Manifestly Phased Communication via Shared Session Types

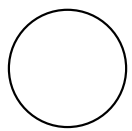
Chuta Sano

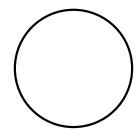
McGill University

October 28, 2024

joint work with Stephanie Balzer and Frank Pfenning

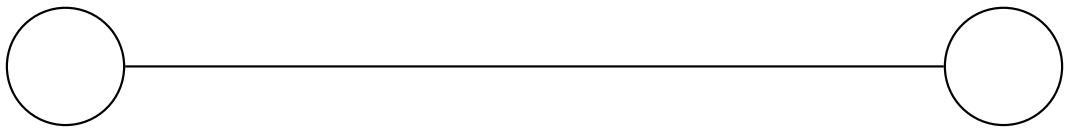
Linear Session Types[1]





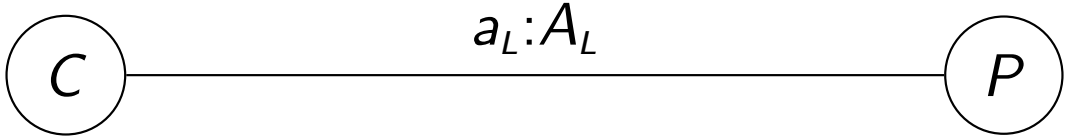
[1] Honda 1993; Caires and Pfenning 2010; Wadler 2012.

Linear Session Types[1]



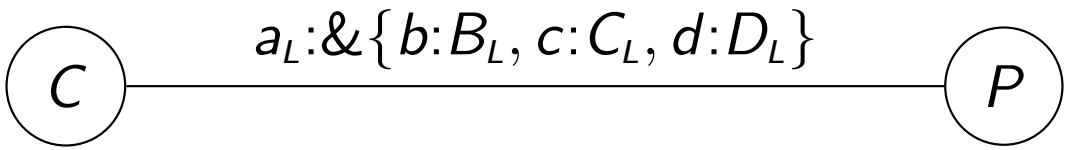
[1] Honda 1993; Caires and Pfenning 2010; Wadler 2012.

Linear Session Types[1]



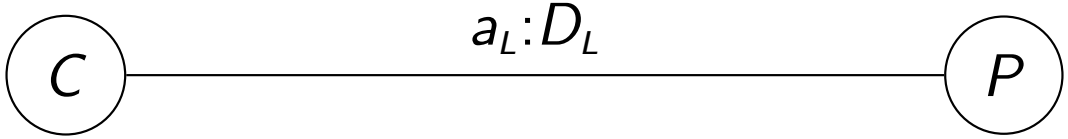
[1] Honda 1993; Caires and Pfenning 2010; Wadler 2012.

Linear Session Types[1]



[1] Honda 1993; Caires and Pfenning 2010; Wadler 2012.

Linear Session Types[1]

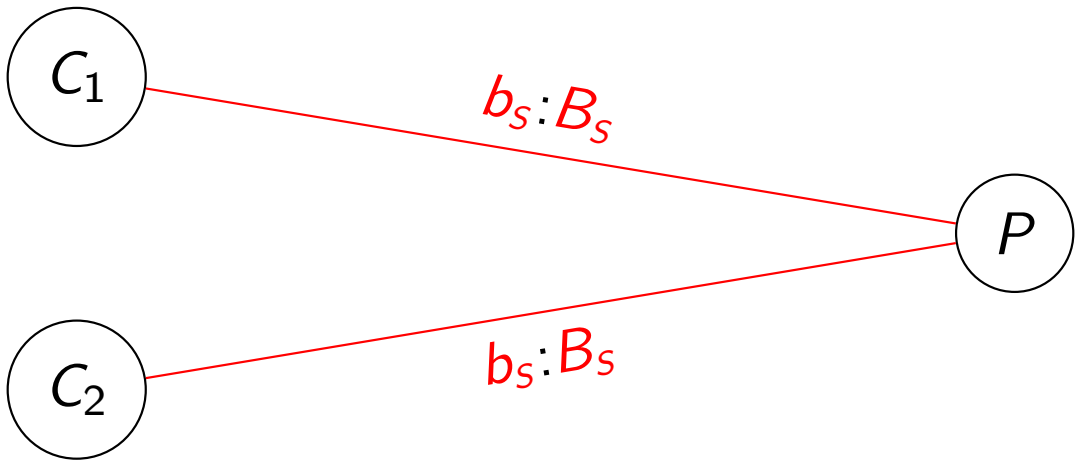


[1] Honda 1993; Caires and Pfenning 2010; Wadler 2012.

Shared Session Types[2]

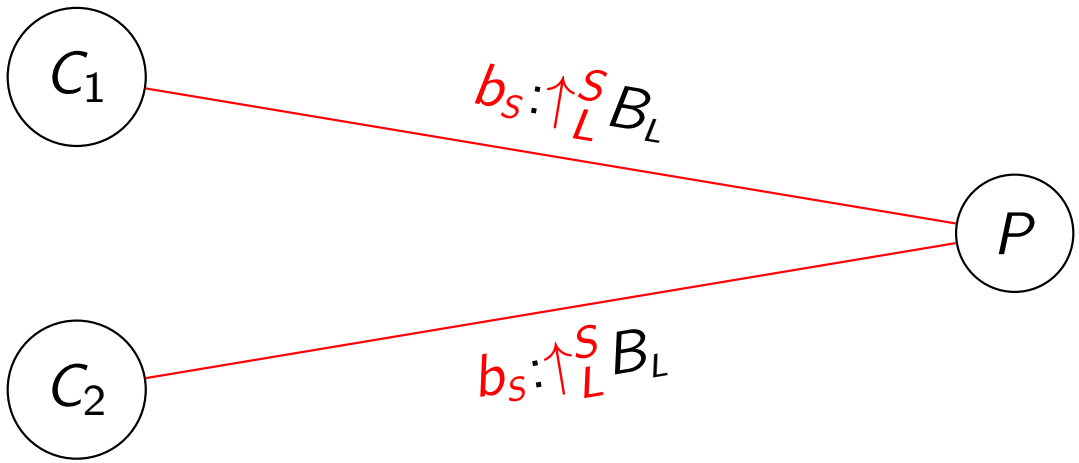
[2] Balzer and Pfenning 2017.

Shared Session Types[2]



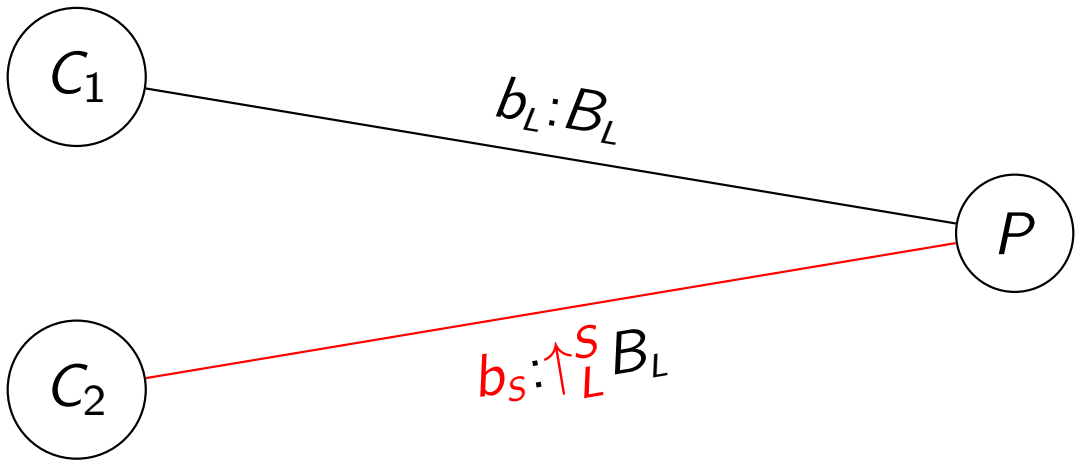
[2] Balzer and Pfenning 2017.

Shared Session Types[2]



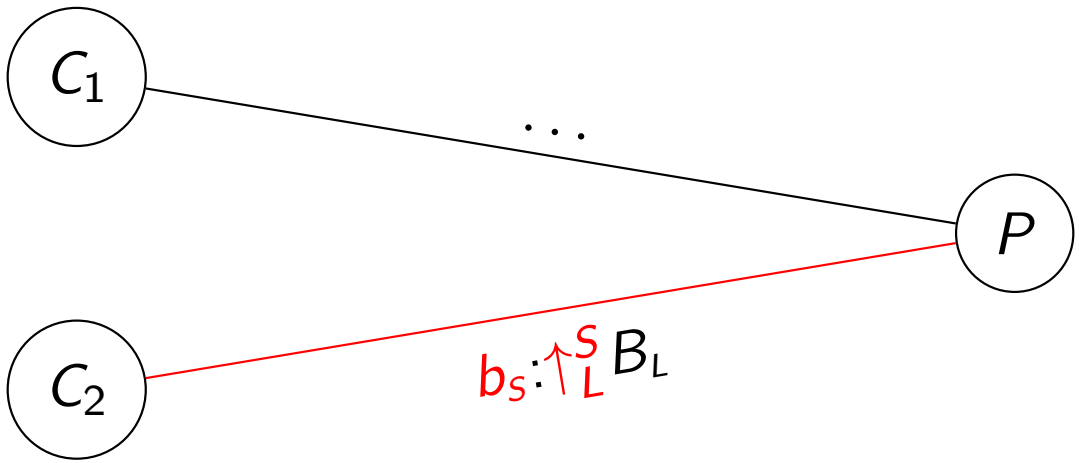
[2] Balzer and Pfenning 2017.

Shared Session Types[2]



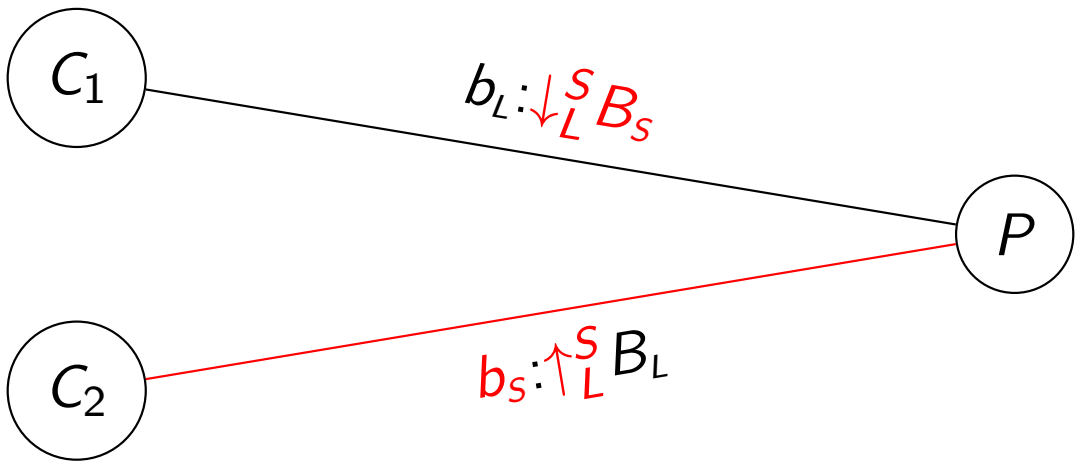
[2] Balzer and Pfenning 2017.

Shared Session Types[2]



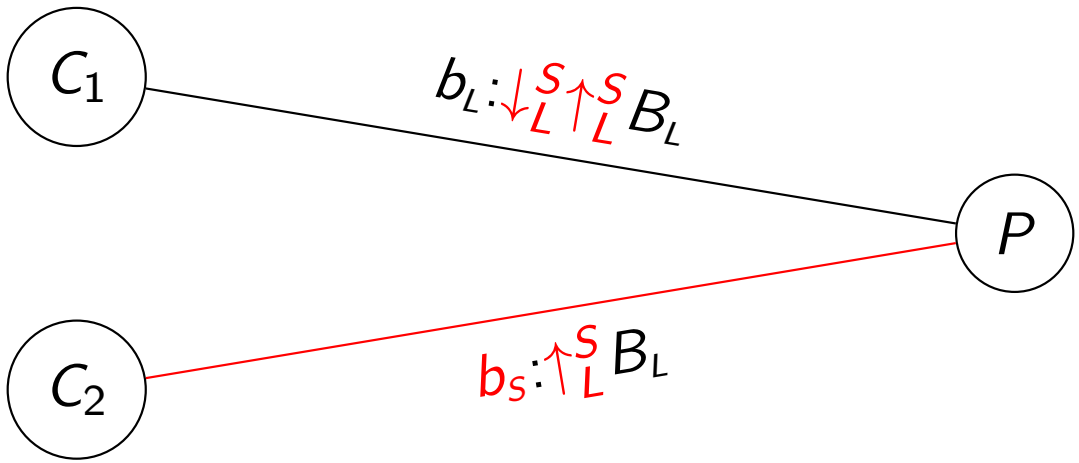
[2] Balzer and Pfenning 2017.

Shared Session Types[2]



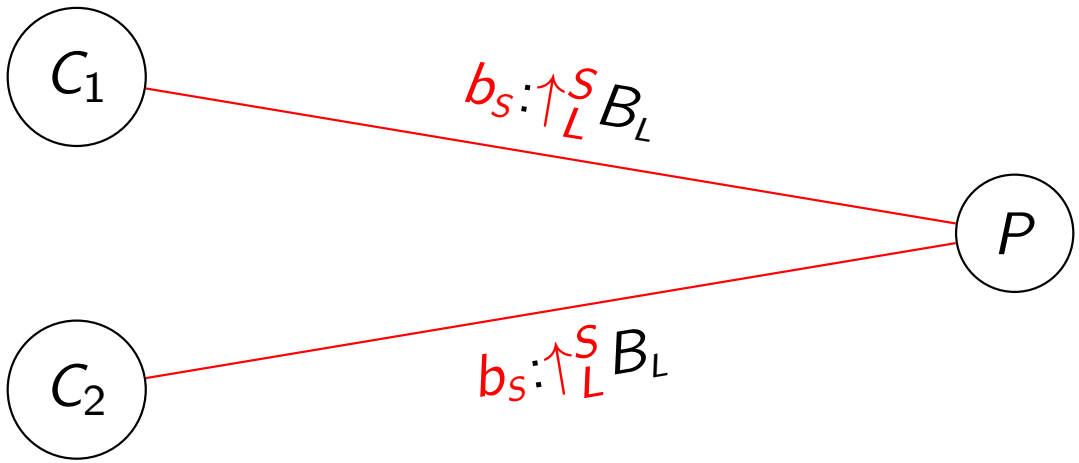
[2] Balzer and Pfenning 2017.

Shared Session Types[2]



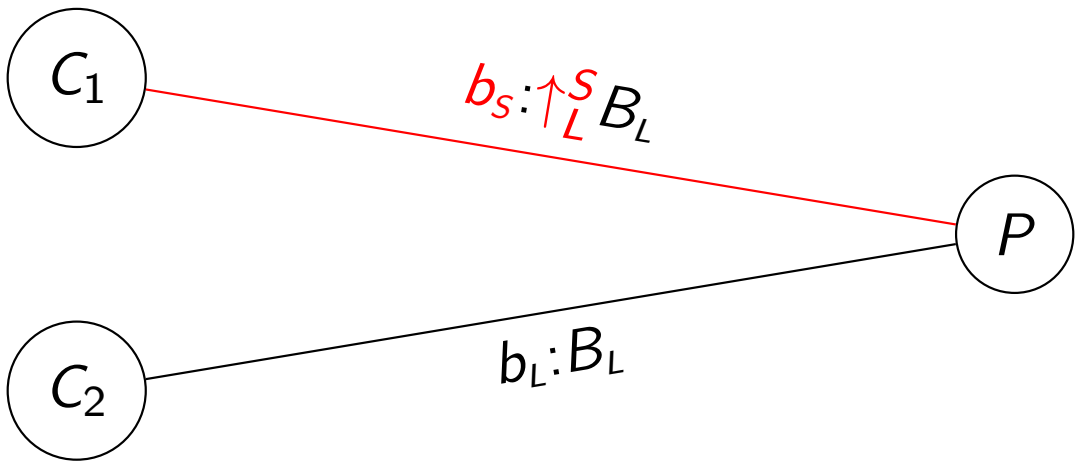
[2] Balzer and Pfenning 2017.

Shared Session Types[2]

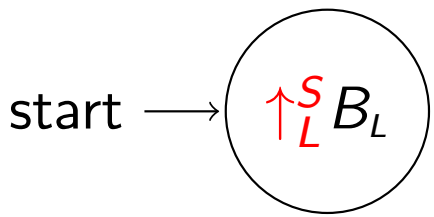


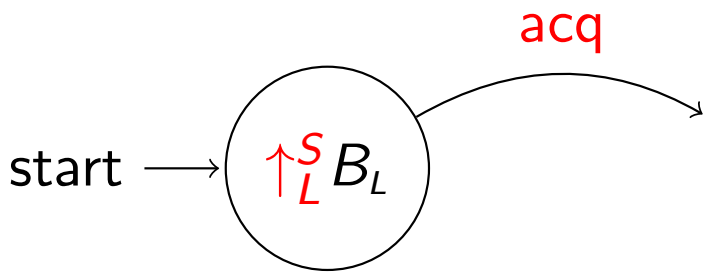
[2] Balzer and Pfenning 2017.

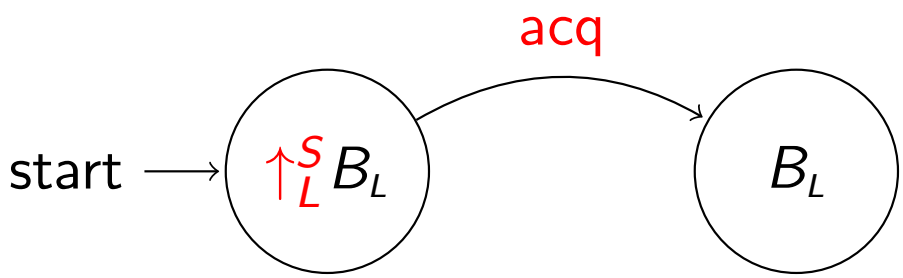
Shared Session Types[2]

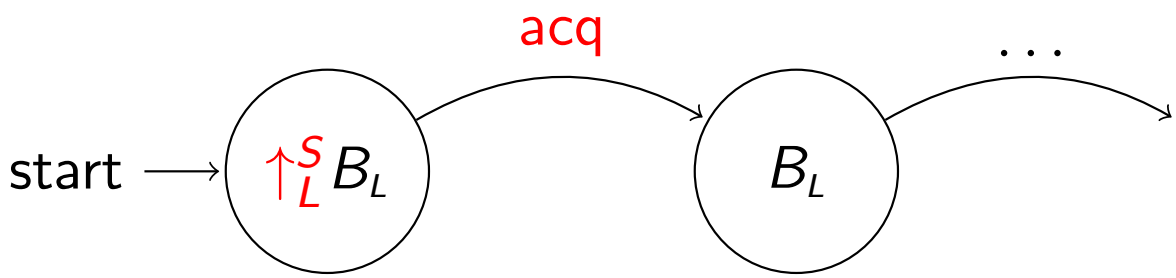


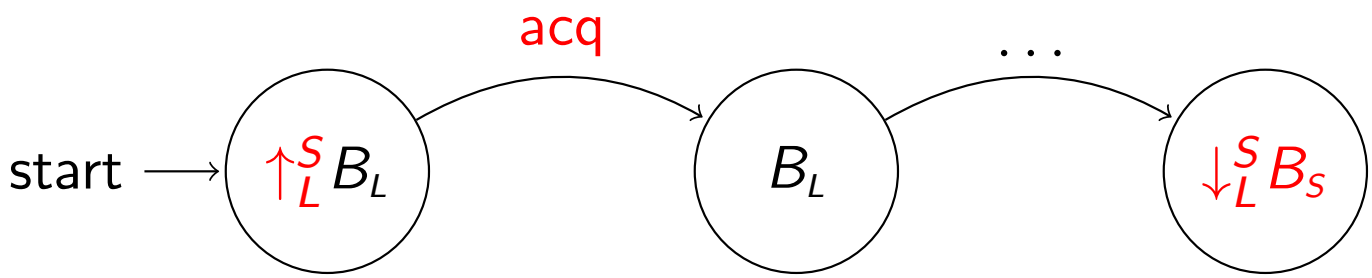
[2] Balzer and Pfenning 2017.

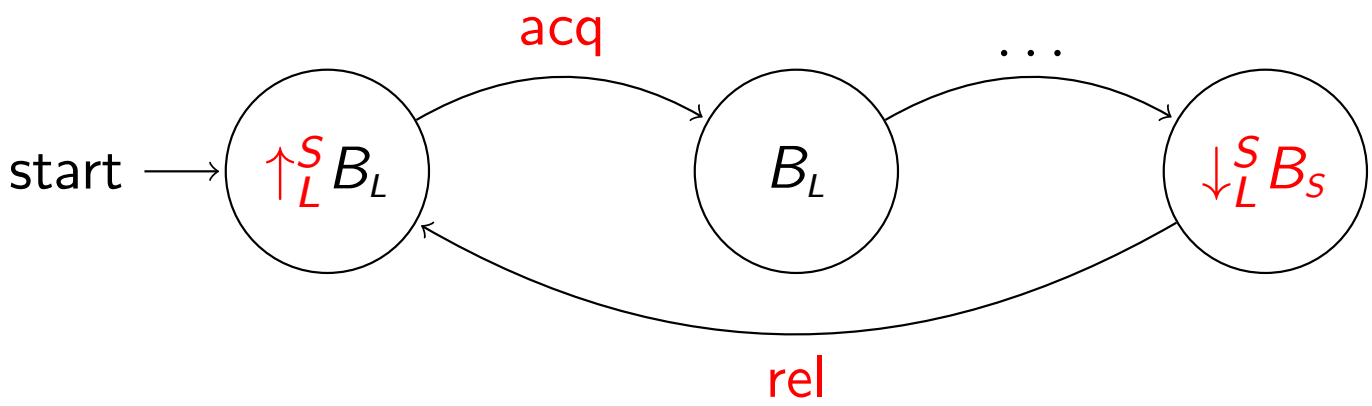

start
$\uparrow_L^S B_L$

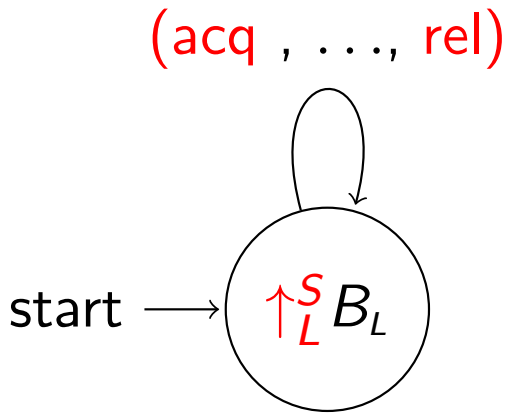

acq
start
$\uparrow_L^S B_L$

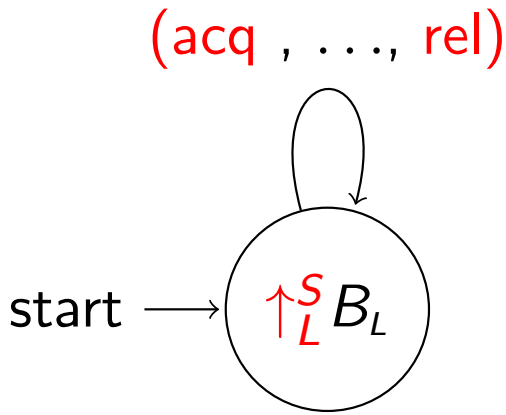

acq
start
$\uparrow_L^S B_L$
B_L


start
$\uparrow_L^S B_L$
acq
B_L
...


start
$\uparrow_L^S B_L$
acq
B_L
...
$\downarrow_L^S B_S$


start
$\uparrow_L^S B_L$
acq
B_L
...
$\downarrow_L^S B_S$
rel


(acq , . . ., rel)
start
$\uparrow_L^S B_L$



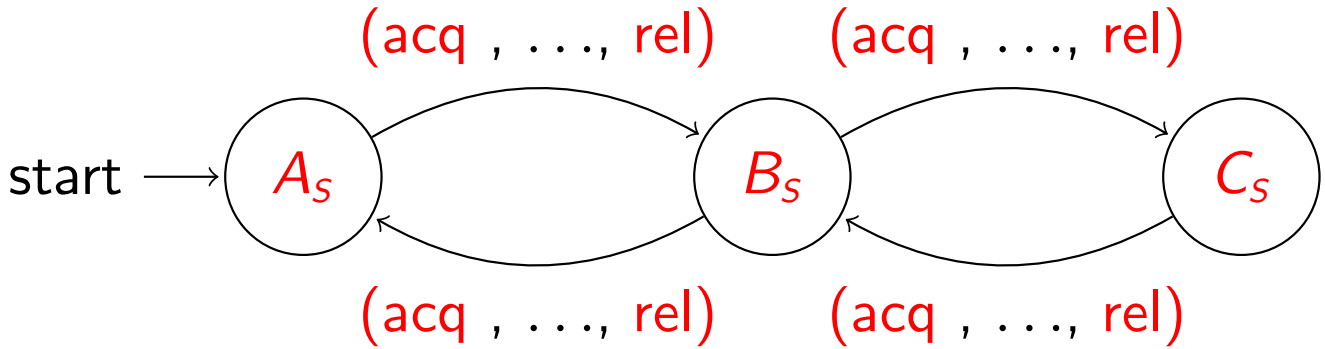
Equi-synchronizing types

Releasing is Too Restrictive

- Session type is “reset”
- Cannot encode *phases*

Releasing is Too Restrictive

- Session type is "reset"
- Cannot encode *phases*

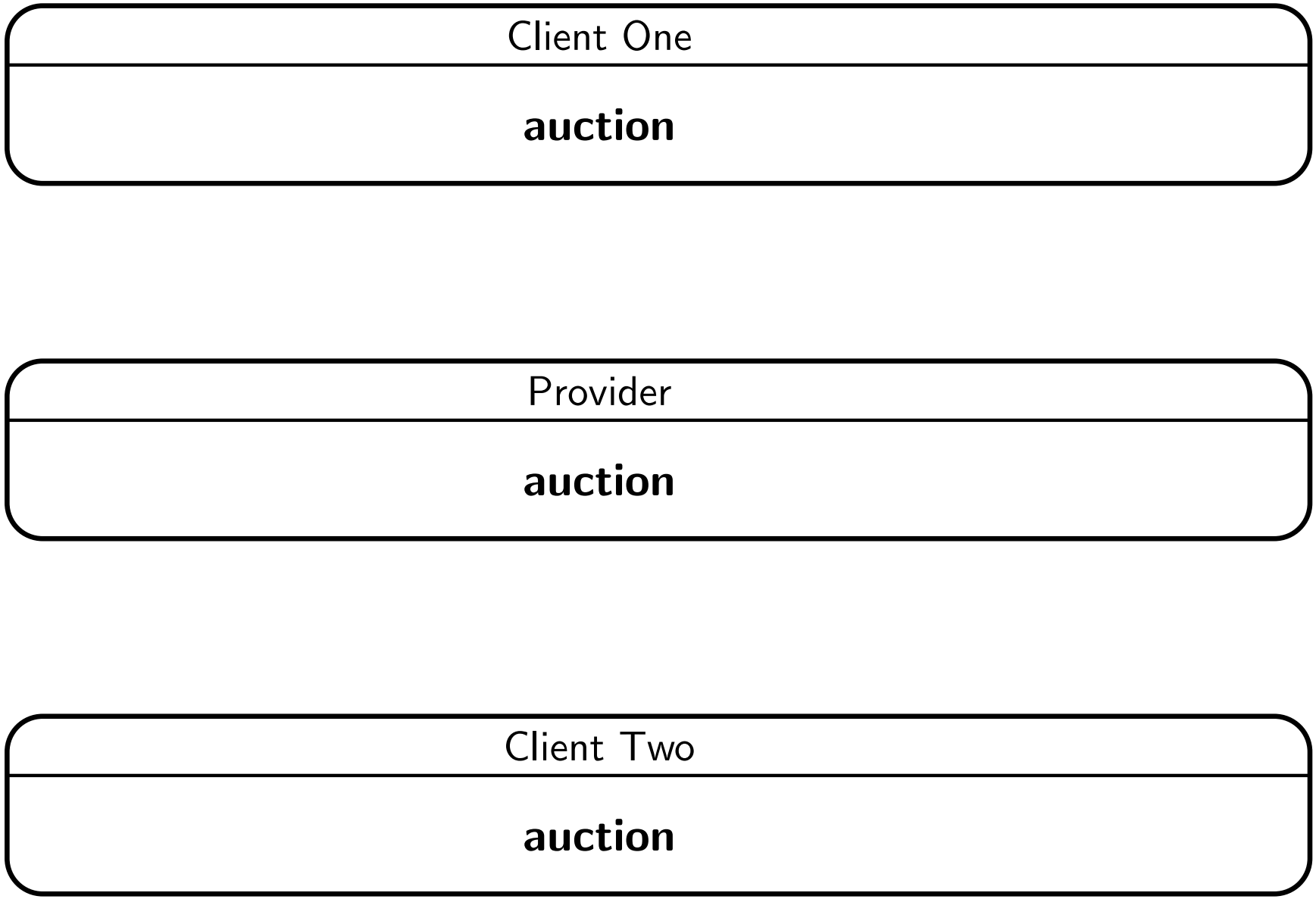


How can we safely represent *phases*?

How can we safely represent *phases*?

Auction

$$\begin{aligned}\textbf{auction} = \uparrow^{S}_{L} \& \{ & \mathit{bid} : \oplus\{\mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow^{S}_{L} \textbf{auction}, \\ & \mathit{collecting} : \downarrow^{S}_{L} \textbf{auction}\}, \\ & \mathit{collect} : \mathsf{id} \supset \oplus\{\mathit{prize} : \mathsf{item} \wedge \downarrow^{S}_{L} \textbf{auction}, \\ & \qquad \mathit{refund} : \mathsf{money} \wedge \downarrow^{S}_{L} \textbf{auction}, \\ & \qquad \mathit{bidding} : \downarrow^{S}_{L} \textbf{auction}\}\}\end{aligned}$$


Client One
auction
Provider
auction
Client Two
auction

Client One

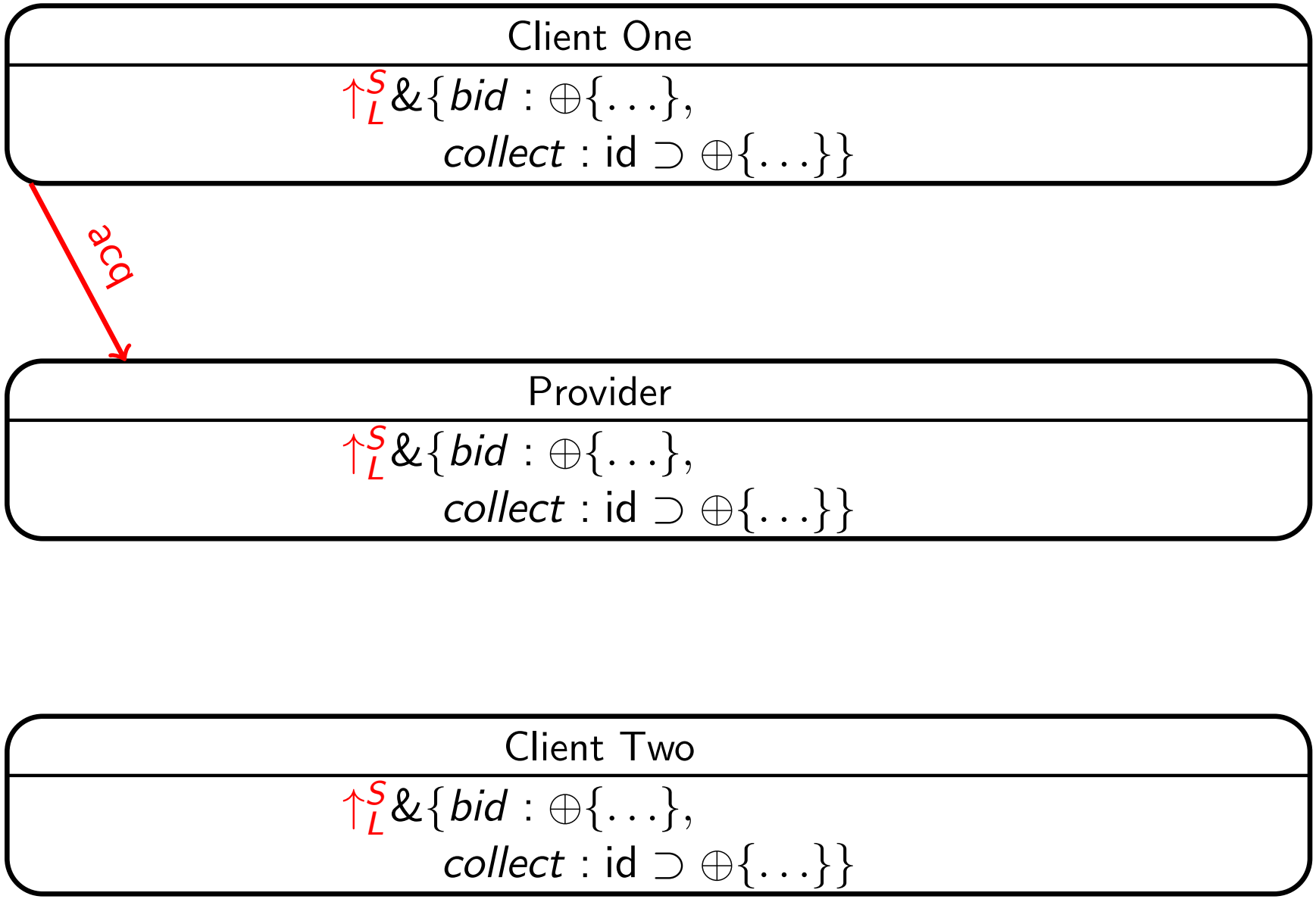
$$\uparrow_L^S \&\{bid : \oplus\{\ldots\},\ collect : \mathrm{id} \supset \oplus\{\ldots\}\}$$

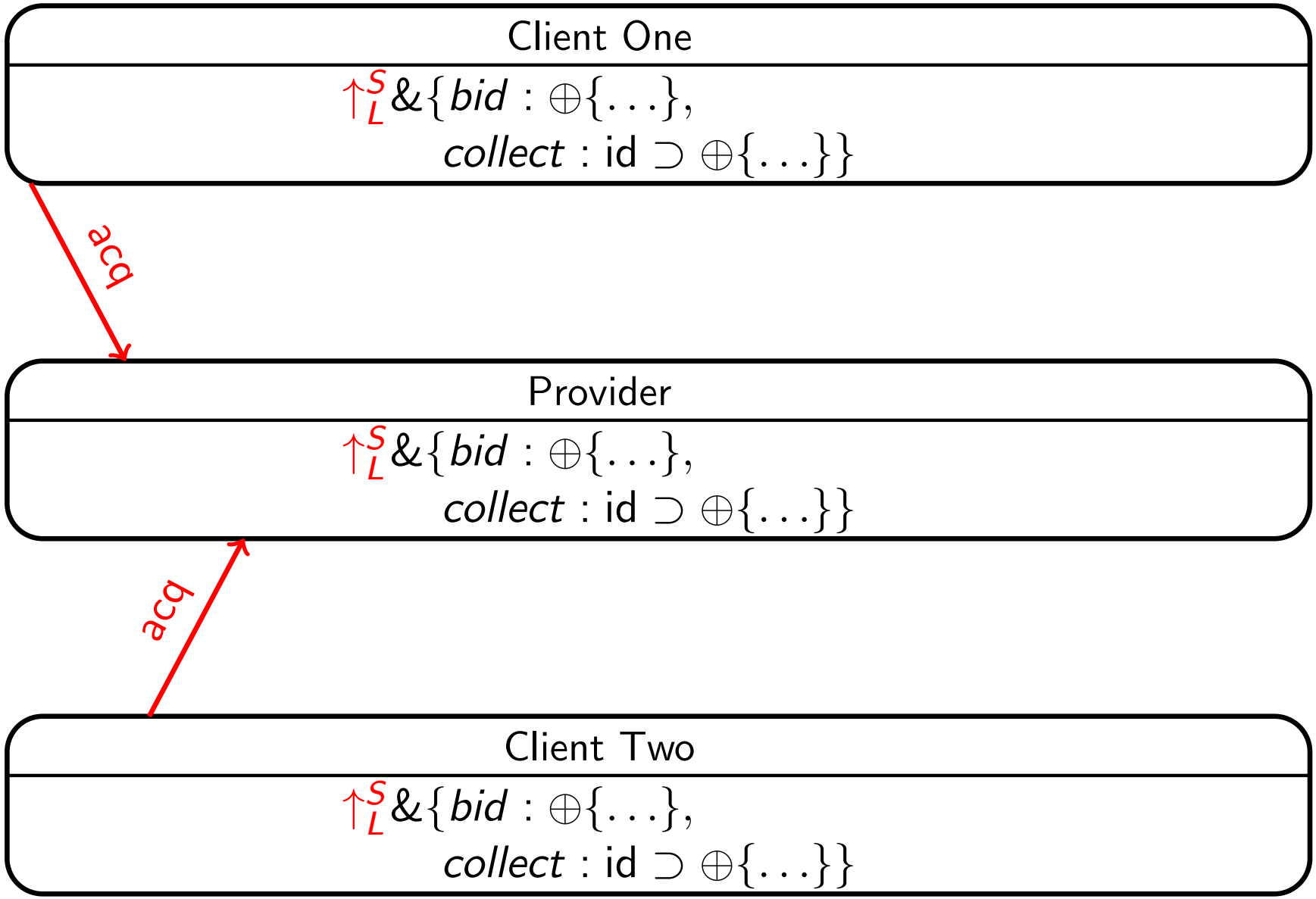
Provider

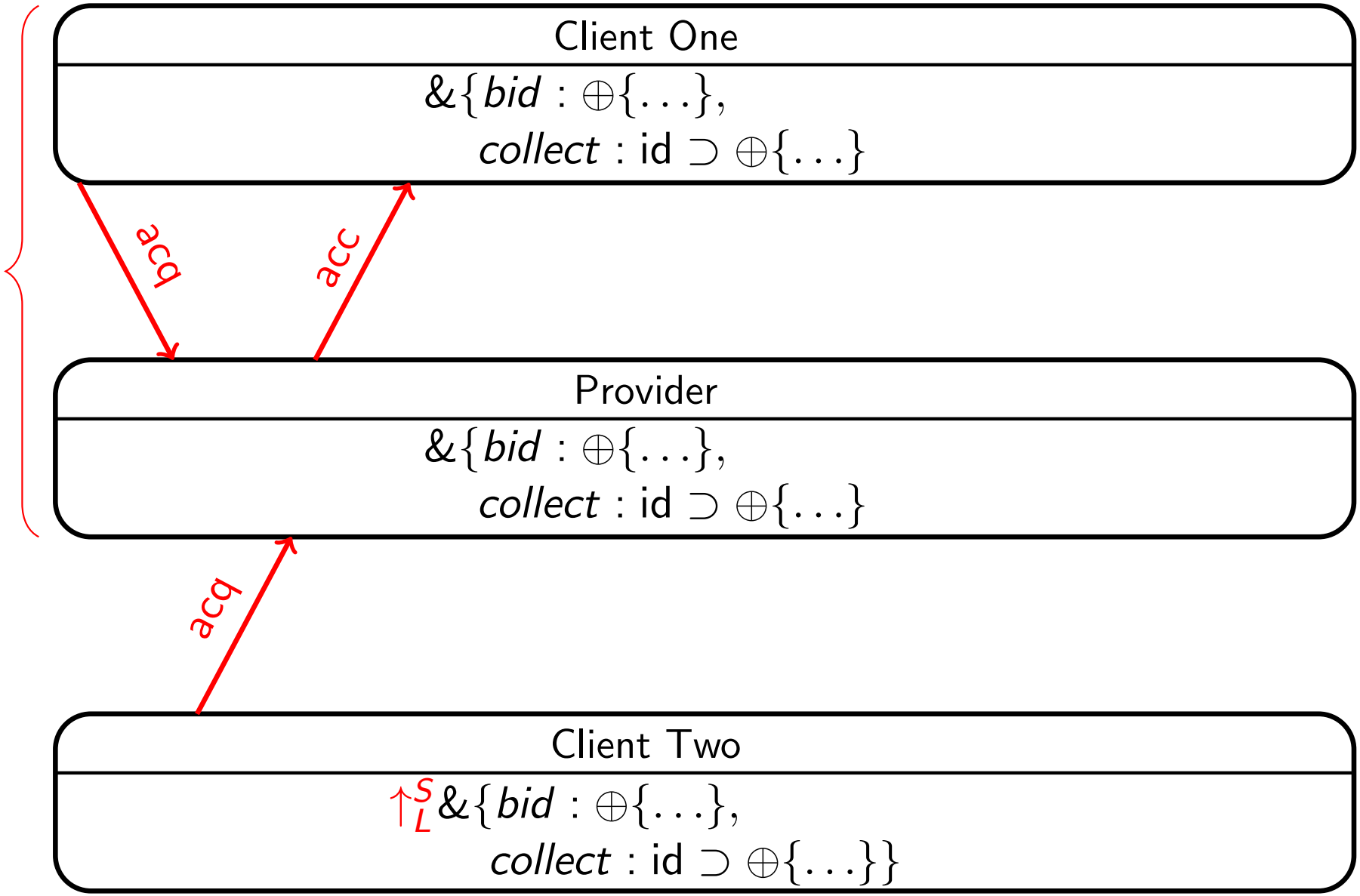
$$\uparrow_L^S \&\{bid : \oplus\{\ldots\},\ collect : \mathrm{id} \supset \oplus\{\ldots\}\}$$

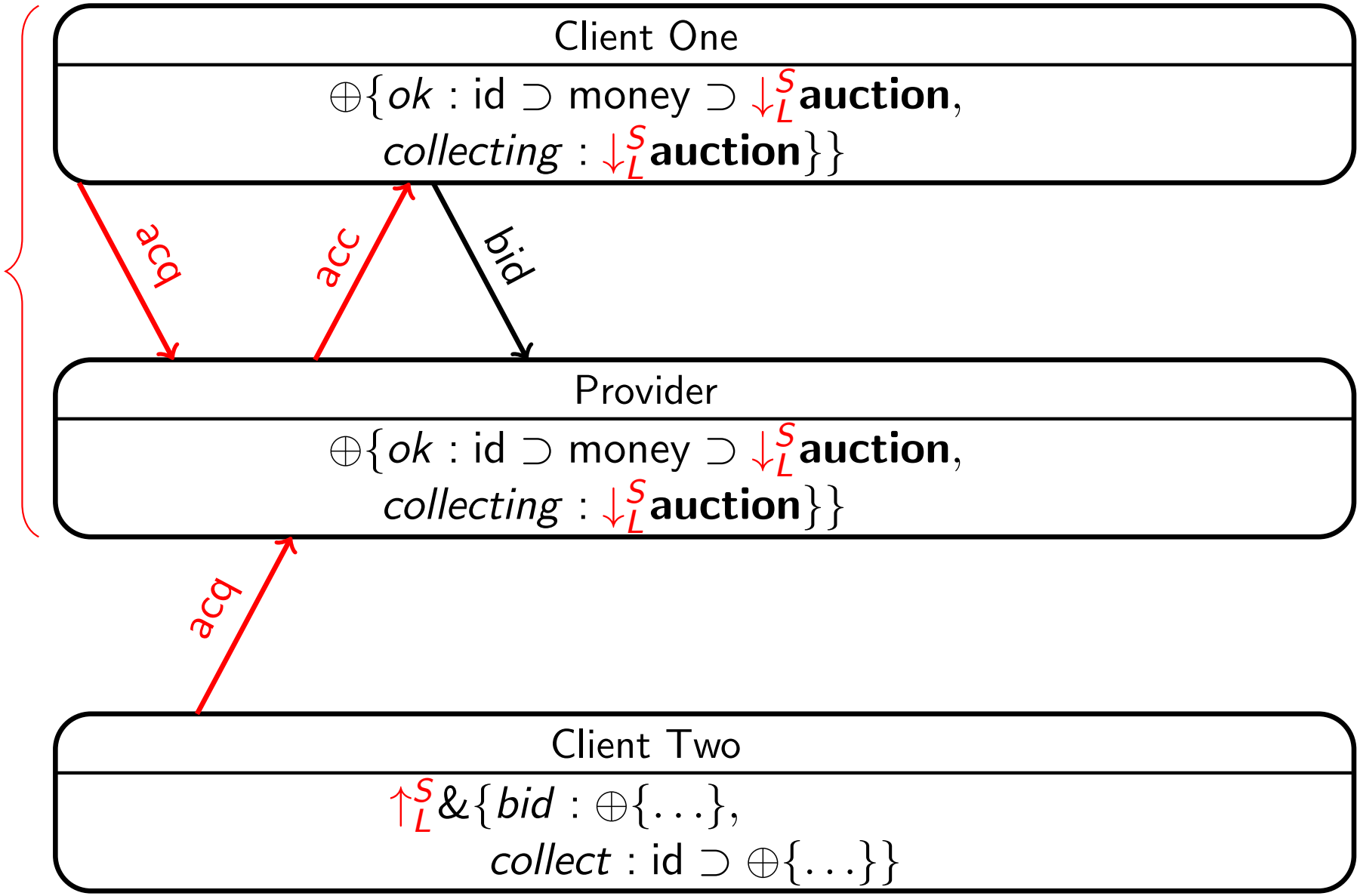
Client Two

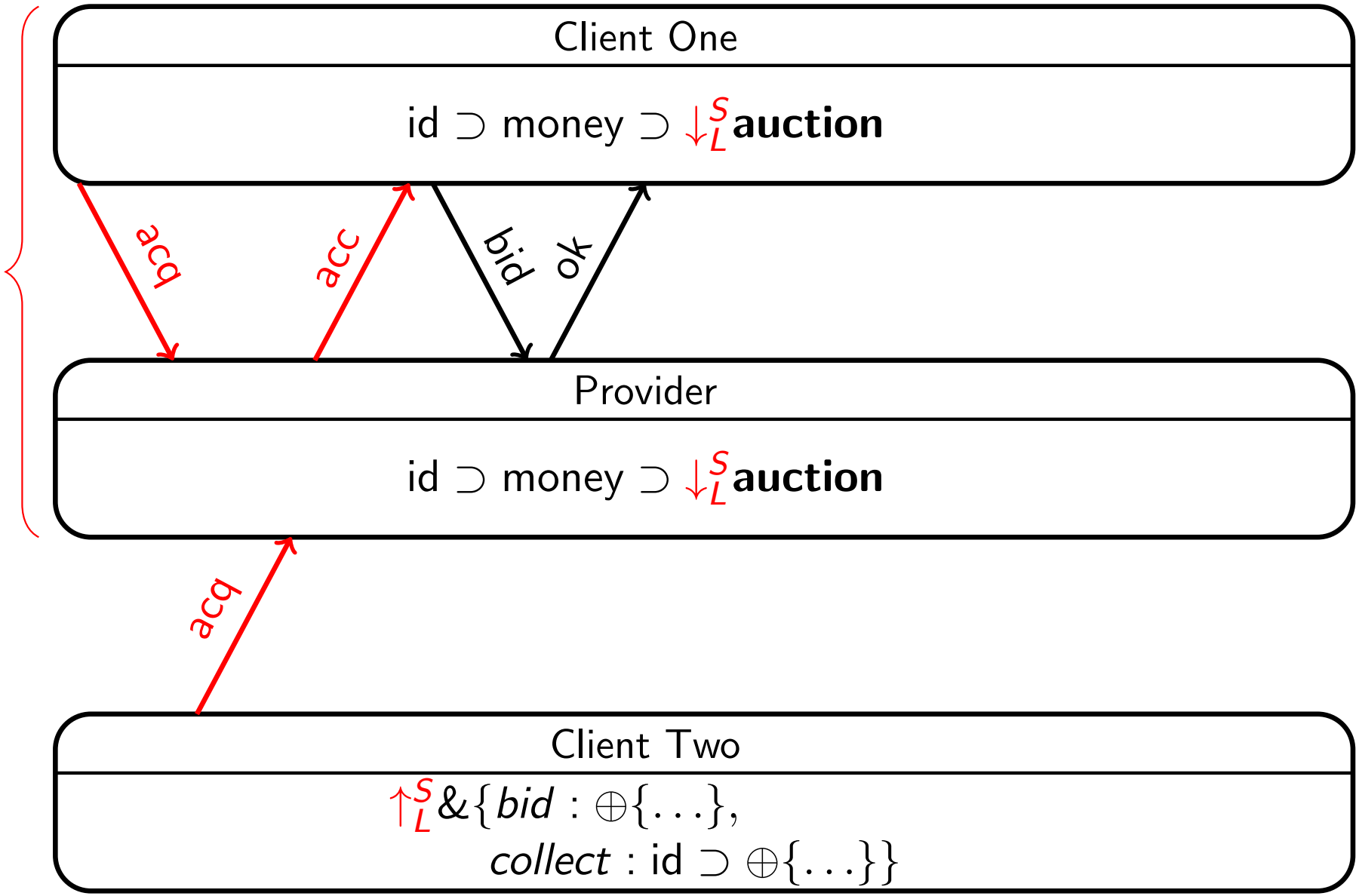
$$\uparrow_L^S \&\{bid : \oplus\{\ldots\},\ collect : \mathrm{id} \supset \oplus\{\ldots\}\}$$

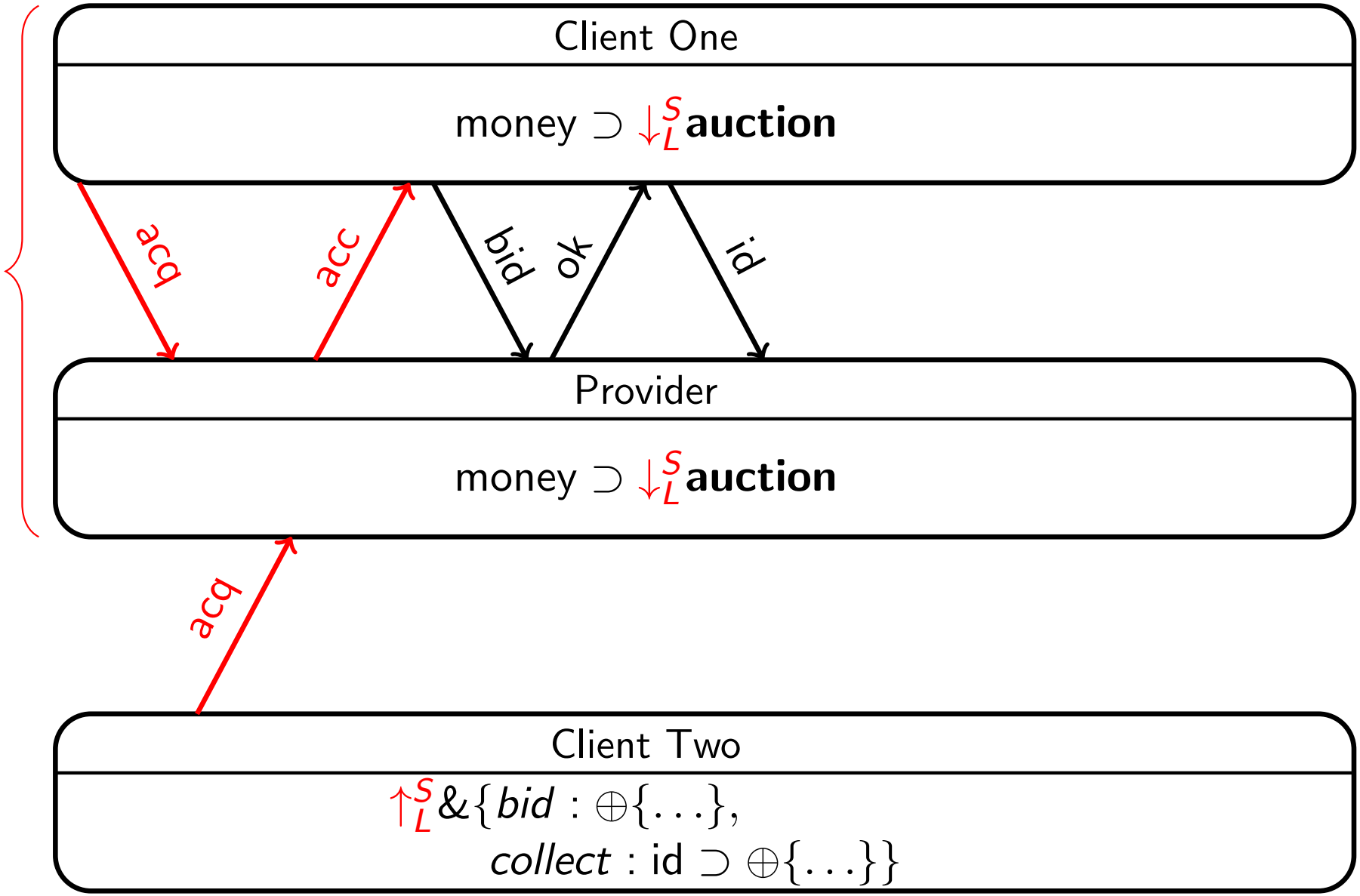

Client One
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Provider
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

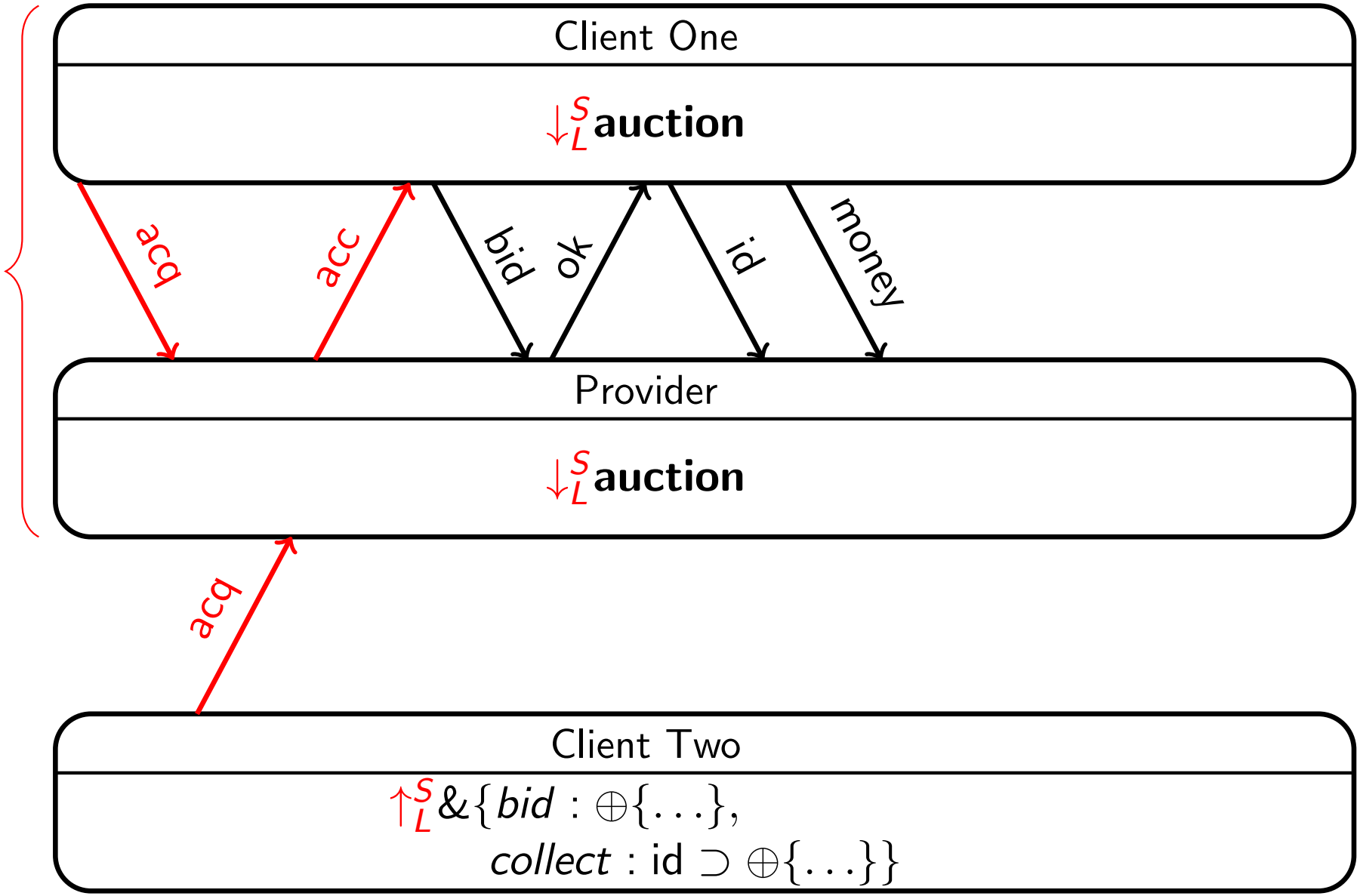

Client One
$\uparrow_L^S \&\{bid : \oplus\{\ldots\}, collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Provider
$\uparrow_L^S \&\{bid : \oplus\{\ldots\}, collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\}, collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

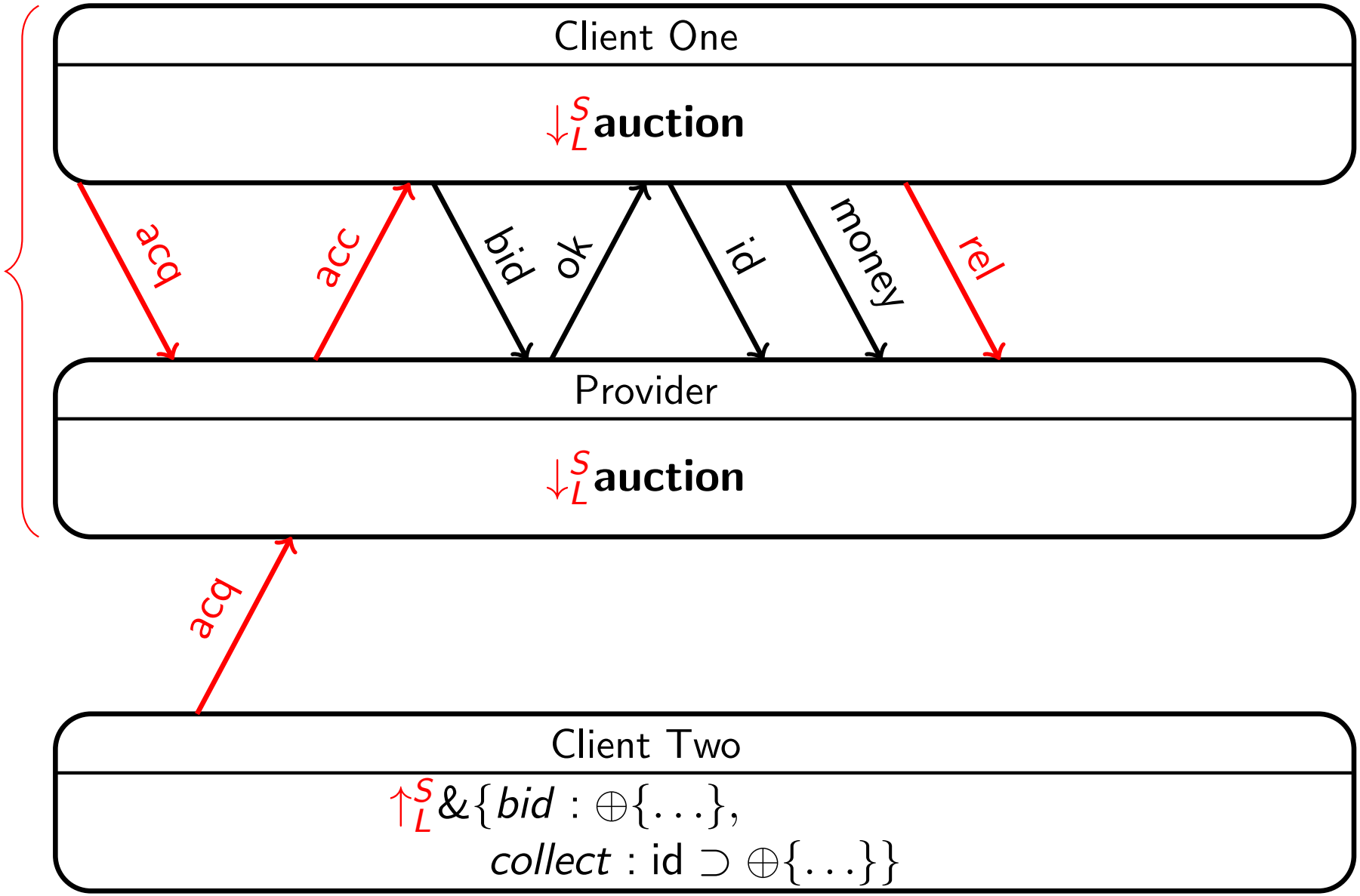

Client One
$\&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}$
acq
acc
Provider
$\&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}$
acq
Client Two
$\uparrow^{S}_{L} \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

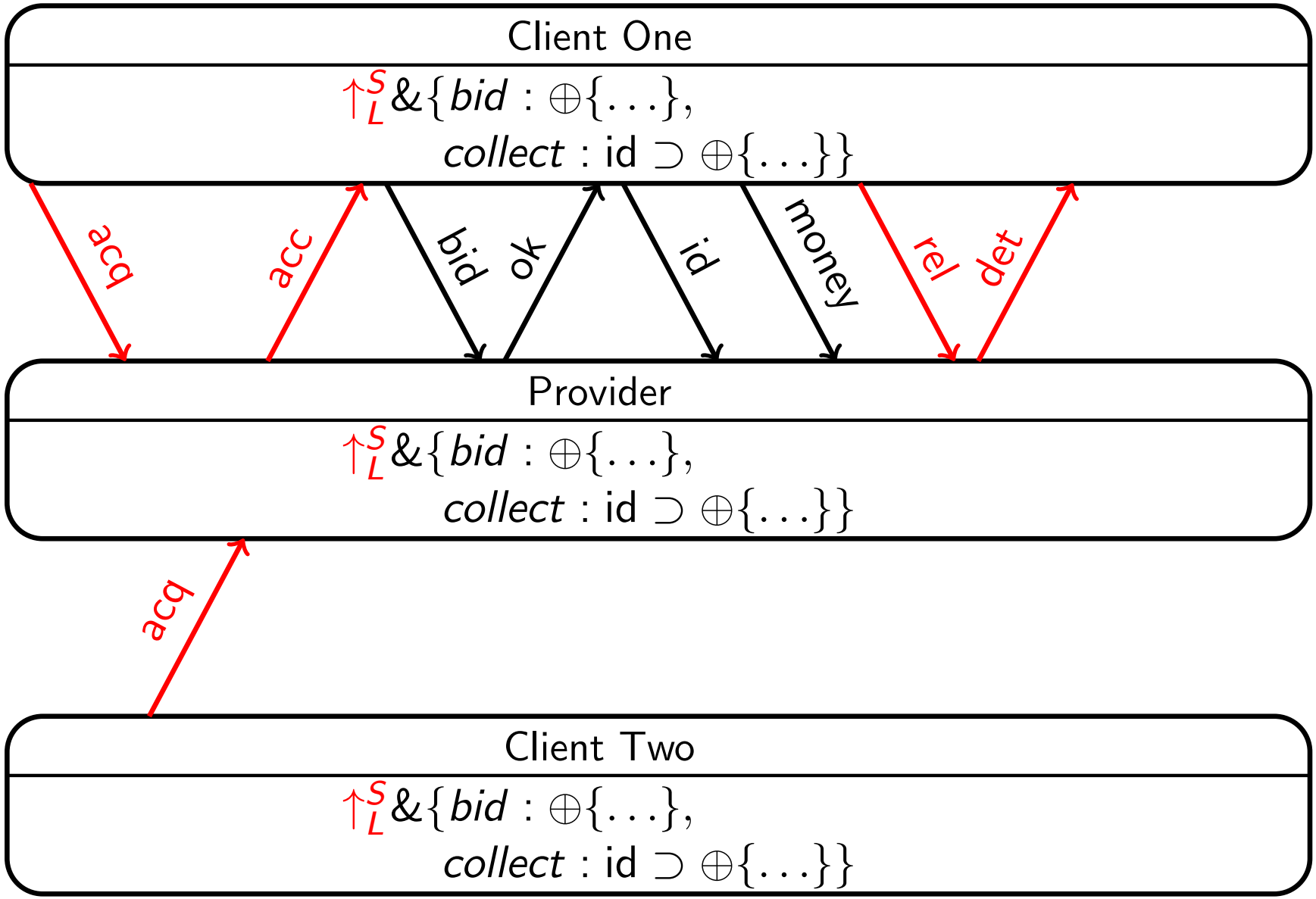

Client One
$\oplus\{ok : \mathrm{id} \supset \mathrm{money} \supset \downarrow_L^S \mathbf{auction},$
$collecting : \downarrow_L^S \mathbf{auction}\}\}$
acq
acc
bid
Provider
$\oplus\{ok : \mathrm{id} \supset \mathrm{money} \supset \downarrow_L^S \mathbf{auction},$
$collecting : \downarrow_L^S \mathbf{auction}\}\}$
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

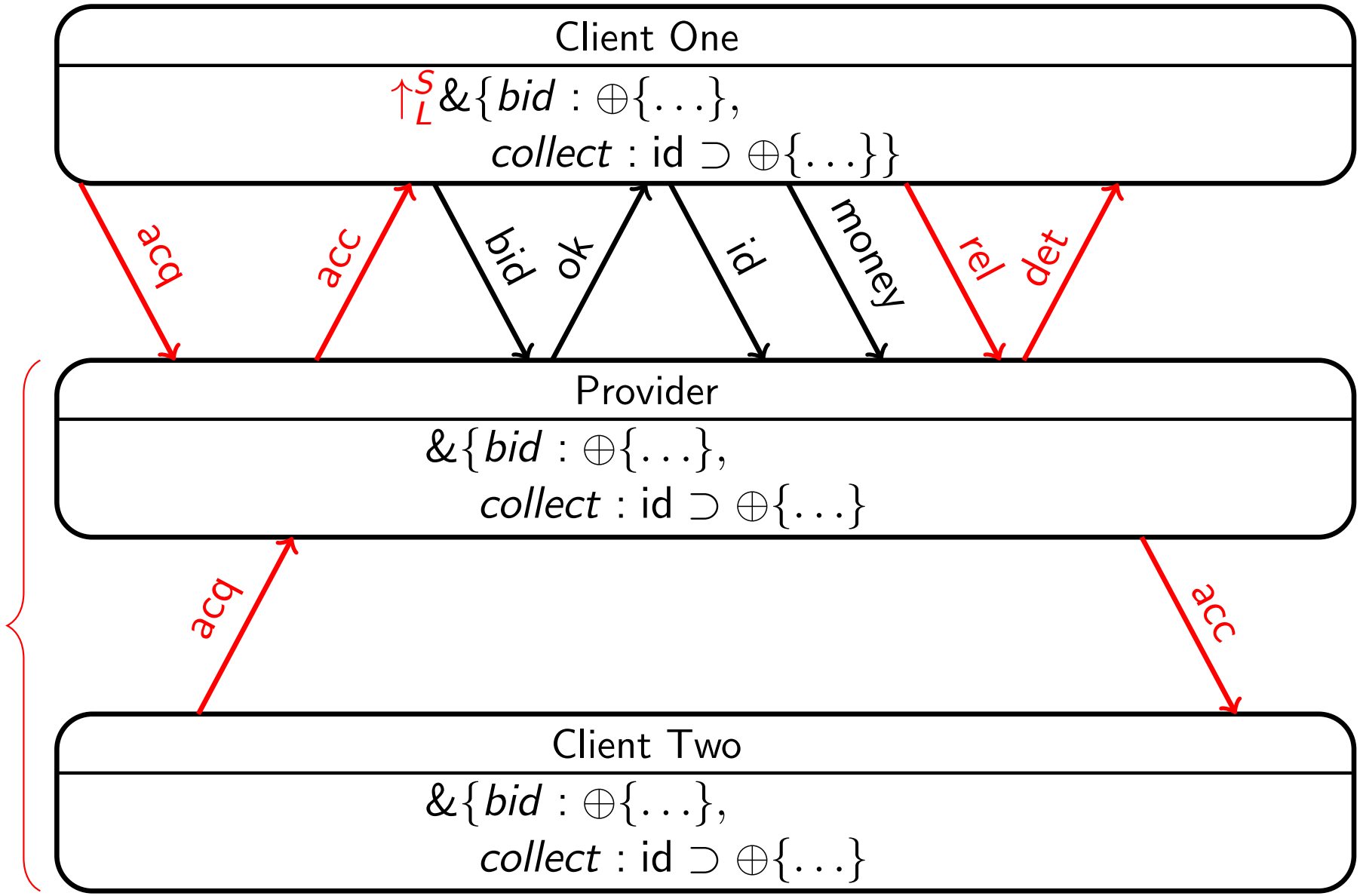

Client One
id ⊃ money ⊃ $\downarrow_L^S$ auction
acq
acc
bid
ok
Provider
id ⊃ money ⊃ $\downarrow_L^S$ auction
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

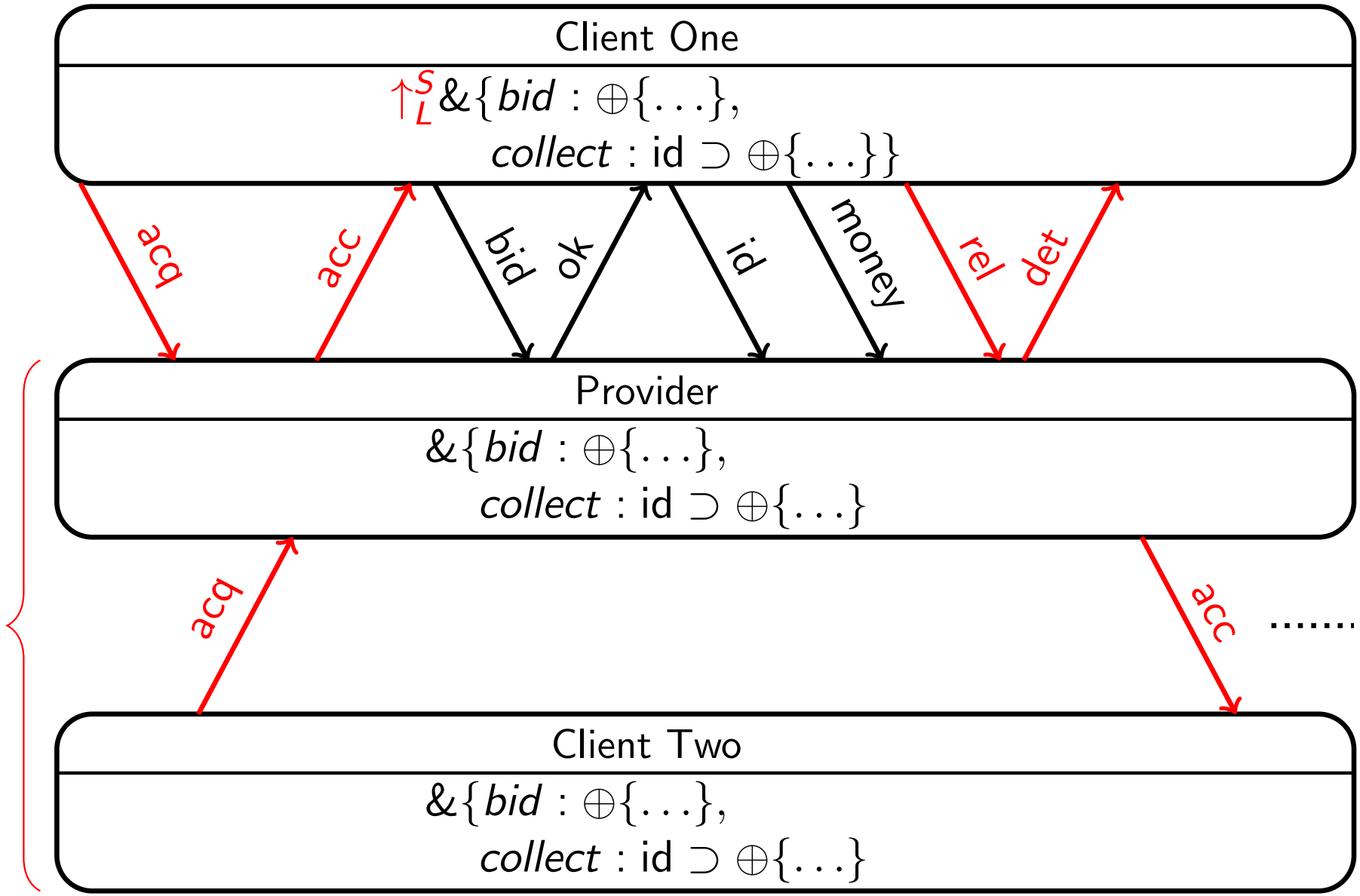

Client One
money ⊃ $\downarrow_L^S$ **auction**
acq
acc
bid
ok
id
Provider
money ⊃ $\downarrow_L^S$ **auction**
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$


Client One
$\downarrow_L^S$auction
acq
acc
bid
ok
id
money
Provider
$\downarrow_L^S$auction
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$


Client One
$\downarrow_L^S$auction
acq
acc
bid
ok
id
money
rel
Provider
$\downarrow_L^S$auction
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$


Client One
$\uparrow_L^S \&\{bid : \oplus\{\ldots\}, collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
acc
bid
ok
id
money
rel
det
Provider
$\uparrow_L^S \&\{bid : \oplus\{\ldots\}, collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Client Two
$\uparrow_L^S \&\{bid : \oplus\{\ldots\}, collect : \mathrm{id} \supset \oplus\{\ldots\}\}$


Client One
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
acc
bid
ok
id
money
rel
det
Provider
$\&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}$
acq
acc
Client Two
$\&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}$

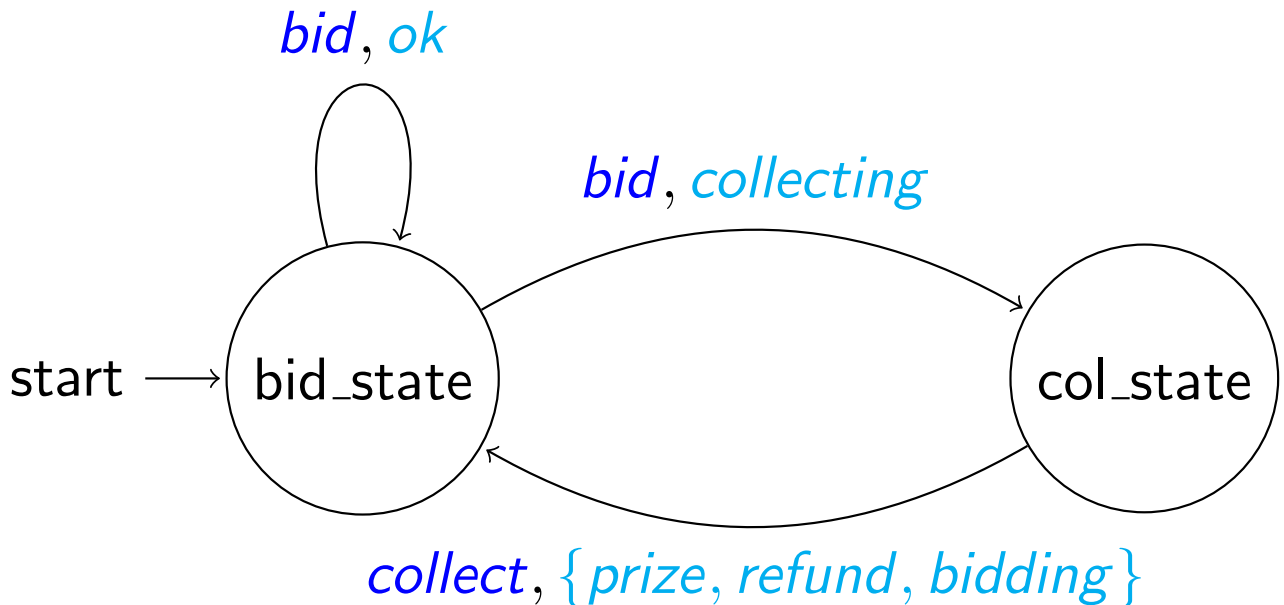

Client One
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
acc
bid
ok
id
money
rel
det
Provider
$\&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}$
acq
acc
.....
Client Two
$\&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}$

Auction

$$\begin{aligned}\textbf{auction} = \uparrow^{S}_{L} \& \{ & \mathit{bid} : \oplus\{\mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow^{S}_{L} \textbf{auction}, \\ & \mathit{collecting} : \downarrow^{S}_{L} \textbf{auction}\}, \\ & \mathit{collect} : \mathsf{id} \supset \oplus\{\mathit{prize} : \mathsf{item} \wedge \downarrow^{S}_{L} \textbf{auction}, \\ & \mathit{refund} : \mathsf{money} \wedge \downarrow^{S}_{L} \textbf{auction}, \\ & \mathit{bidding} : \downarrow^{S}_{L} \textbf{auction}\}\}\end{aligned}$$

Auction

$$\textbf{auction} = \uparrow^S_L \& \{ \mathit{bid} : \oplus \{ \mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow^S_L \textbf{auction},$$
$$\mathit{collecting} : \downarrow^S_L \textbf{auction} \},$$
$$\mathit{collect} : \mathsf{id} \supset \oplus \{ \mathit{prize} : \mathsf{item} \wedge \downarrow^S_L \textbf{auction},$$
$$\mathit{refund} : \mathsf{money} \wedge \downarrow^S_L \textbf{auction},$$
$$\mathit{bidding} : \downarrow^S_L \textbf{auction} \} \}$$



Subtyping[3] to the Rescue?

$A \leq B$ (Provider A can communicate with client B.)

[3] Gay and Hole 2005.

Subtyping[3] to the Rescue?

$A \leq B$ (Provider A can communicate with client B.)

$$\frac{}{1 \leq 1}\ \leq_1 \qquad \frac{A_L \leq A'_L \qquad B_L \leq B'_L}{A_L \otimes B_L \leq A'_L \otimes B'_L}\ \leq_\otimes \qquad \frac{A'_L \leq A_L \qquad B_L \leq B'_L}{A_L \multimap B_L \leq A'_L \multimap B'_L}\ \leq_\multimap$$

$$\frac{\forall i \in \bar{I} \quad A_{i\,L} \leq A'_{i\,L}}{\oplus\{\overline{l{:}A_L}\} \leq \oplus\{\overline{l{:}A'_L}, \overline{m{:}B_L}\}}\ \leq_\oplus \qquad \frac{\forall i \in \bar{I} \quad A_{i\,L} \leq A'_{i\,L}}{\&\{\overline{l{:}A_L}, \overline{m{:}B_L}\} \leq \&\{\overline{l{:}A'_L}\}}\ \leq_\&$$

[3] Gay and Hole 2005.

Subtyping[3] to the Rescue?

$A \leq B$ (Provider A can communicate with client B.)

$$\frac{}{1 \leq 1}\ \leq_1 \qquad \frac{A_L \leq A'_L \qquad B_L \leq B'_L}{A_L \otimes B_L \leq A'_L \otimes B'_L}\ \leq_\otimes \qquad \frac{A'_L \leq A_L \qquad B_L \leq B'_L}{A_L \multimap B_L \leq A'_L \multimap B'_L}\ \leq_\multimap$$

$$\frac{\forall i \in \bar{I} \quad A_{i\,L} \leq A'_{i\,L}}{\oplus\{\overline{l{:}A_L}\} \leq \oplus\{\overline{l{:}A'_L}, \overline{m{:}B_L}\}}\ \leq_\oplus \qquad \frac{\forall i \in \bar{I} \quad A_{i\,L} \leq A'_{i\,L}}{\&\{\overline{l{:}A_L}, \overline{m{:}B_L}\} \leq \&\{\overline{l{:}A'_L}\}}\ \leq_\&$$

$$\frac{A_L \leq B_L}{\uparrow^S_L A_L \leq \uparrow^S_L B_L}\ \leq_{\uparrow^S_L} \qquad \frac{A_S \leq B_S}{\downarrow^S_L A_S \leq \downarrow^S_L B_S}\ \leq_{\downarrow^S_L}$$

[3] Gay and Hole 2005.

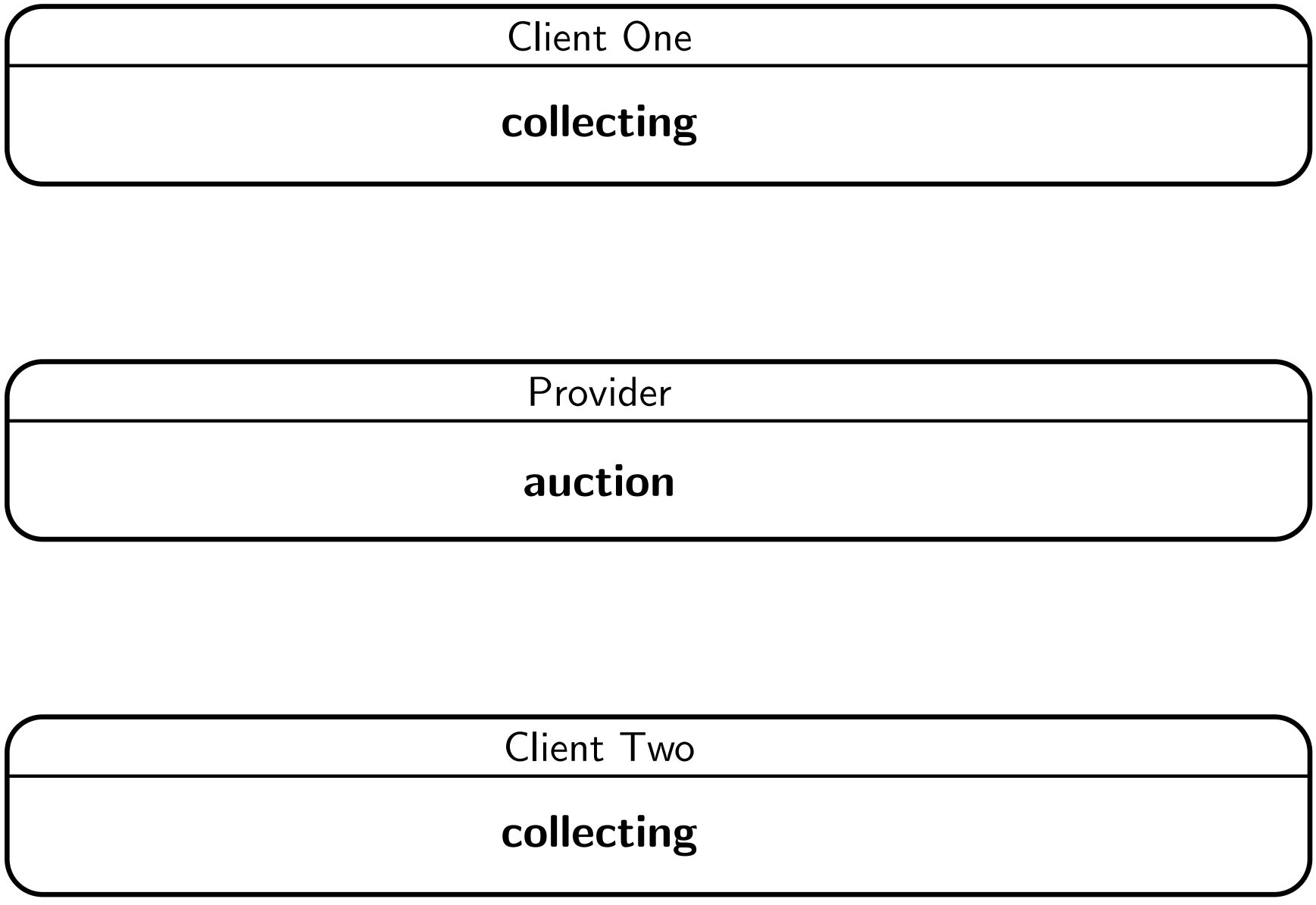
Auction With Subtyping

$$\textbf{auction} \leq \textbf{bidding}$$

$$\textbf{auction} \leq \textbf{collecting}$$

$$\text{provider} \begin{cases} \textbf{auction} = \uparrow_L^S \& \{ \mathit{bid} : \oplus \{ \mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow_L^S \textbf{auction}, \\ \qquad\qquad \mathit{collecting} : \downarrow_L^S \textbf{auction} \}, \\ \qquad \mathit{collect} : \mathsf{id} \supset \oplus \{ \mathit{prize} : \mathsf{item} \wedge \downarrow_L^S \textbf{auction}, \\ \qquad\qquad \mathit{refund} : \mathsf{money} \wedge \downarrow_L^S \textbf{auction}, \\ \qquad\qquad \mathit{bidding} : \downarrow_L^S \textbf{auction} \} \} \end{cases}$$

$$\text{clients} \begin{cases} \textbf{bidding} = \uparrow_L^S \& \{ \mathit{bid} : \oplus \{ \mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow_L^S \textbf{bidding}, \\ \qquad\qquad \mathit{collecting} : \downarrow_L^S \textbf{collecting} \} \} \\ \textbf{collecting} = \uparrow_L^S \& \{ \mathit{collect} : \mathsf{id} \supset \oplus \{ \mathit{prize} : \mathsf{item} \wedge \downarrow_L^S \textbf{bidding}, \\ \qquad\qquad \mathit{refund} : \mathsf{money} \wedge \downarrow_L^S \textbf{bidding}, \\ \qquad\qquad \mathit{bidding} : \downarrow_L^S \textbf{bidding} \} \} \end{cases}$$


Client One
collecting
Provider
auction
Client Two
collecting

Client One

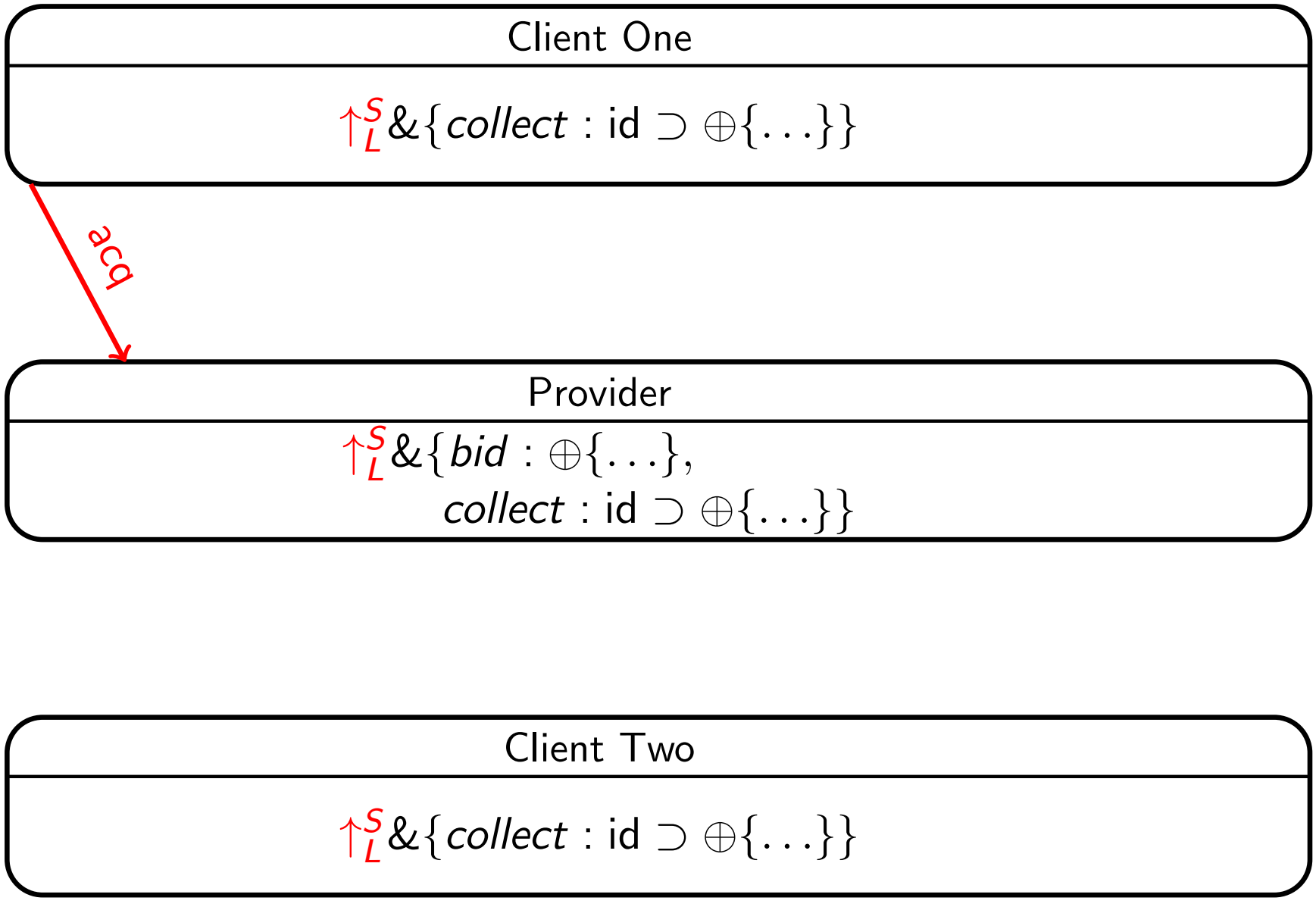
$$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$$

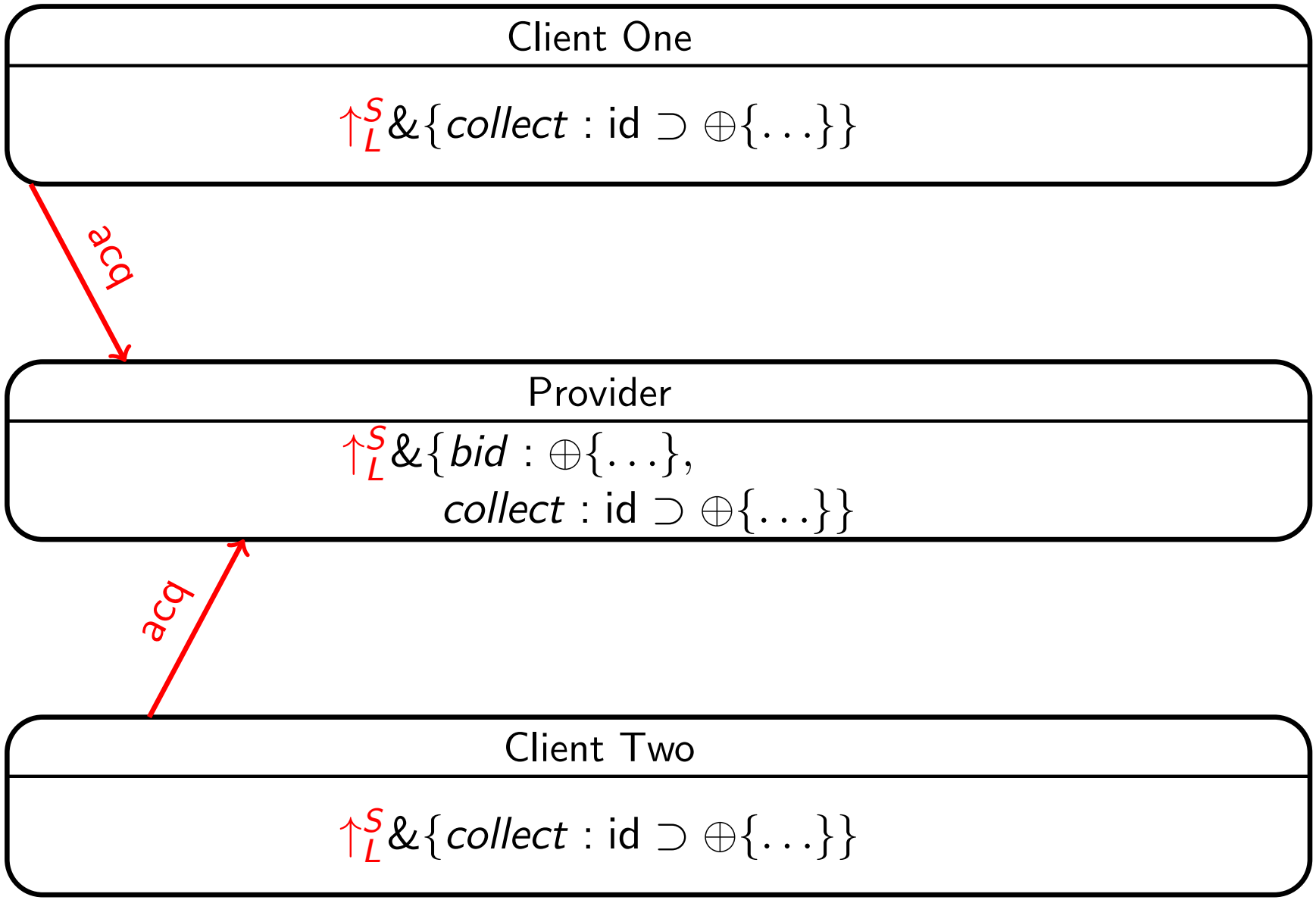
Provider

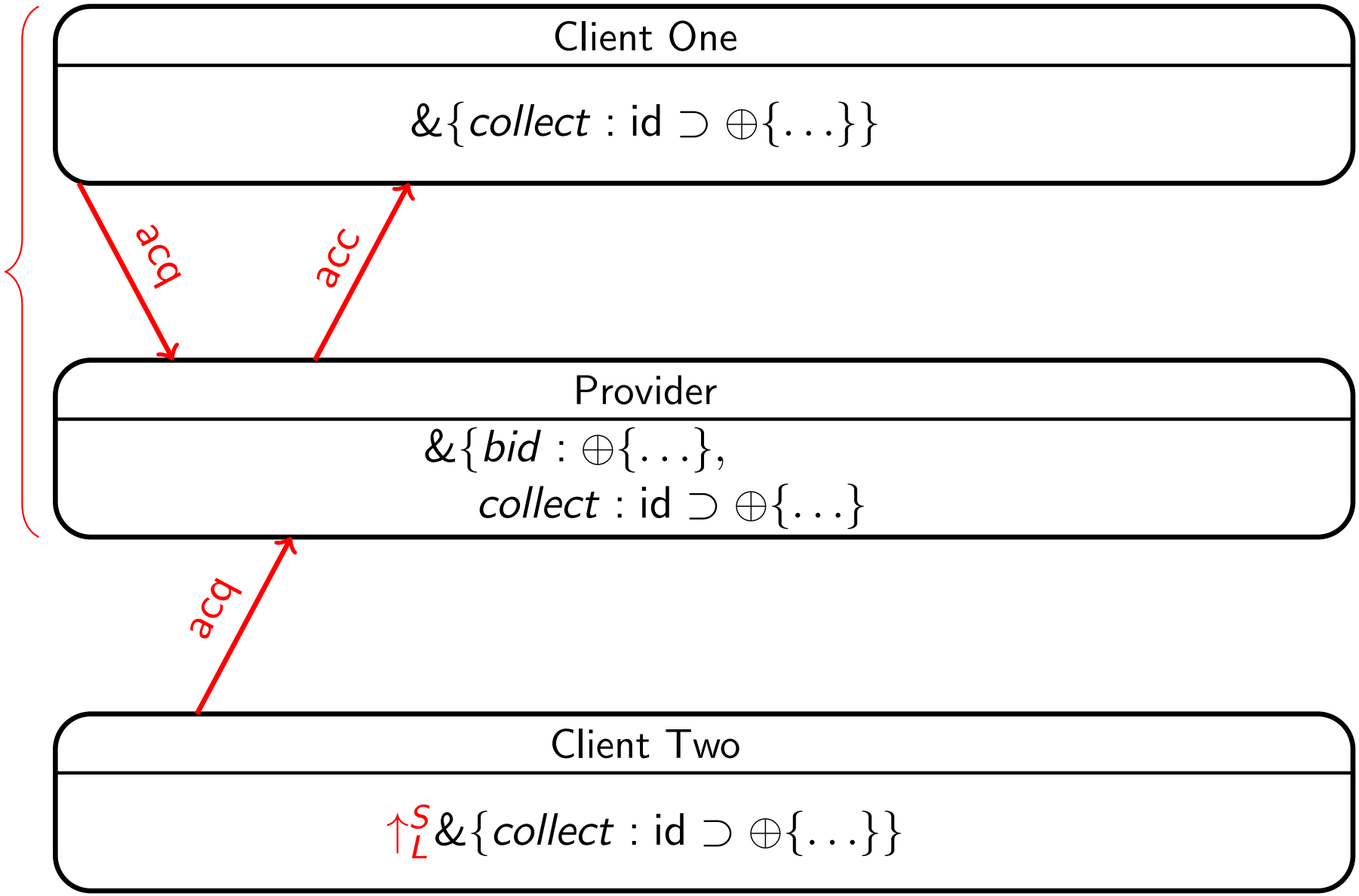
$$\uparrow_L^S \&\{bid : \oplus\{\ldots\},\ collect : \mathrm{id} \supset \oplus\{\ldots\}\}$$

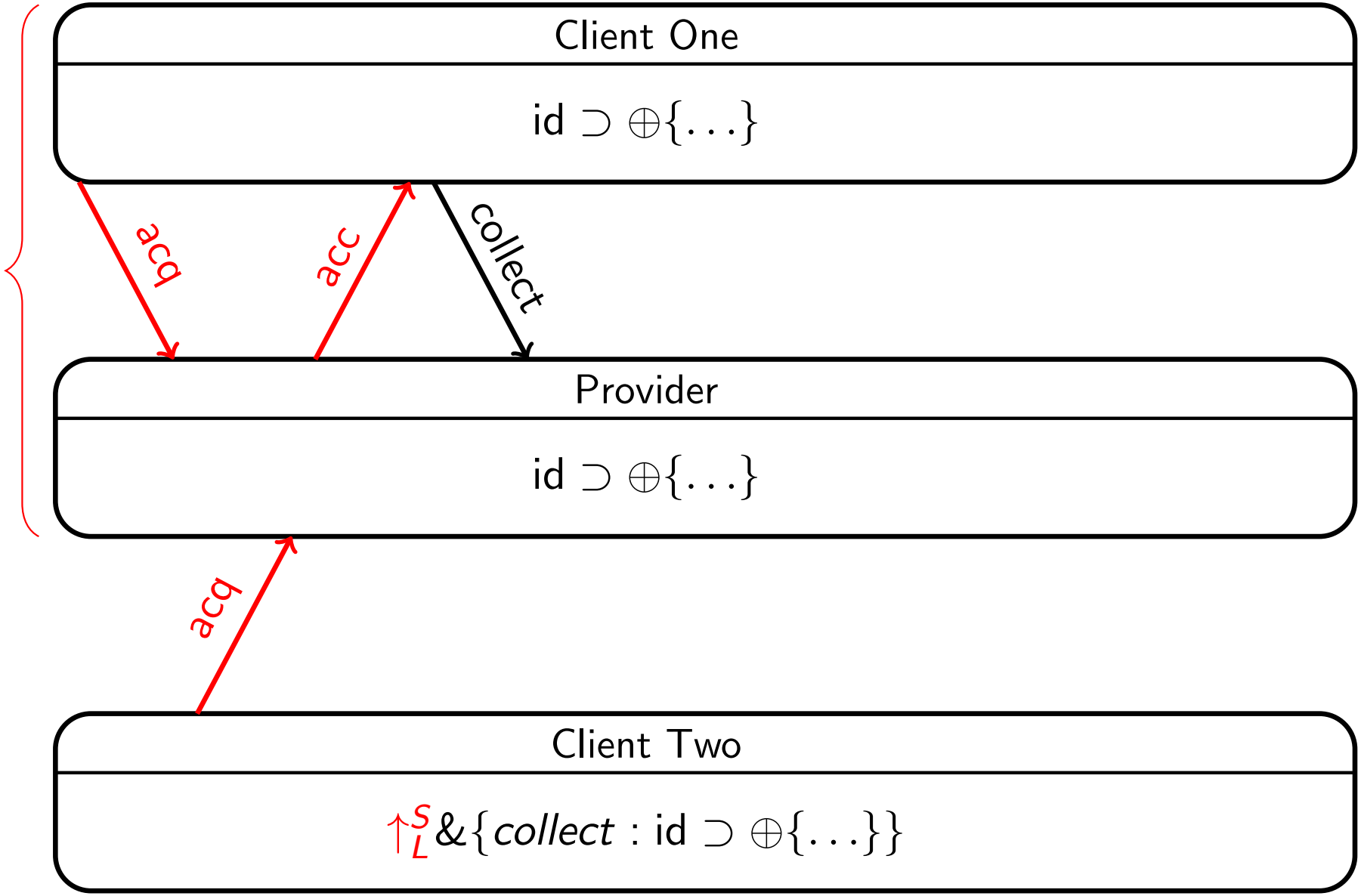
Client Two

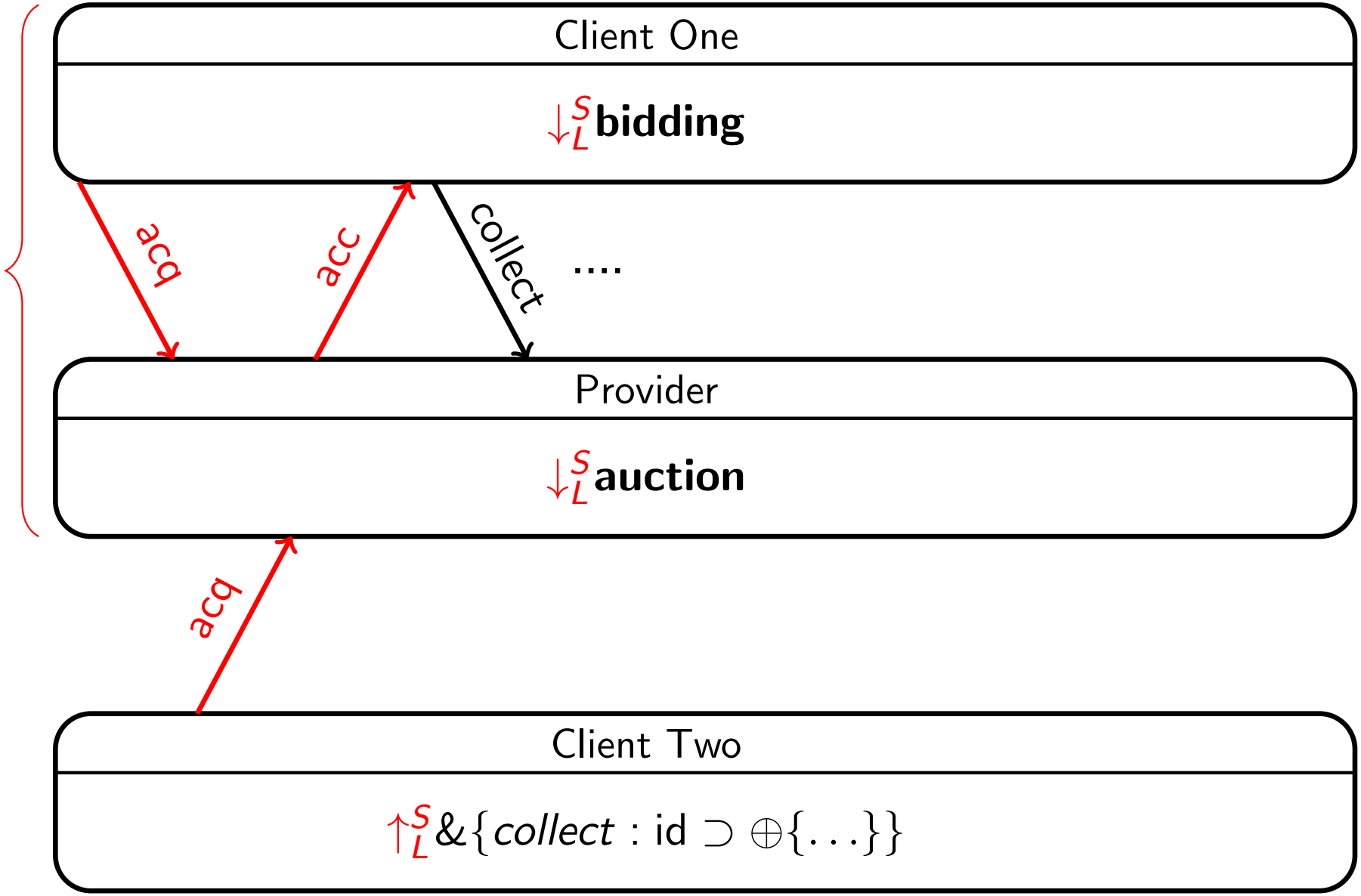
$$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$$

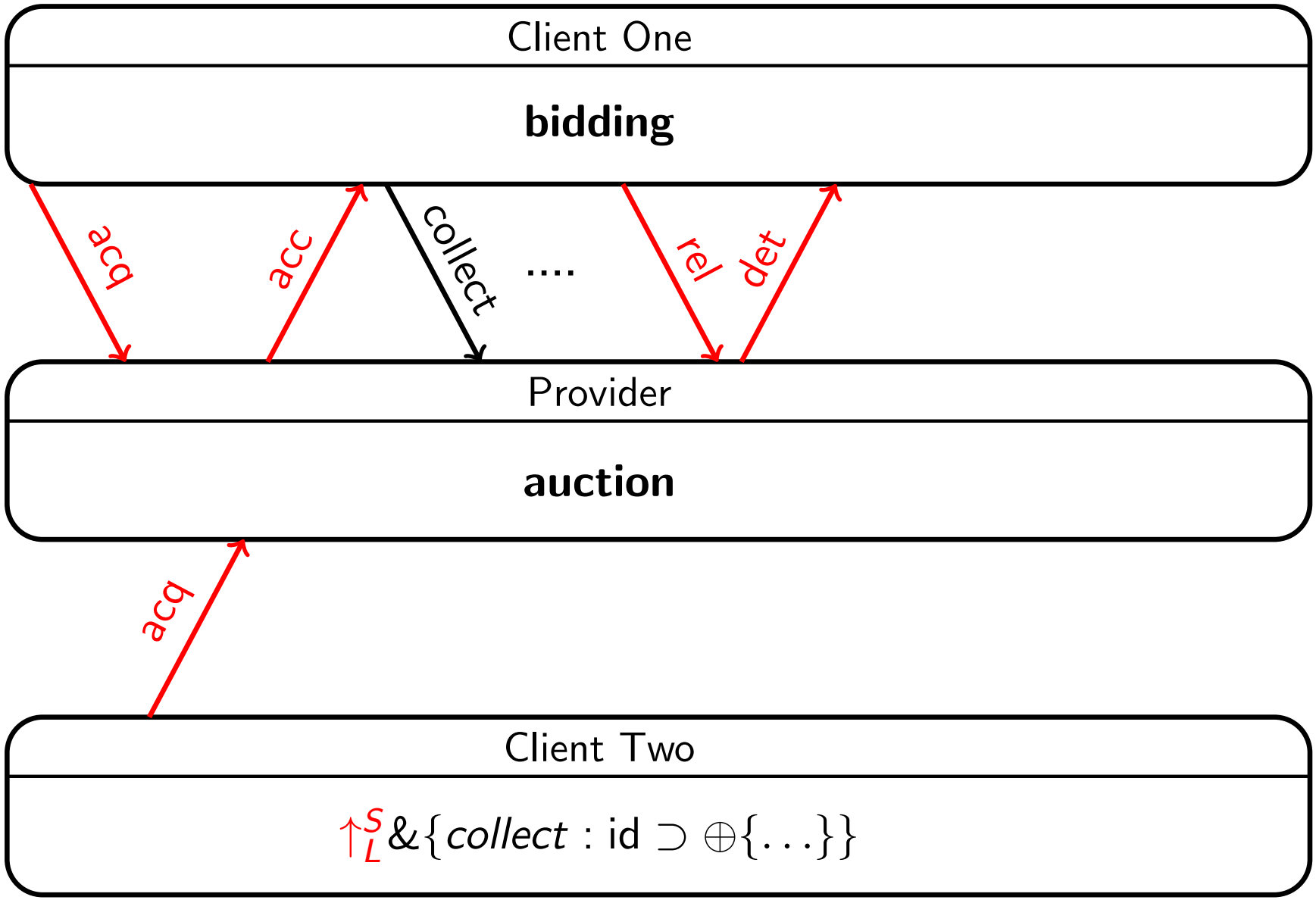

Client One
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Provider
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
Client Two
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

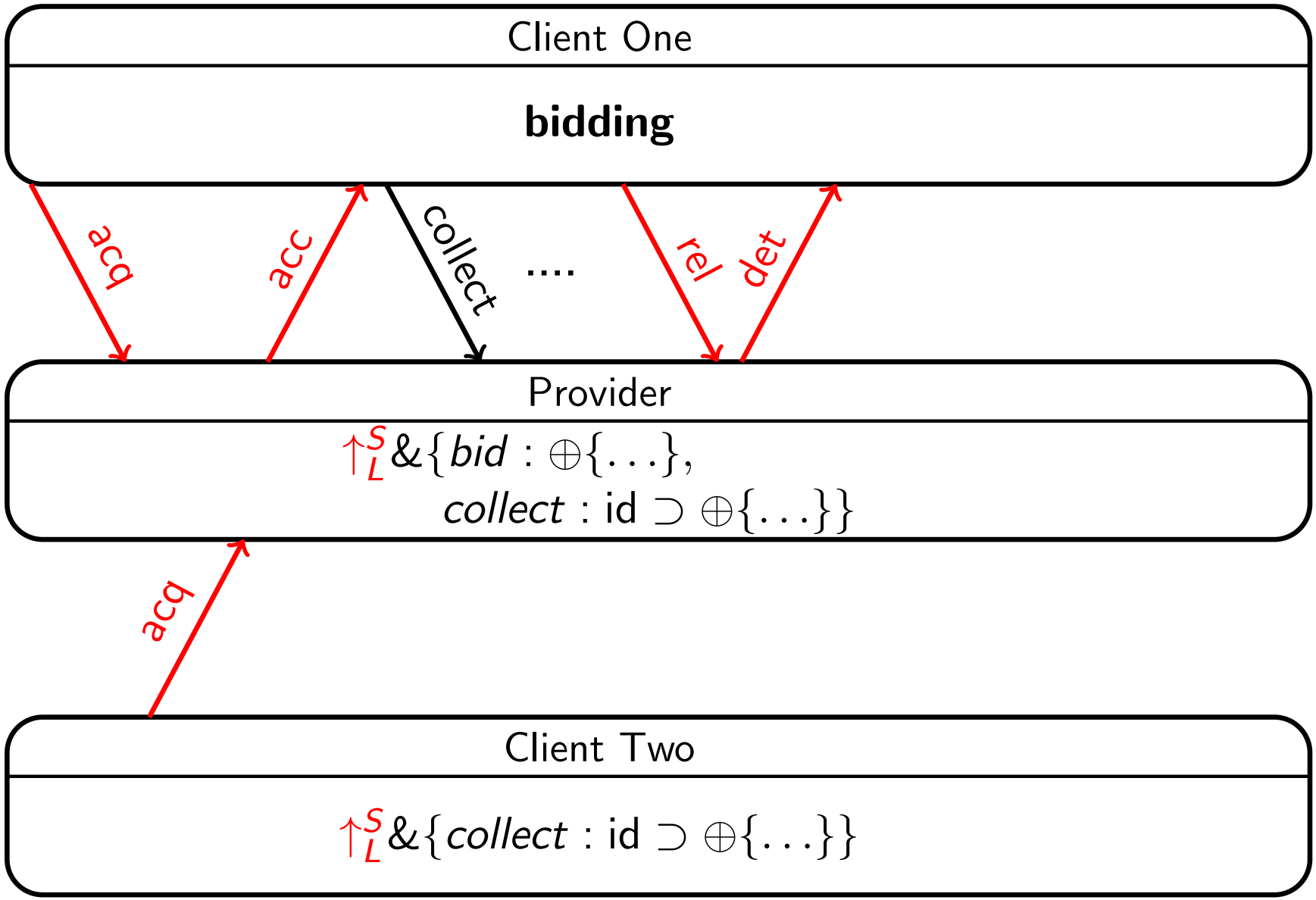

Client One
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Provider
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Client Two
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

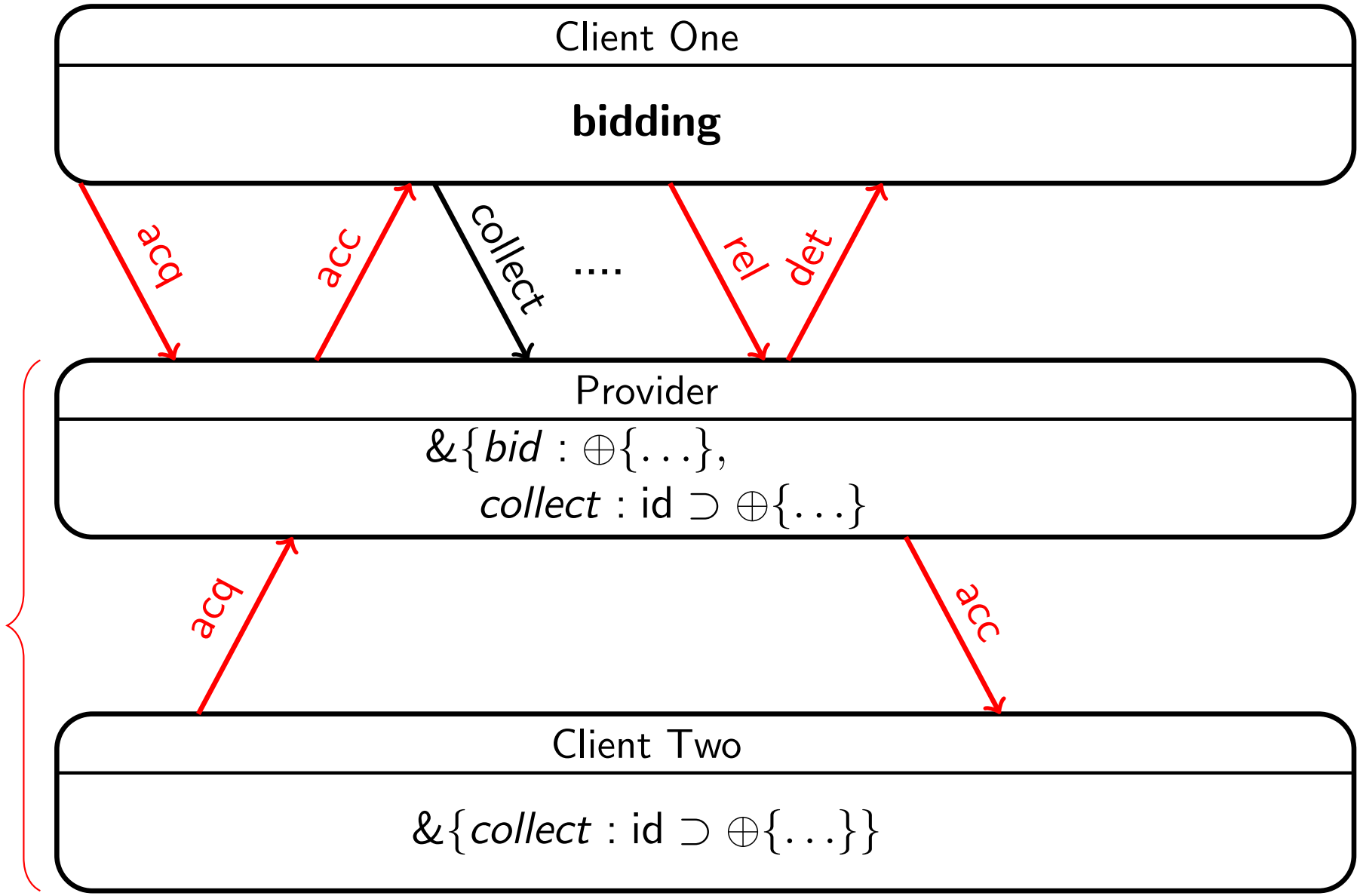

Client One
&{collect : id ⊃ ⊕{...}}
acq
acc
Provider
&{bid : ⊕{...},
collect : id ⊃ ⊕{...}
acq
Client Two
↑$^{S}_{L}$&{collect : id ⊃ ⊕{...}}

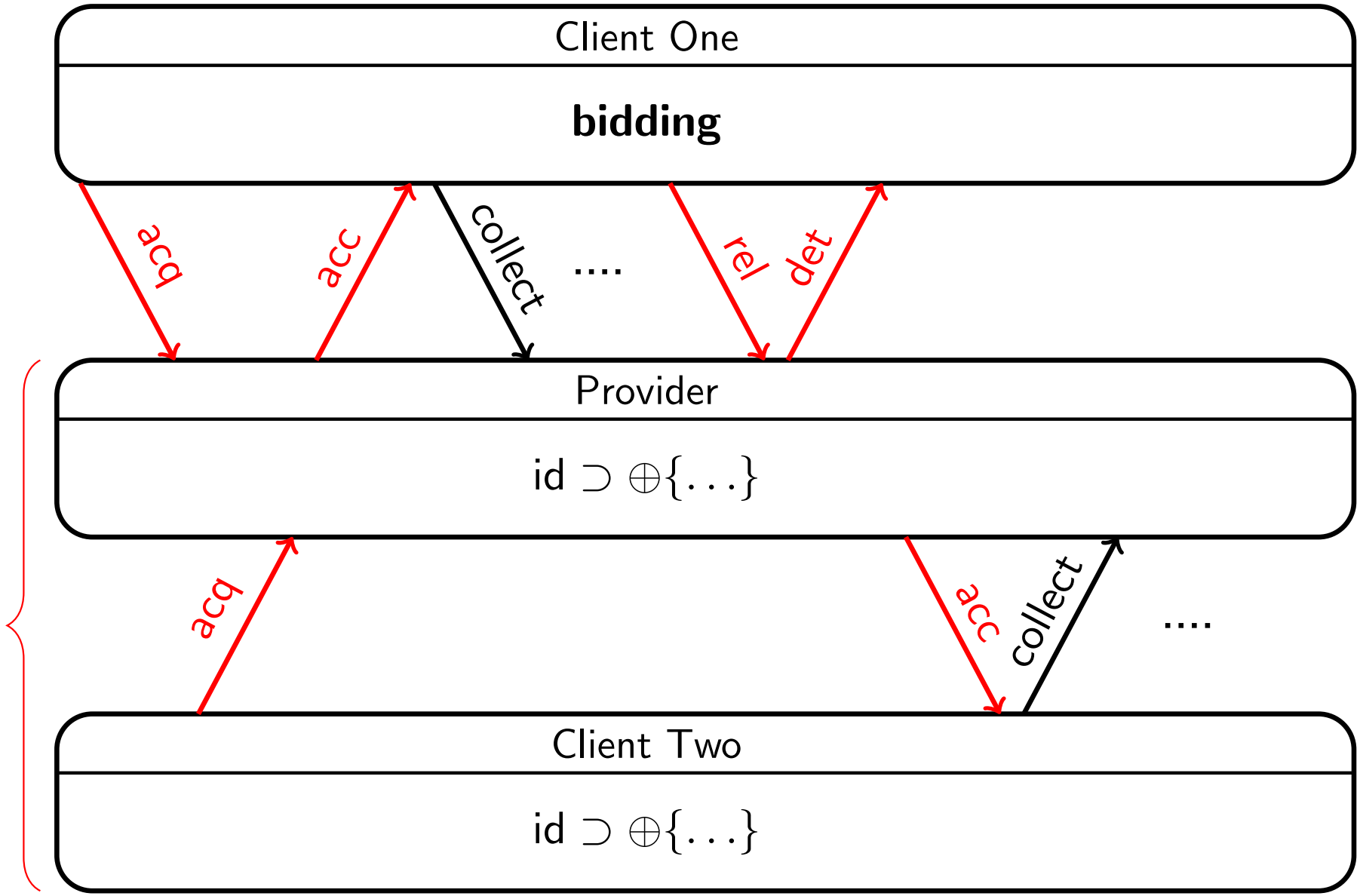

Client One
id ⊃ ⊕{...}
acq
acc
collect
Provider
id ⊃ ⊕{...}
acq
Client Two
↑$^{S}_{L}$&{collect : id ⊃ ⊕{...}}

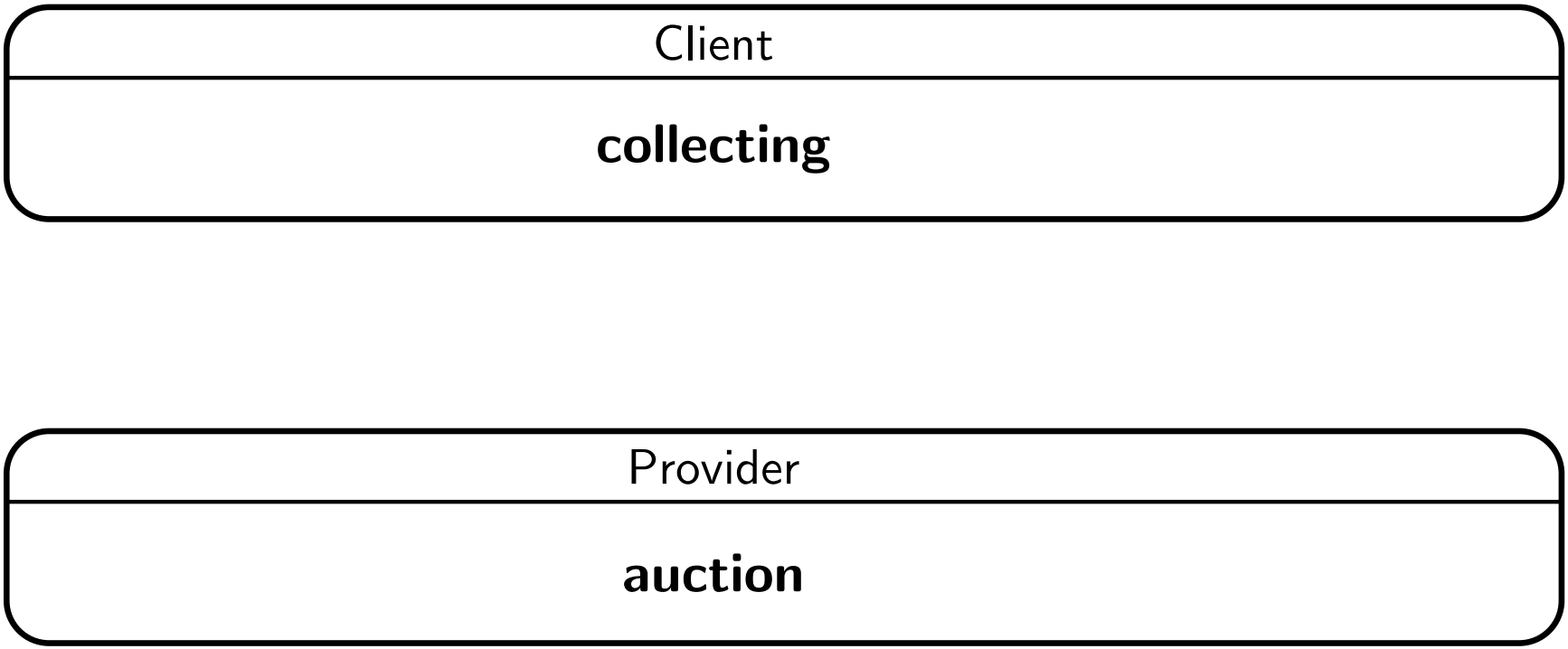

Client One
$\downarrow_L^S$ **bidding**
acq
acc
collect
....
Provider
$\downarrow_L^S$ **auction**
acq
Client Two
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$


Client One
bidding
acq
acc
collect
....
rel
det
Provider
auction
acq
Client Two
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$

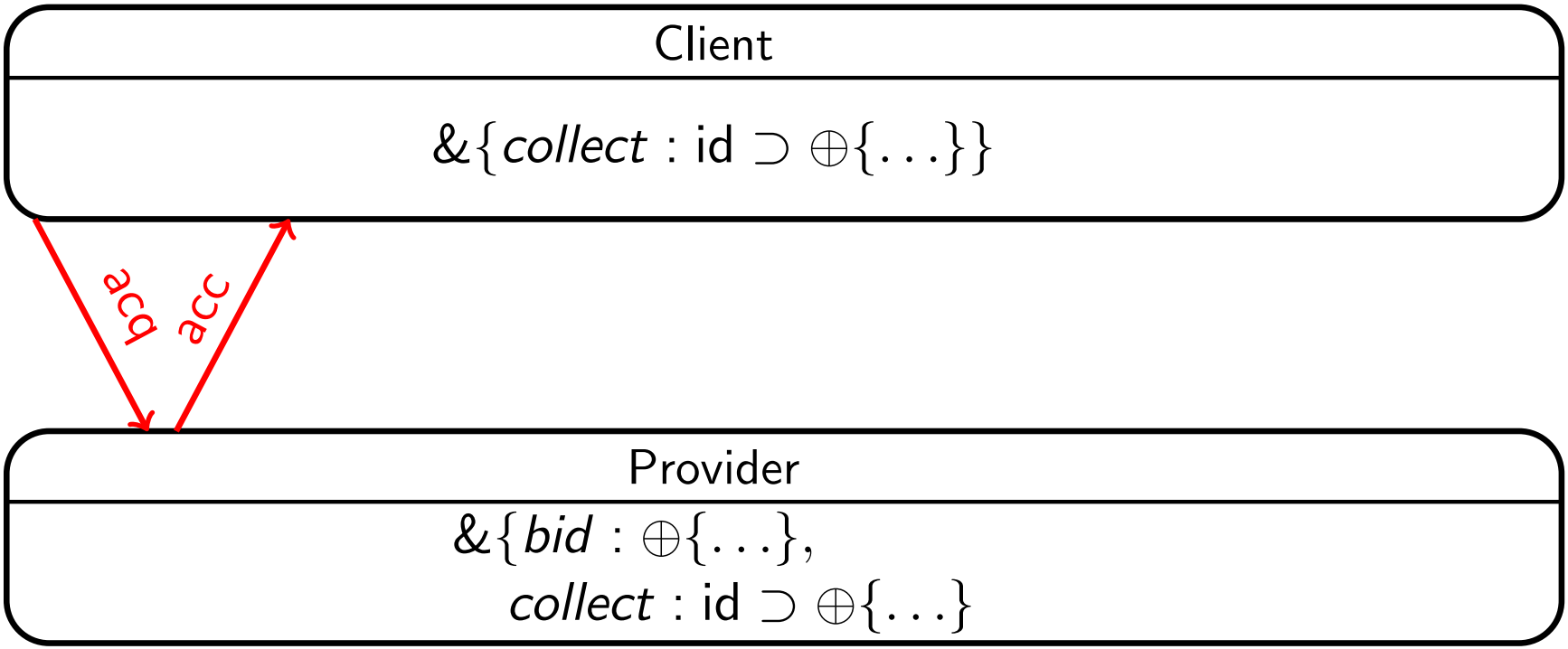

Client One
bidding
acq
acc
collect
....
rel
det
Provider
$\uparrow_L^S \&\{bid : \oplus\{\ldots\},$
$collect : \mathrm{id} \supset \oplus\{\ldots\}\}$
acq
Client Two
$\uparrow_L^S \&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\}$


Client One
bidding
acq
acc
collect
....
rel
det
Provider
&{bid : ⊕{...},
collect : id ⊃ ⊕{...}
acq
acc
Client Two
&{collect : id ⊃ ⊕{...}}

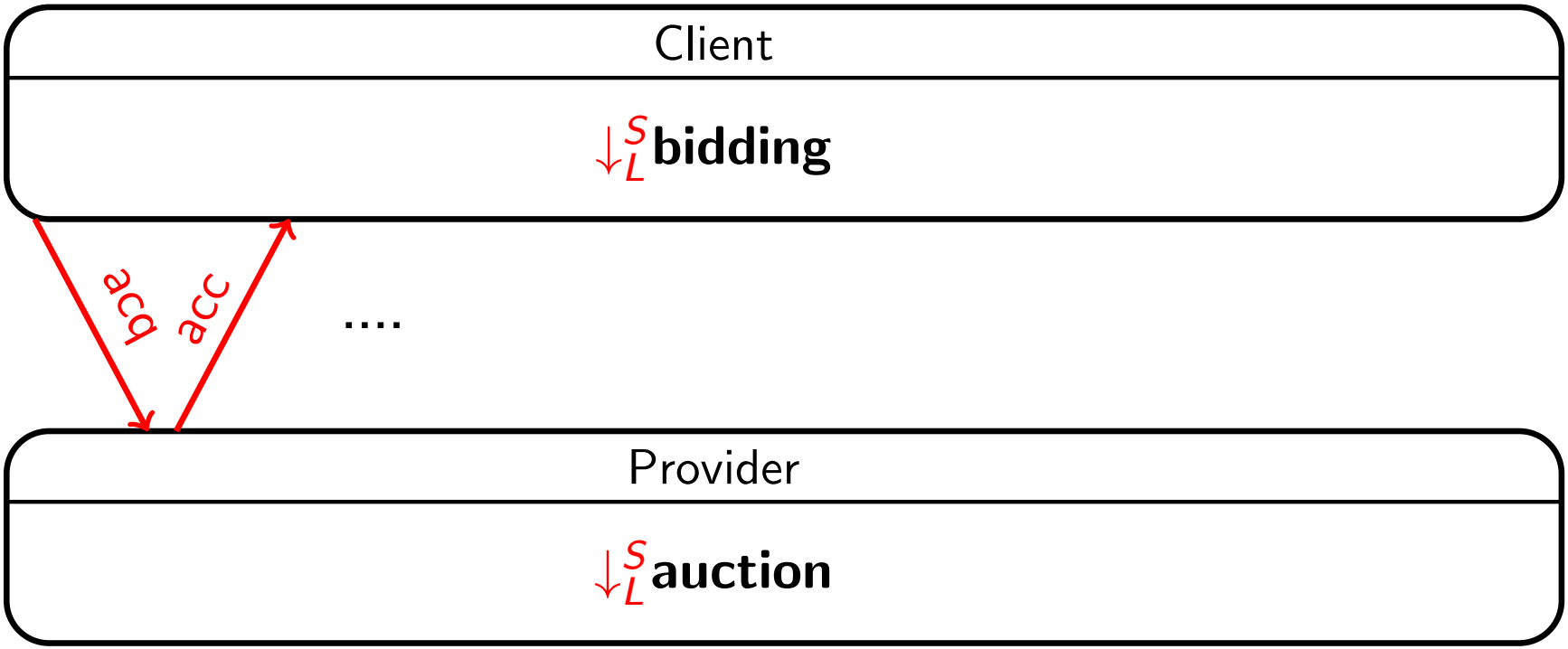

Client One
bidding
acq
acc
collect
....
rel
det
Provider
id ⊃ ⊕{...}
acq
acc
collect
....
Client Two
id ⊃ ⊕{...}



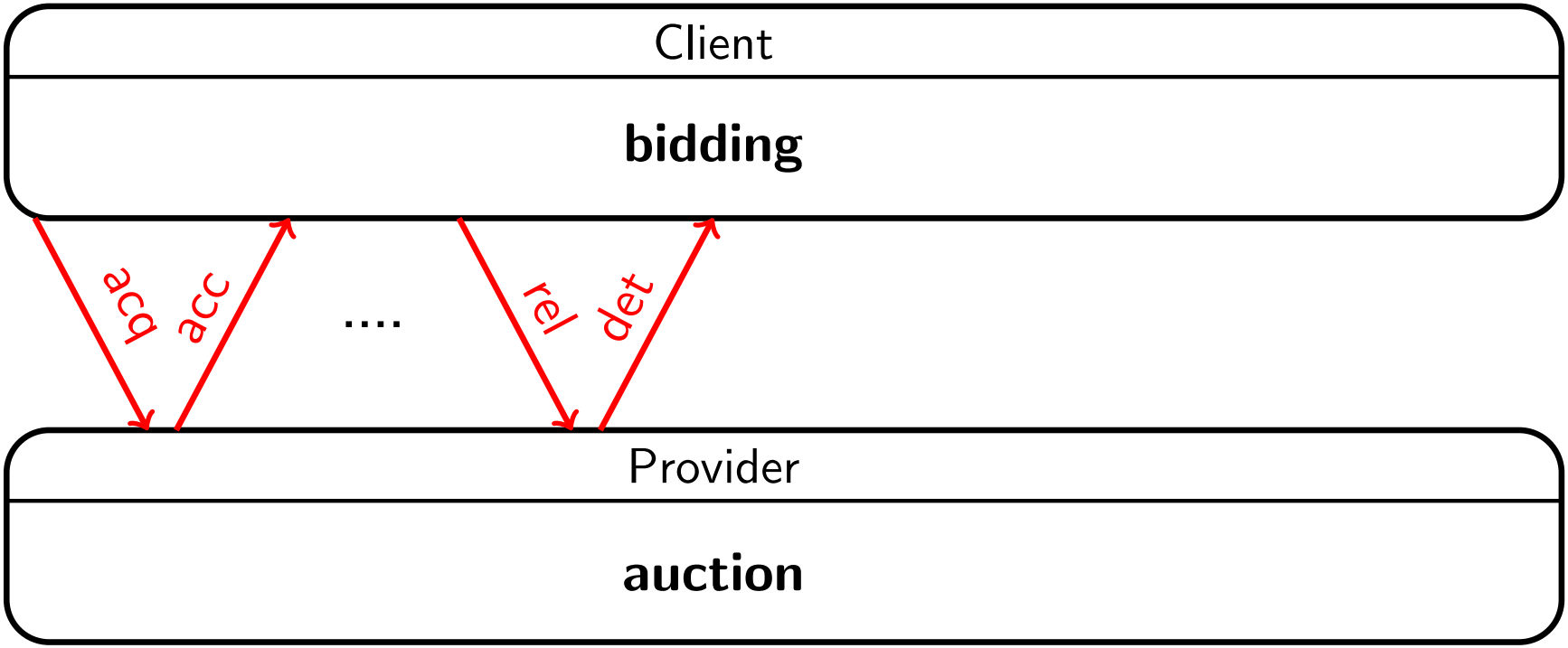
$$\Gamma, a_S{:}\mathbf{collecting}; \Delta \vdash P :: (c_L{:}C_L)$$



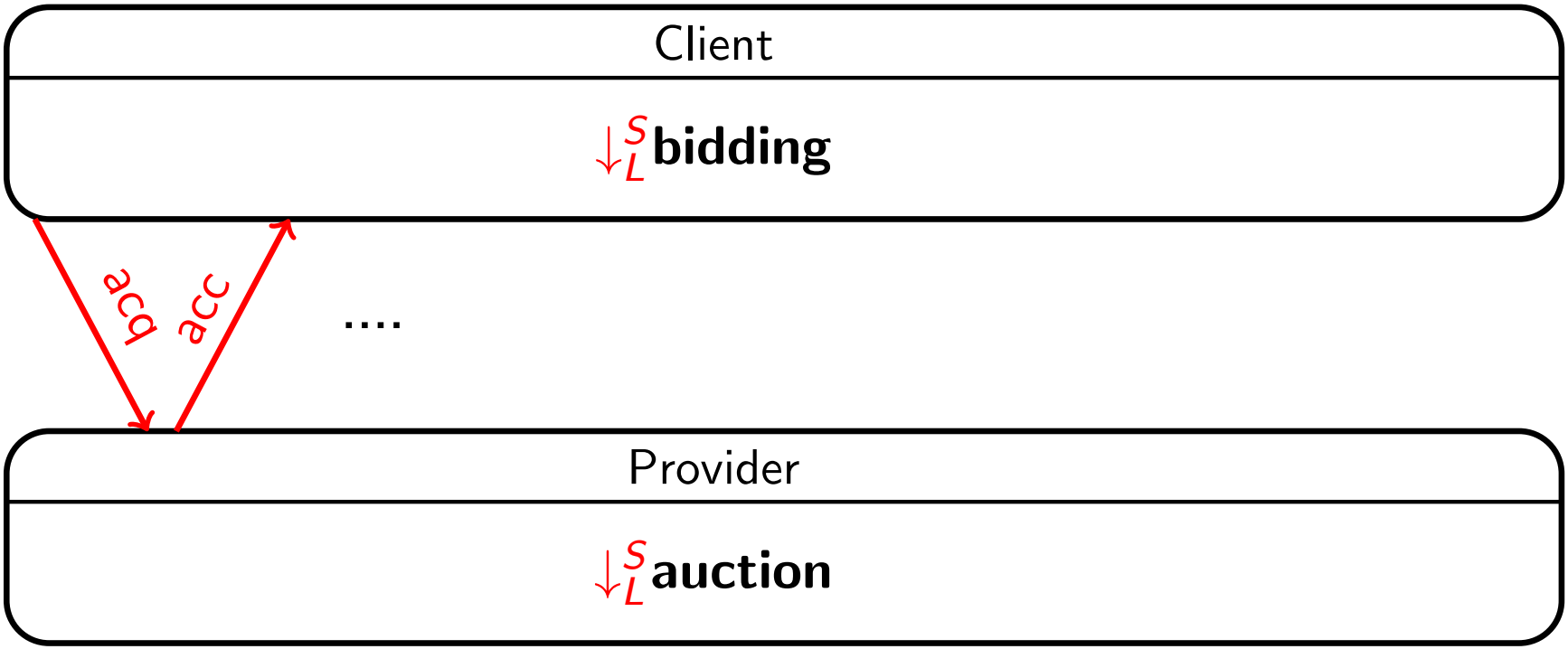
$\Gamma, a_S{:}\mathbf{collecting}; \Delta, a_L{:}\&\{collect : \mathrm{id} \supset \oplus\{\ldots\}\} \vdash P' :: (c_L{:}C_L)$



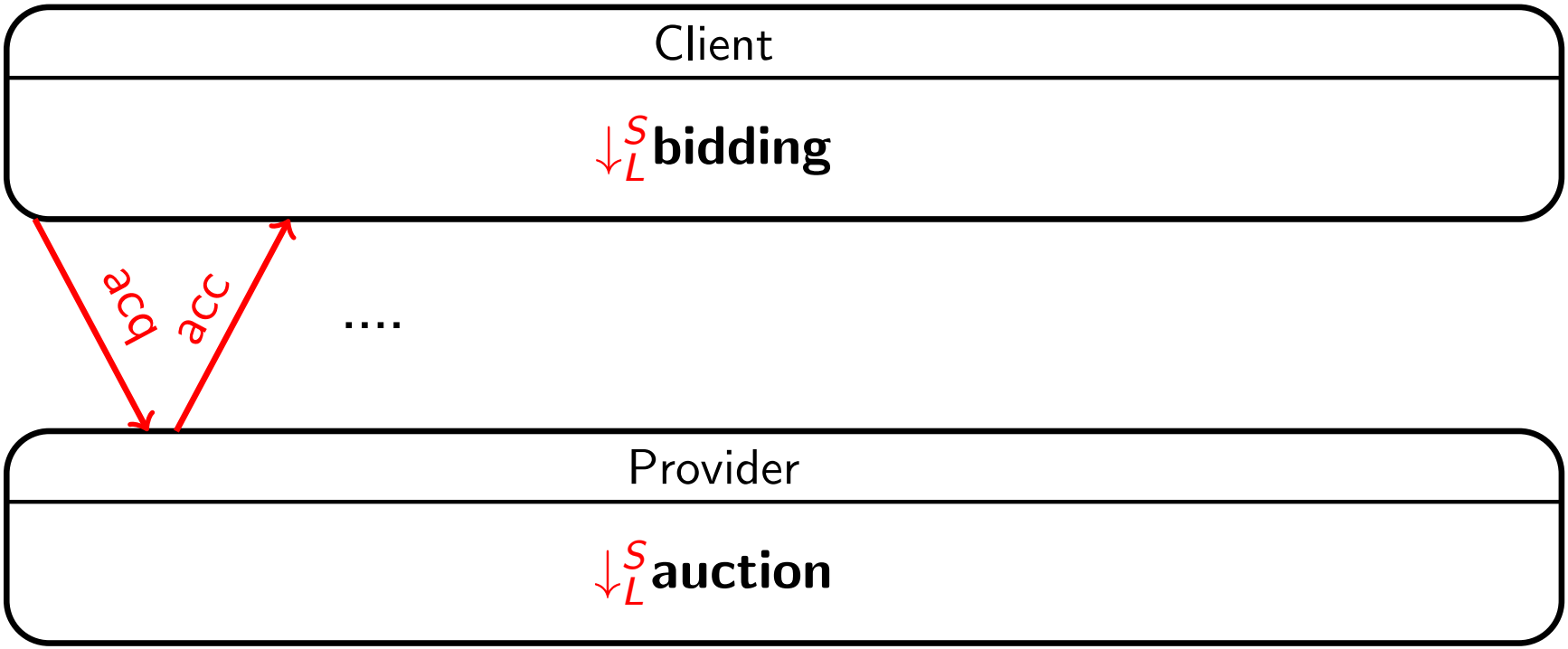
$$\Gamma, a_S{:}\mathbf{collecting}; \Delta, a_L{:}\downarrow_L^S \mathbf{bidding} \vdash P'' :: (c_L{:}C_L)$$



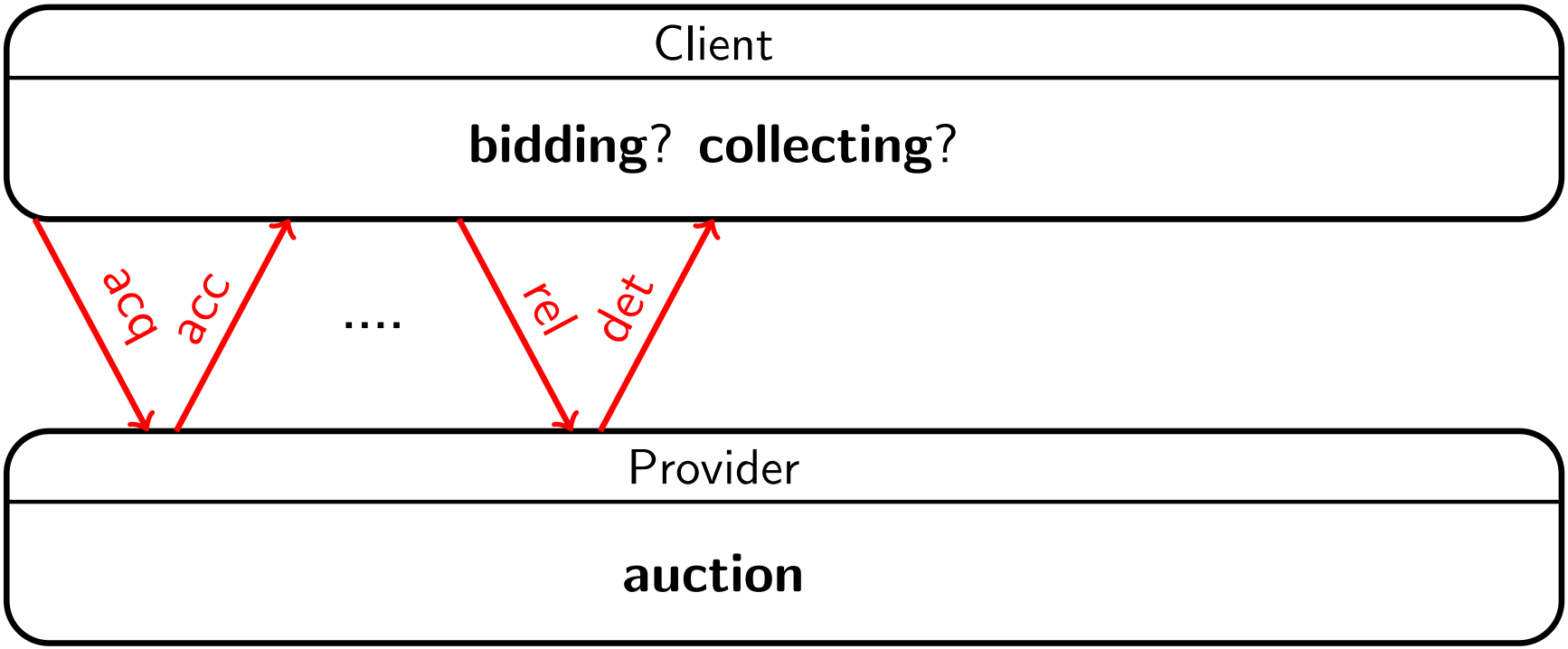
$\Gamma, a_S{:}\mathbf{bidding}; \Delta \vdash P''' :: (c_L{:}C_L)$



$\Gamma, a_S{:}\mathbf{collecting}; \Delta, a_L{:}\downarrow_L^S\mathbf{bidding} \vdash P'' :: (c_L{:}C_L)$



$\Gamma, a_S{:}\mathbf{collecting}, b_S{:}\mathbf{collecting}; \Delta, a_L{:}\downarrow_L^S\mathbf{bidding} \vdash Q :: (c_L{:}C_L)$



$\Gamma, a_S{:}\mathbf{bidding}, b_S{:}\mathbf{collecting}; \Delta \vdash Q' :: (c_L{:}C_L)$

One more problem...

One more problem...

- Γ is a structural context (shared channels can be aliased)

One more problem...

- Γ is a structural context (shared channels can be aliased)
- Malicious clients can store and reuse references to shared channels!

L-L Shifts

$$
\begin{aligned}
A_S &::= \uparrow_L^S A_L \\
A_L, B_L &::= 1 \mid A_L \otimes B_L \mid A_L \multimap B_L \mid \oplus\{\overline{I{:}A_L}\} \mid \&\{\overline{I{:}A_L}\} \\
&\quad \mid A_L \wedge B_L \mid A_L \supset B_L \mid \downarrow_L^S A_S
\end{aligned}
$$

L-L Shifts

$$
\begin{aligned}
A_S &::= \uparrow^S_L A_L \\
A_L, B_L &::= 1 \mid A_L \otimes B_L \mid A_L \multimap B_L \mid \oplus\{\overline{I{:}A_L}\} \mid \&\{\overline{I{:}A_L}\} \\
&\quad \mid A_L \wedge B_L \mid A_L \supset B_L \mid \downarrow^S_L A_S \mid \downarrow^L_L A_L \mid \uparrow^L_L A_L
\end{aligned}
$$

Additional Subtyping Rules

$$\frac{A_L \leq B_L}{\uparrow^L_L A_L \leq \uparrow^L_L B_L} \leq_{\uparrow^L_L} \qquad \frac{A_L \leq B_L}{\downarrow^L_L A_L \leq \downarrow^L_L B_L} \leq_{\downarrow^L_L}$$

Additional Subtyping Rules

$$\frac{A_L \leq B_L}{\uparrow^L_L A_L \leq \uparrow^L_L B_L} \leq_{\uparrow^L_L} \qquad \frac{A_L \leq B_L}{\downarrow^L_L A_L \leq \downarrow^L_L B_L} \leq_{\downarrow^L_L}$$

$$\frac{A_L \leq B_L}{\uparrow^S_L A_L \leq \uparrow^L_L B_L} \leq_{\uparrow^S_L \uparrow^L_L} \qquad \frac{A_S \leq B_L}{\downarrow^S_L A_S \leq \downarrow^L_L B_L} \leq_{\downarrow^S_L \downarrow^L_L}$$

Auction with Phases

$$\mathbf{auction} \leq \mathbf{bidding}$$

$$\mathbf{auction} \leq \mathbf{collecting}$$

$$\text{provider} \begin{cases} \mathbf{auction} = \uparrow^{S}_{L} \& \{ \mathit{bid} : \oplus \{ \mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow^{S}_{L} \mathbf{auction}, \\ \qquad\qquad \mathit{collecting} : \downarrow^{S}_{L} \mathbf{auction} \}, \\ \qquad \mathit{collect} : \mathsf{id} \supset \oplus \{ \mathit{prize} : \mathsf{item} \wedge \downarrow^{S}_{L} \mathbf{auction}, \\ \qquad\qquad \mathit{refund} : \mathsf{money} \wedge \downarrow^{S}_{L} \mathbf{auction}, \\ \qquad\qquad \mathit{bidding} : \downarrow^{S}_{L} \mathbf{auction} \} \} \end{cases}$$

$$\text{clients} \begin{cases} \mathbf{bidding} = \uparrow^{L}_{L} \& \{ \mathit{bid} : \oplus \{ \mathit{ok} : \mathsf{id} \supset \mathsf{money} \supset \downarrow^{L}_{L} \mathbf{bidding}, \\ \qquad\qquad \mathit{collecting} : \downarrow^{L}_{L} \mathbf{collecting} \} \} \\ \mathbf{collecting} = \uparrow^{L}_{L} \& \{ \mathit{collect} : \mathsf{id} \supset \oplus \{ \mathit{prize} : \mathsf{item} \wedge \downarrow^{L}_{L} \mathbf{bidding}, \\ \qquad\qquad \mathit{refund} : \mathsf{money} \wedge \downarrow^{L}_{L} \mathbf{bidding}, \\ \qquad\qquad \mathit{bidding} : \downarrow^{L}_{L} \mathbf{bidding} \} \} \end{cases}$$

Conclusion

- Phases manifest at the type level
- Subtyping as a technical device

Conclusion

- Phases manifest at the type level
- Subtyping as a technical device
- Future work:
  - Phases for provider
  - Relation with MPST

Conclusion

- Phases manifest at the type level
- Subtyping as a technical device
- Future work:
  - Phases for provider
  - Relation with MPST
- Technical report (arXiv:2101.06249):
  - Progress and Preservation Theorems
  - Additional examples

Technical Results

- A proposal for subtyping across shared and linear modalities
- Proof that said subtyping is safe:
  - Progress
  - Preservation