

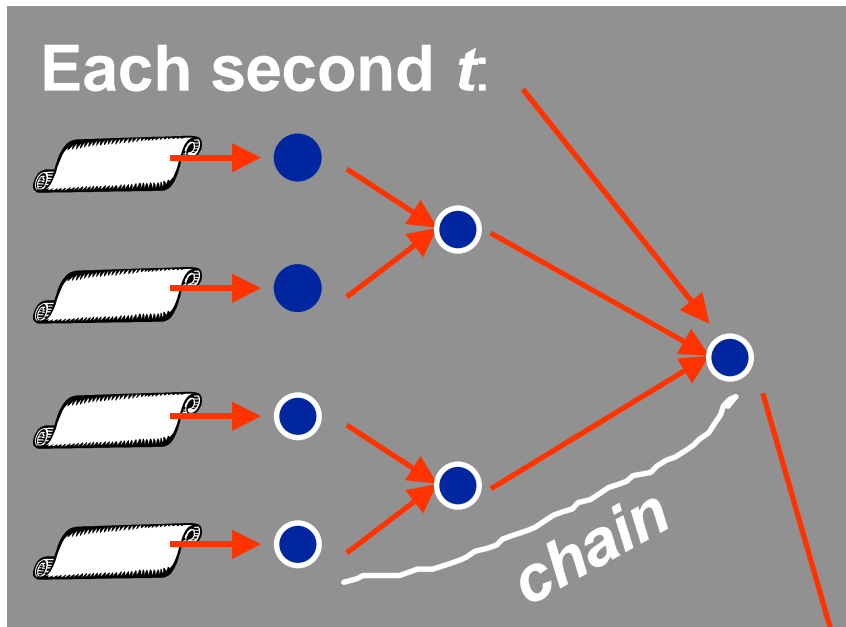
Outline



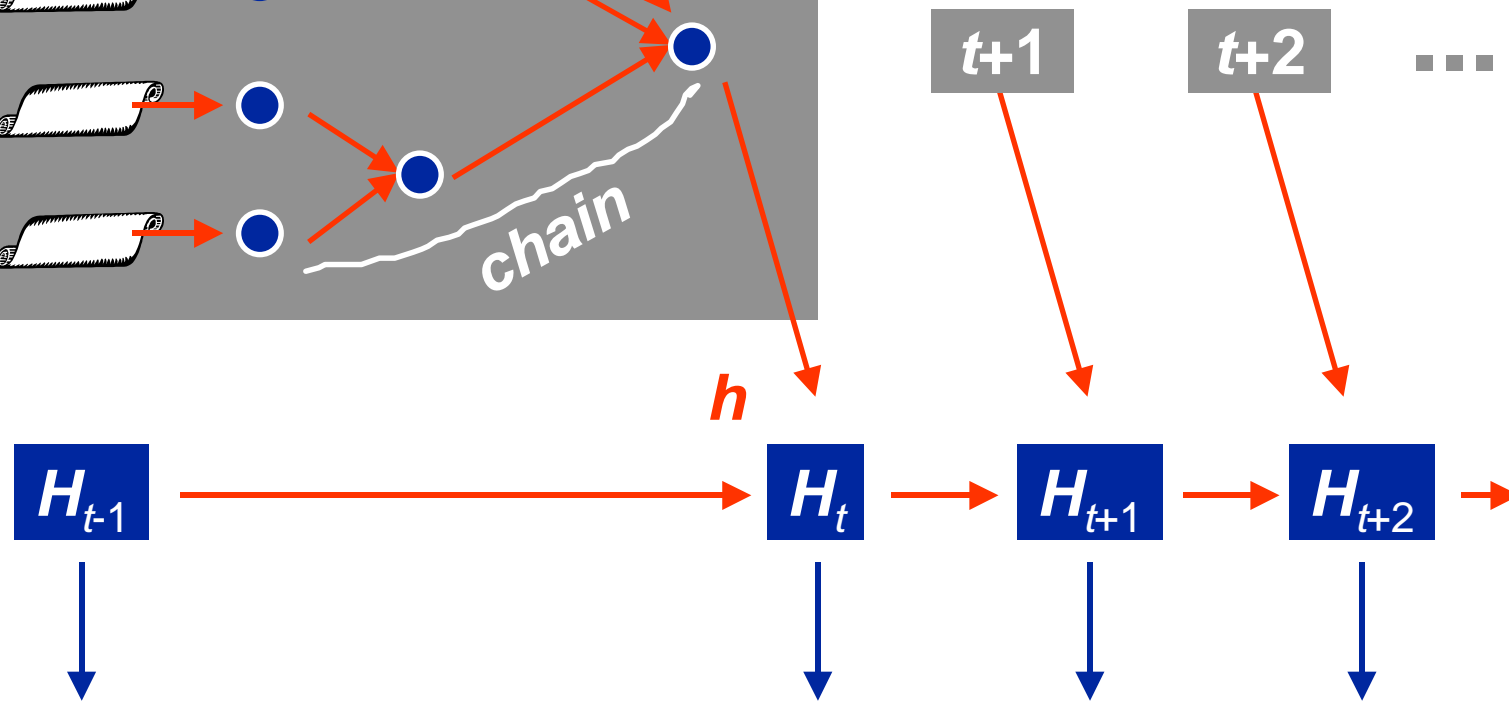
Notary services



Logical Time Stamps



h = collision-resistant one-way hash-function

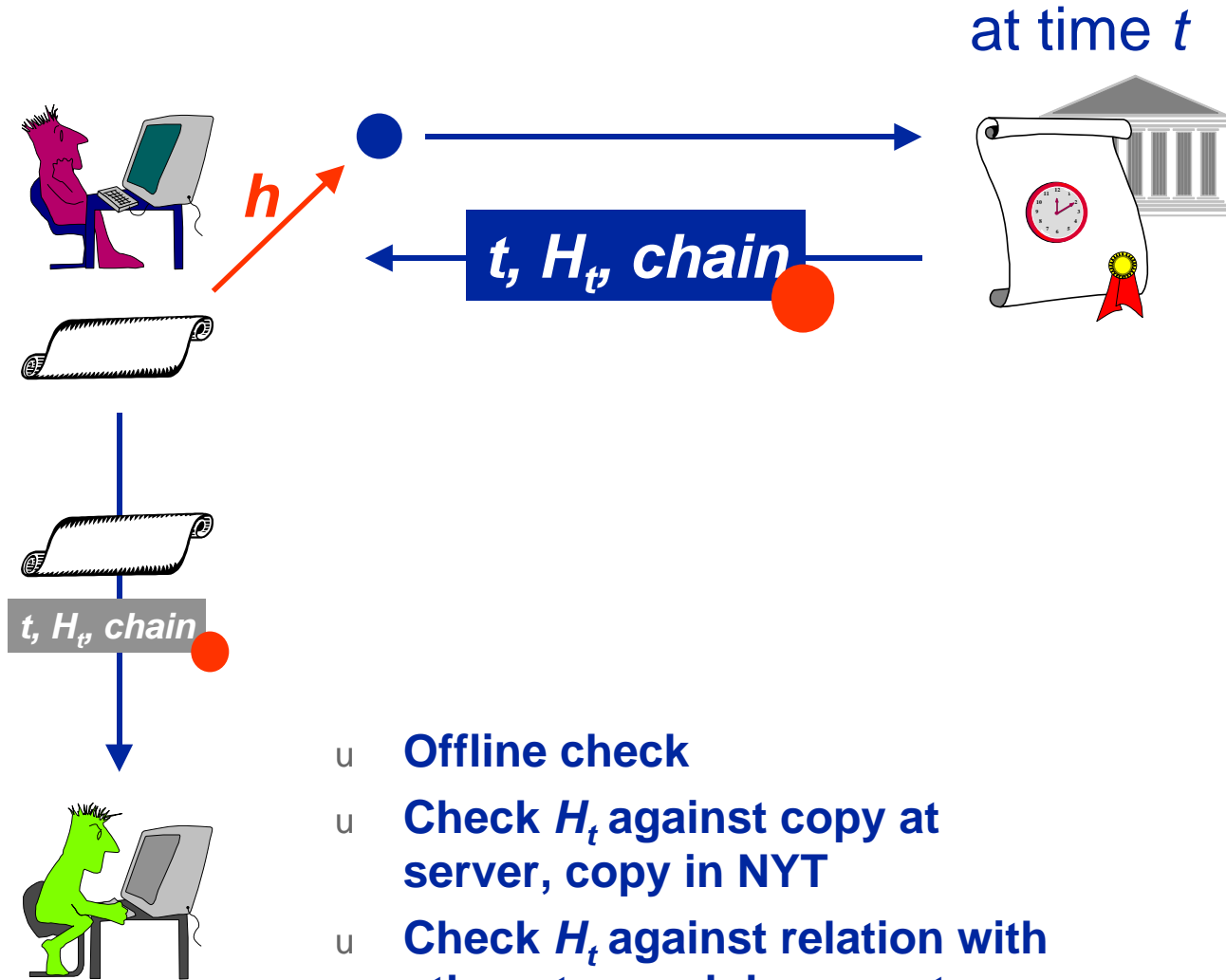


Recorded on server, published in NYT

Notary Services



Logical Time Stamps





Logical Time Stamps



- u Provides real time
- u Minimal trust in time stamping server
 - u Server cannot change order
 - u Network of servers can distribute trust
- u Only hash of documents are stamped
- u Efficient
 - u $\log(\#\text{docs})$ h/s



- u Online service
 - u Server potential bottleneck
 - u *but*: Network of time-stamping servers possible
- u “Eternity” problem



Fairness

- u **Fairness**

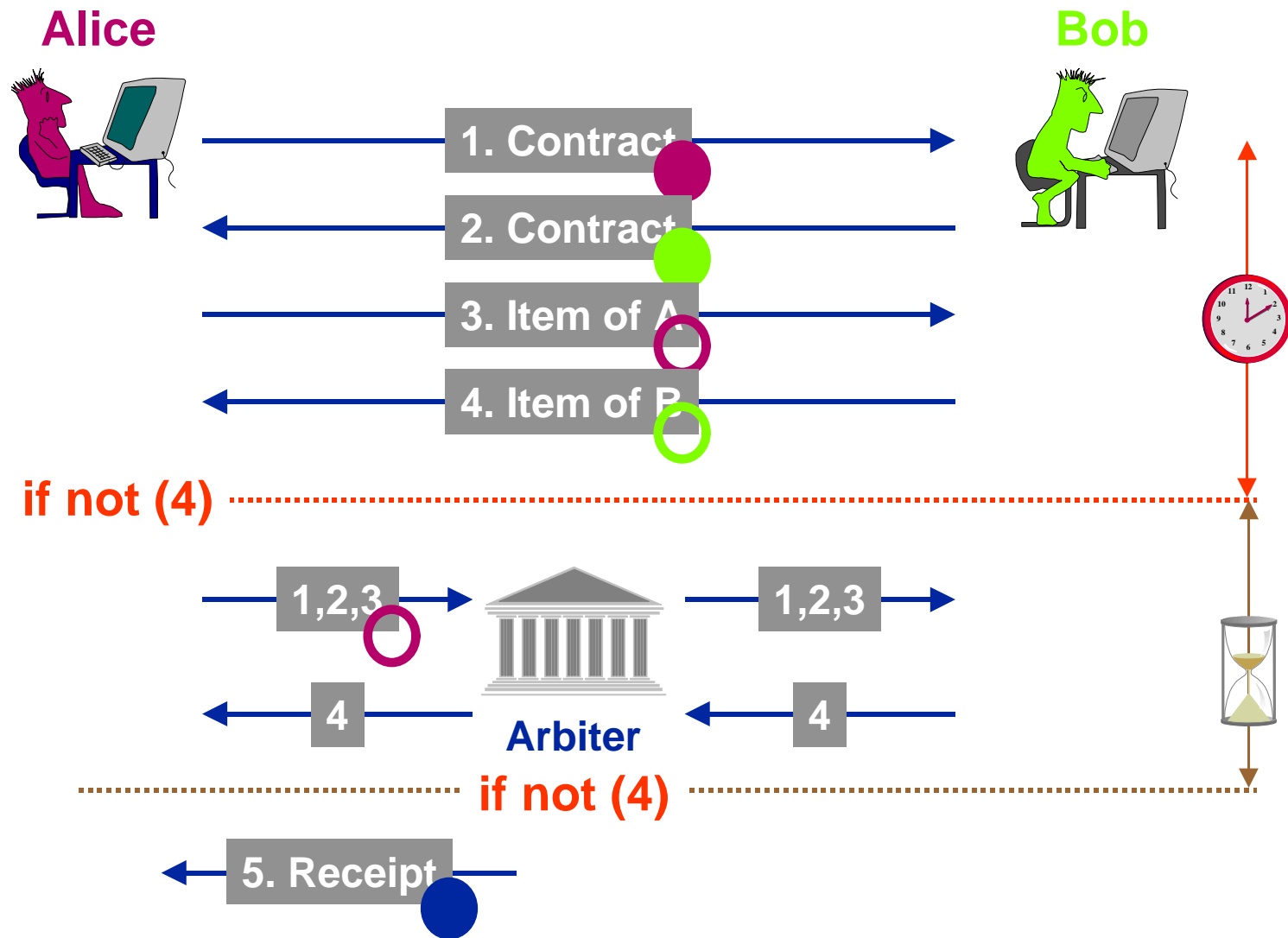
- u Non-repudiation of
 - u submission / delivery / receipt
- u Payment for
 - u receipt, online goods
- u Contract signing

- u **Objectives**

- u Minimize use of third party
- u Minimize use of expensive computations
- u Generic protocols that are independent of the items to be exchanged



Optimistic 2-Party Fair Exchange





Optimistic 2-Party Fair Exchange

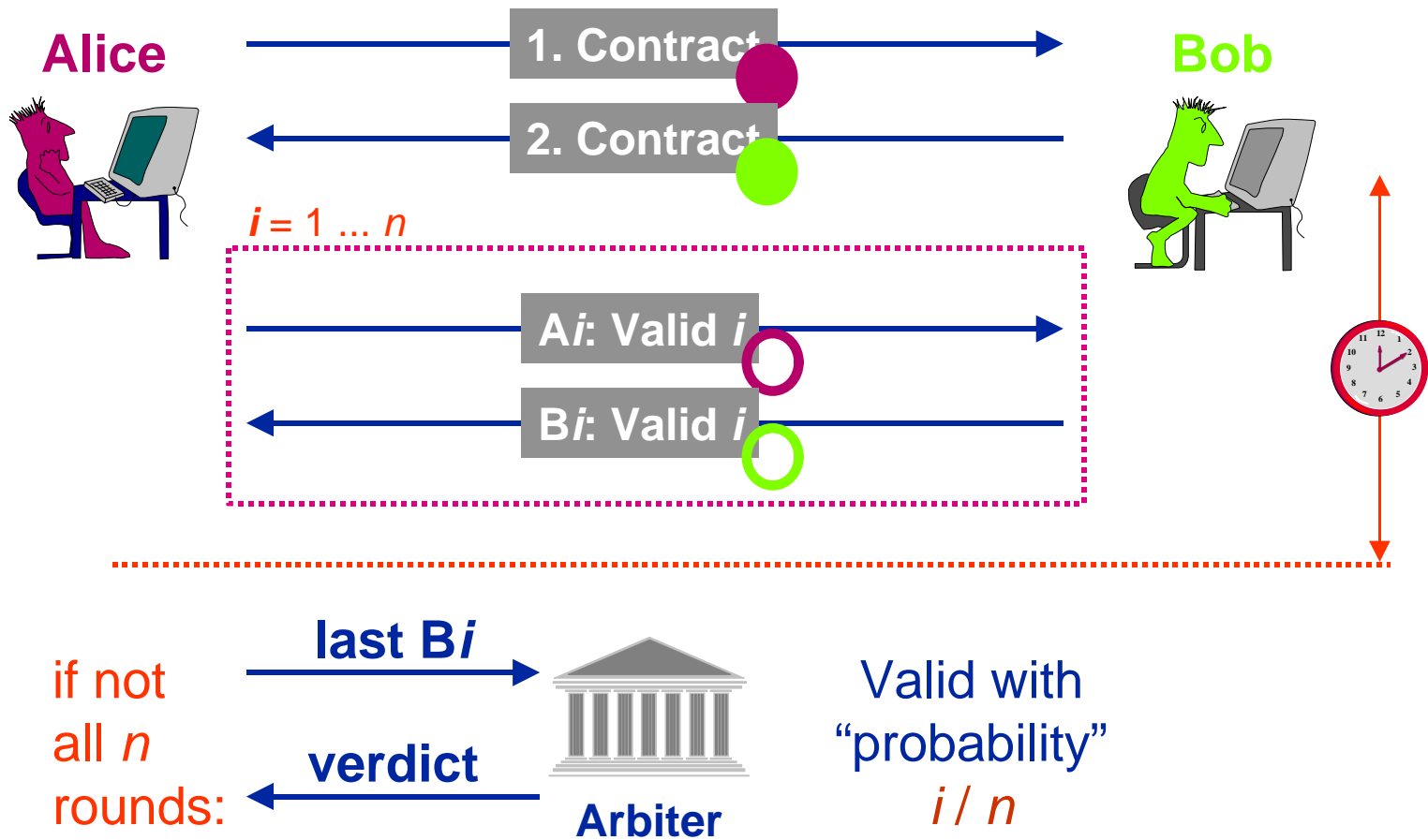


- u **Efficient in correct case**
 - u early termination
 - u 4 messages
 - u 2 signatures
 - u no 3rd party involved
- u **Generic approach**
 - u Non-repudiation of origin and receipt
 - u Contract signing
 - u Payment for receipt
 - u Fair purchase



- u **Weak fairness for Alice**
 - u “Receipt by arbiter”
not always sufficient
- u **Reliable communication with arbiter**
- u **Late final termination**

Contract Signing “w/o Third Party”





Contract Signing “w/o Third Party”



- u Small disadvantage might be acceptable



- u Specific for contracts
- u Many messages
- u Third party still needed
- u Late final termination