

And even, where did the aluminum that was used in car with vin # come from?

Tokenization of Agents

Agent Types

- Person as an aggregation of digital identities
 - Medical
 - Financial
 - Academic
 - Social
 -
- Companies as an aggregation digital identities and as an aggregation of persons with digital identities
- Rather than a single uPort key the registry keeps a hash of all identities so `Information_return (medkey, uPort)` returns the medical information but does not provide access to financial
- `Information_return(BP,uPort)` could return information on the company such that `Information_return((Token_name(_component)),uPort)` could return information on the company that made the engine for a particular car

Juels, A. (2016). Reassembling Our Digital Selves. *Daedalus*, 145(1), 45-53.

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. (2016). *U-PORT: A Platform for Self-Sovereign Identity (Draft Version 2016-10-20)*. NY: Consensys.

References

- “Query Issues in Continuous Reporting Environment,” *Journal of Emerging Technologies*, 2008.
- The REA Ontology, AAA Monograph forthcoming.