

Tehnologija veriženja blokov

Infosec seminar, Ljubljana 26.10.2018

Tadej Hren, SI-CERT Arnes

Zgostitveni algoritmi (hash)

`# ("abcdef")=54187745`

`# ("abcdeF")=69841542`

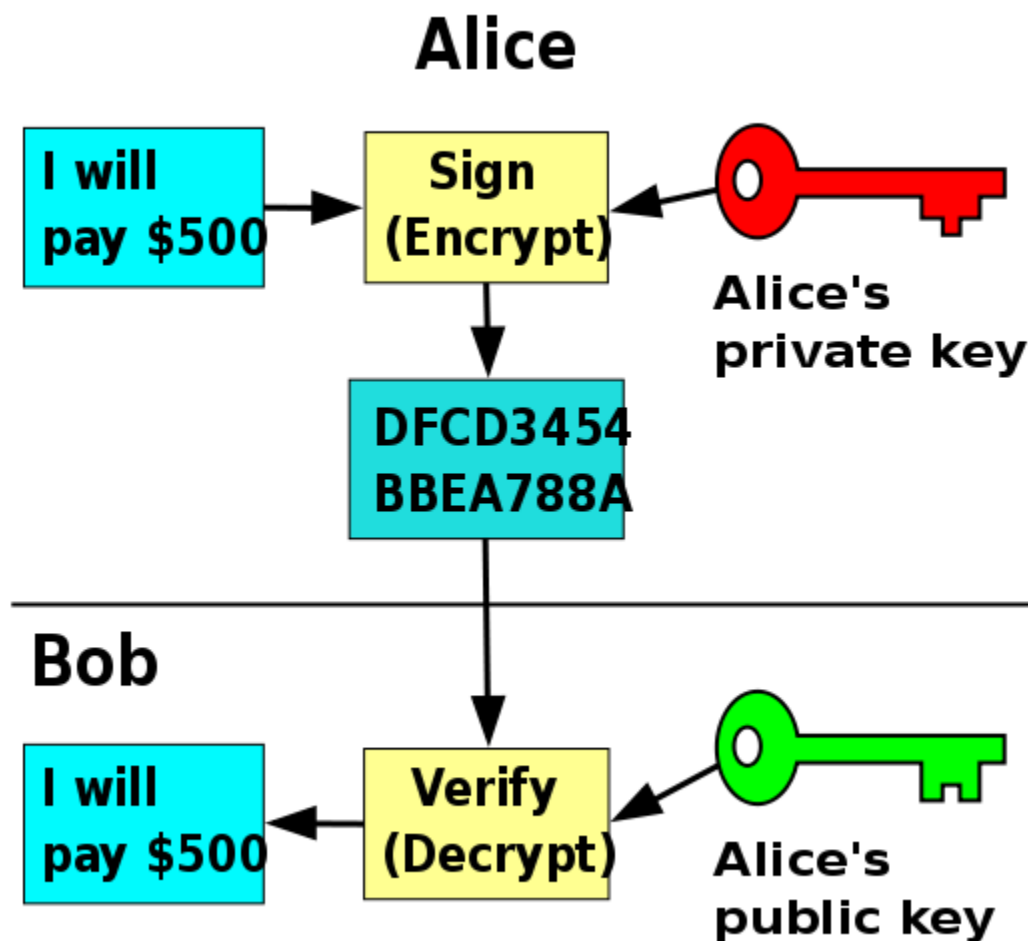
`# ("Infosek seminar")=12570001`

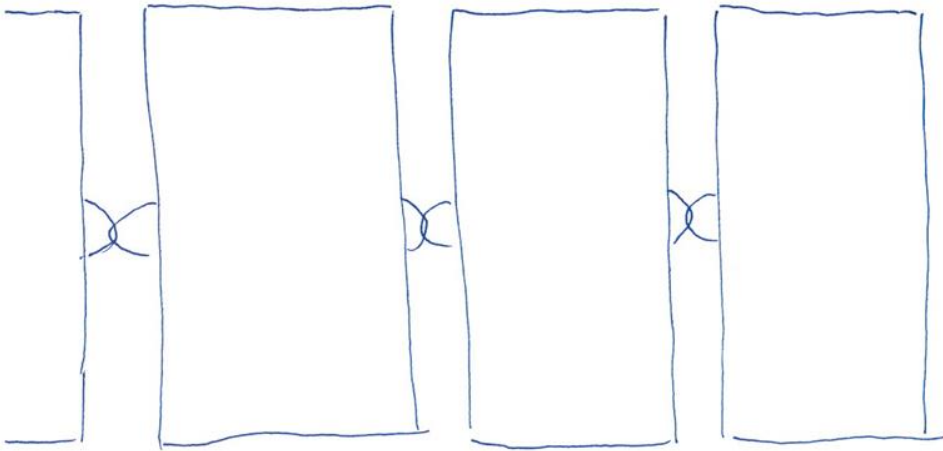
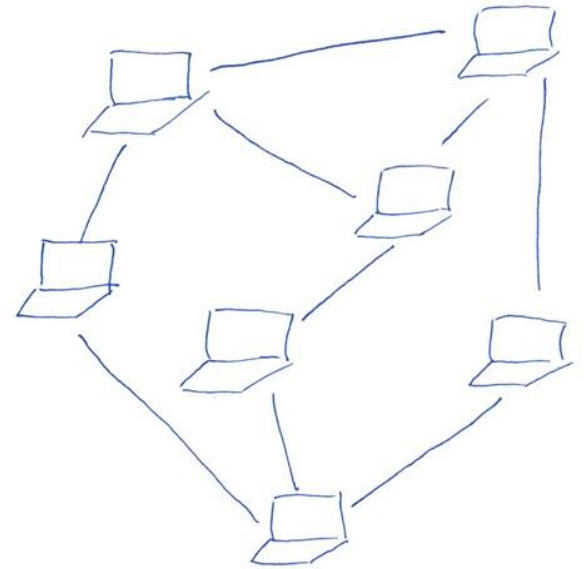
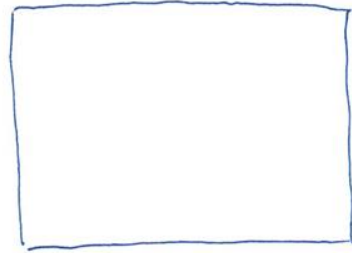
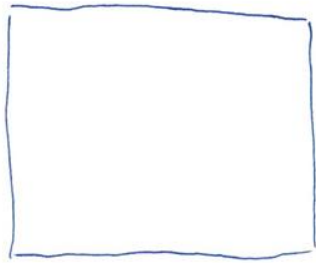
`# ("a")=22547845`

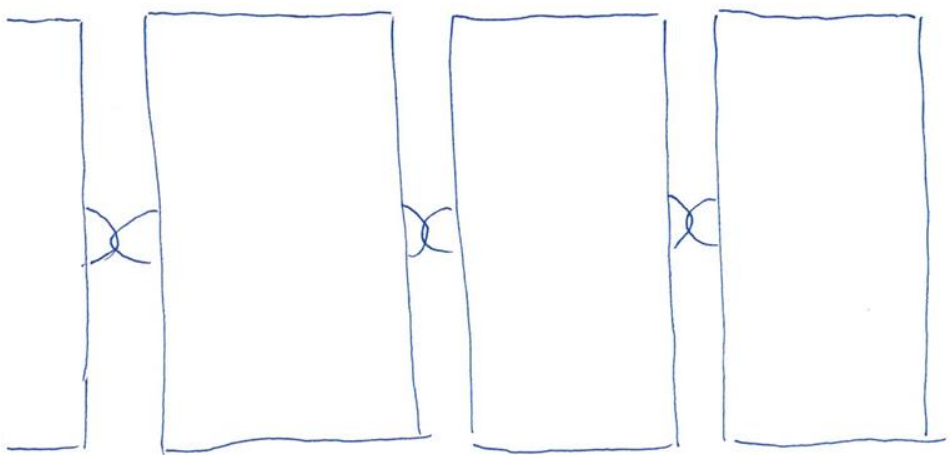
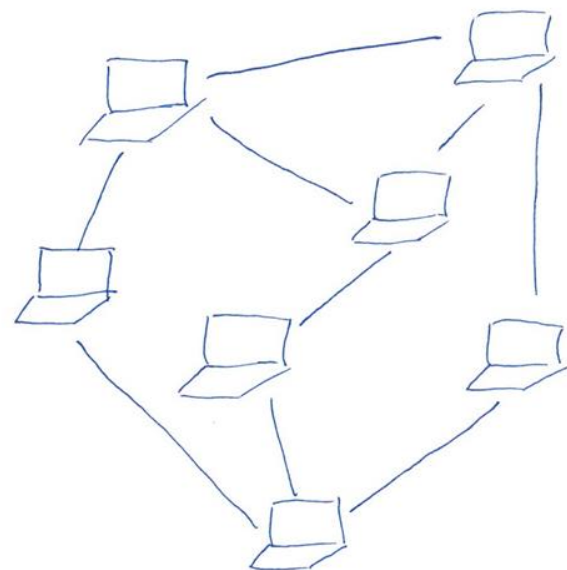
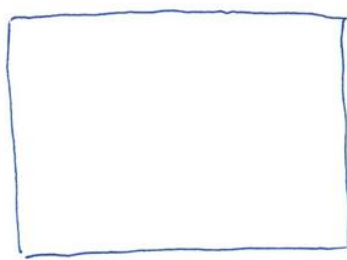
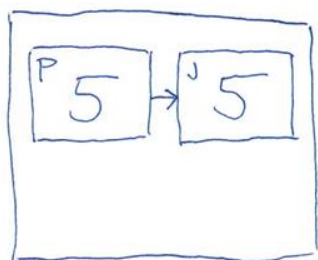
`sha256 ("Hello, world")=`

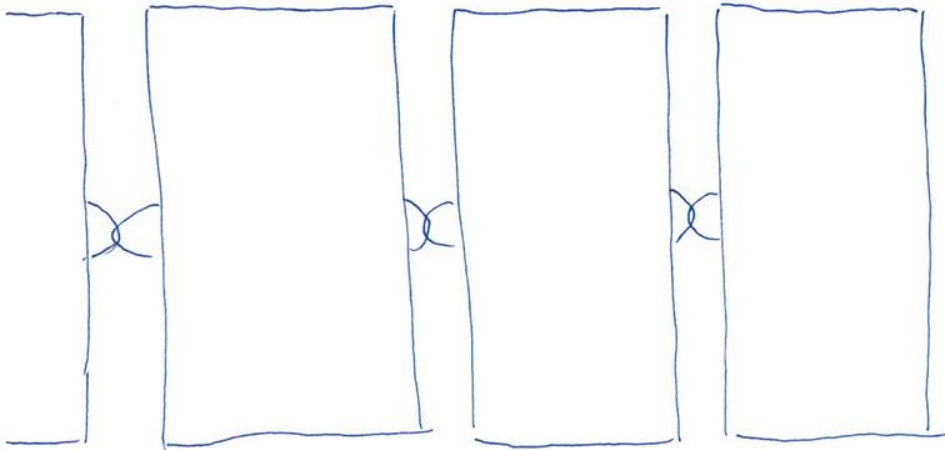
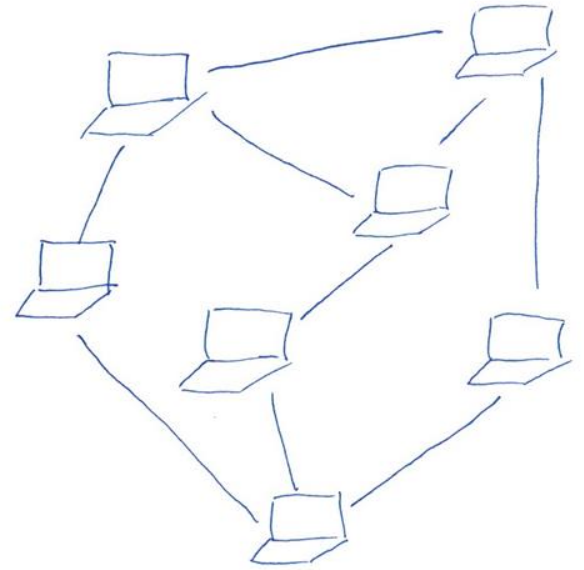
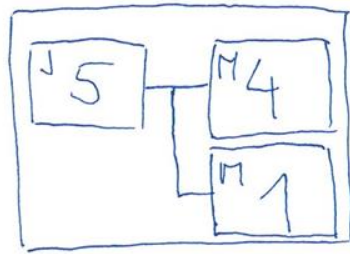
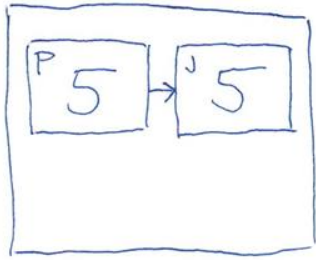
`4AE7C3B6AC0BEFF671EFA8CF57386151C06E58CA53
A78D83F36107316CEC125F`

Asimetrična kriptografija z javnim ključem

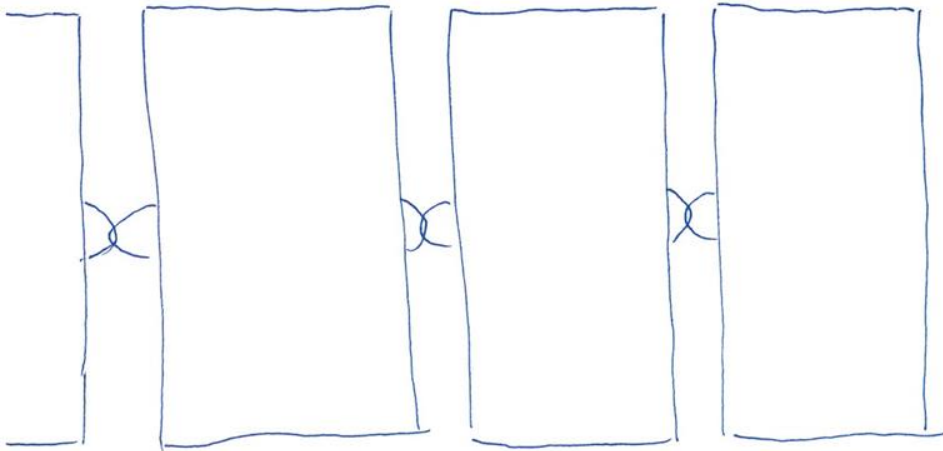
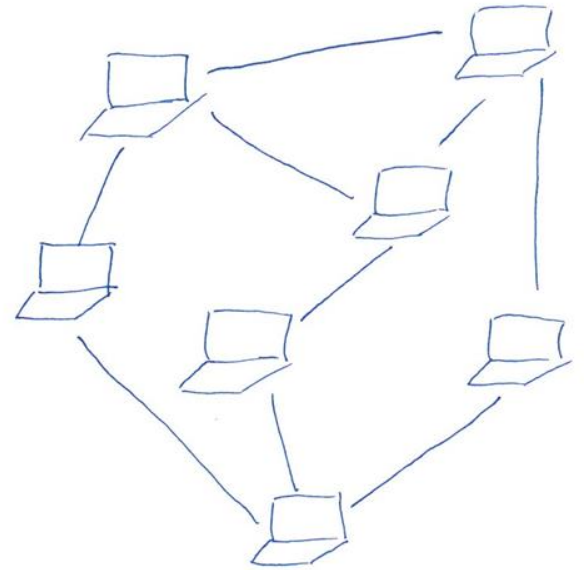
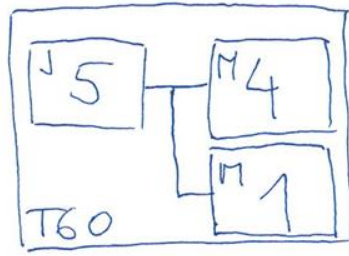
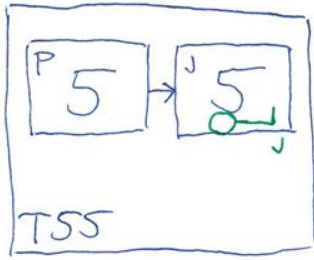


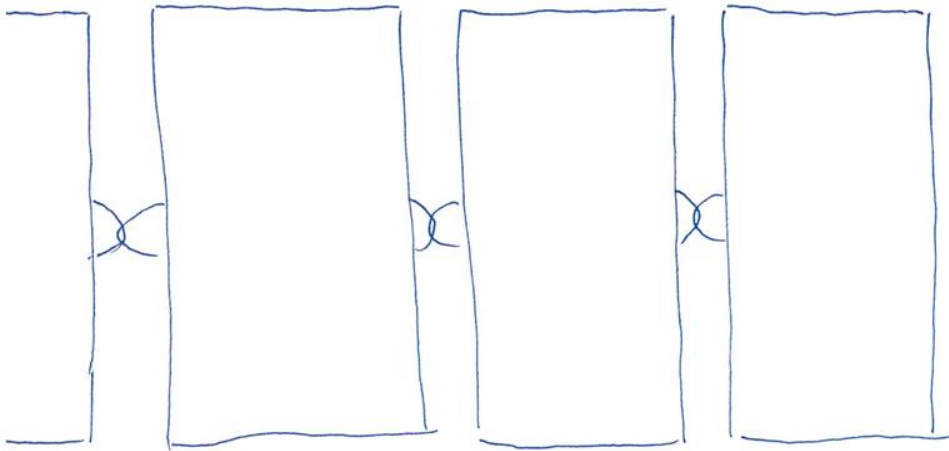
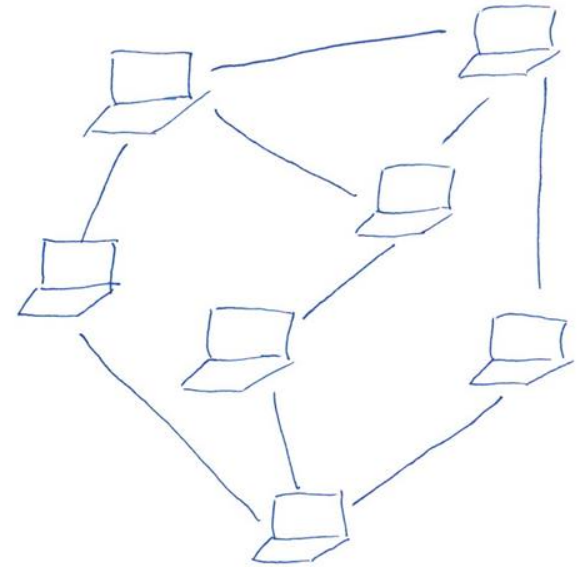
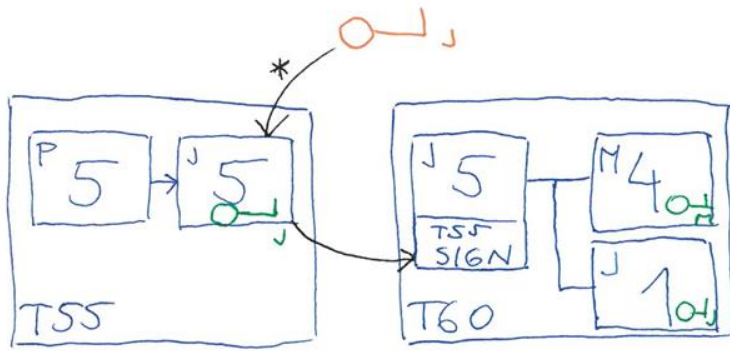


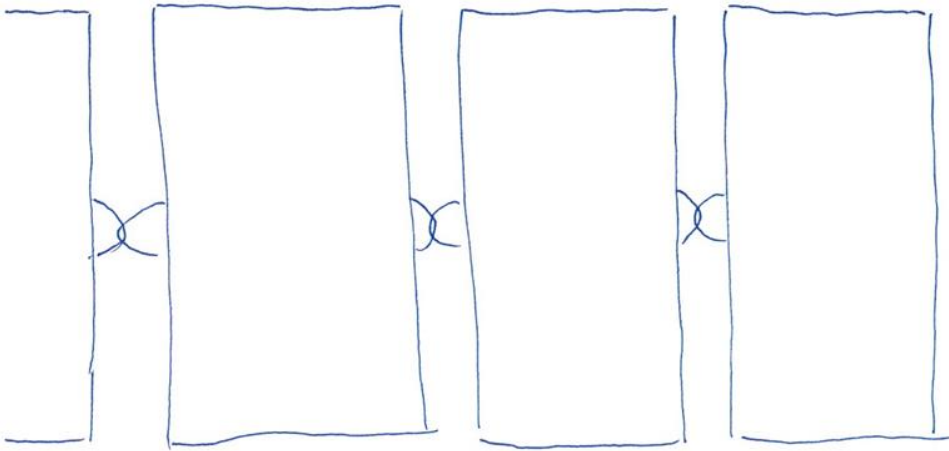
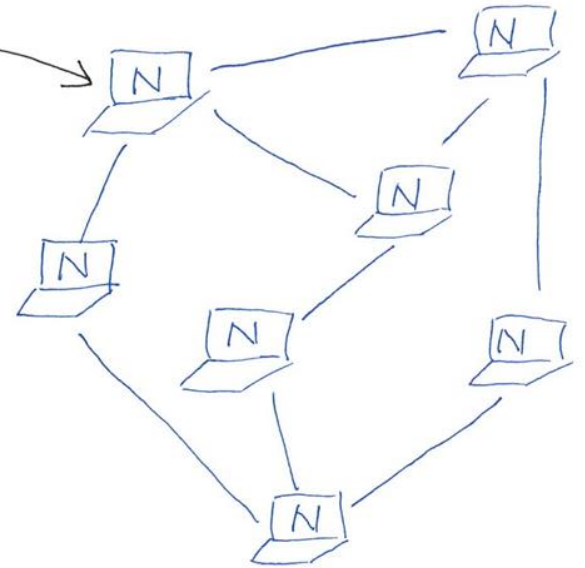
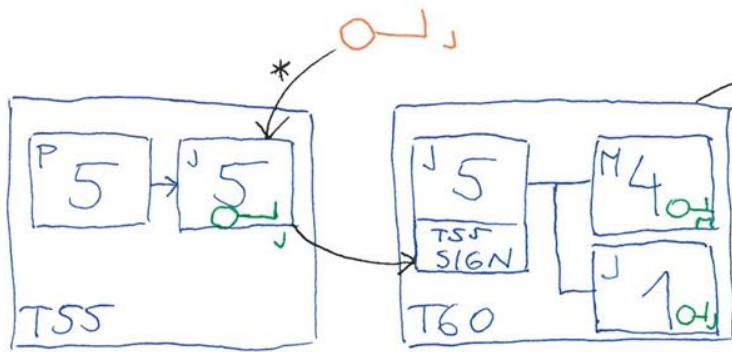


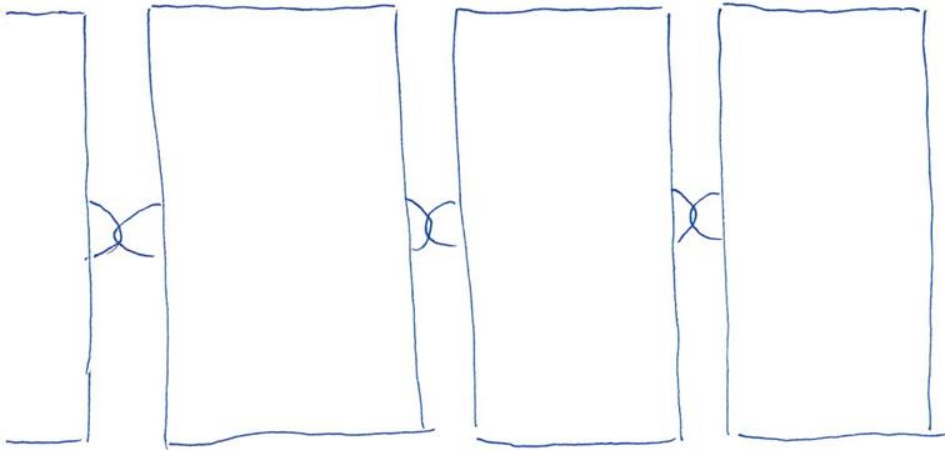
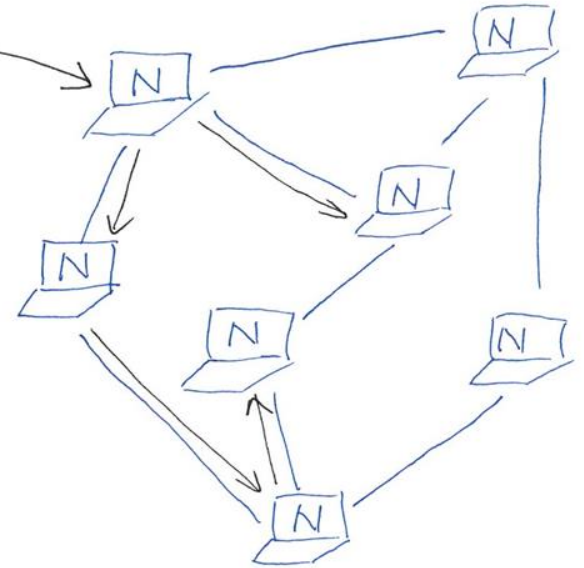
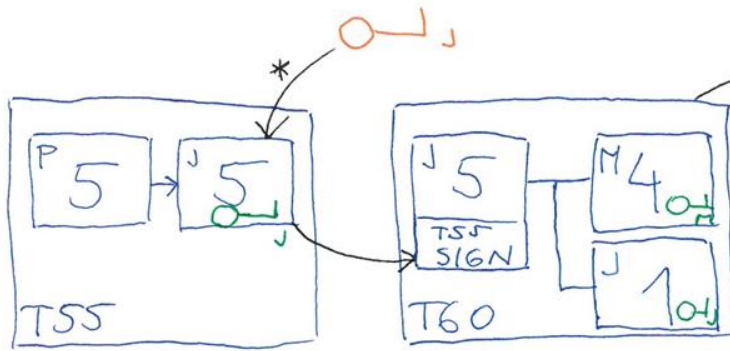


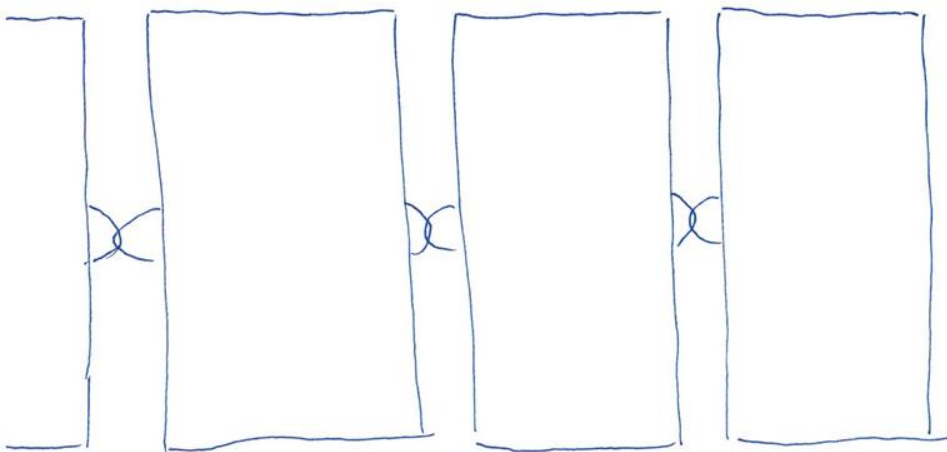
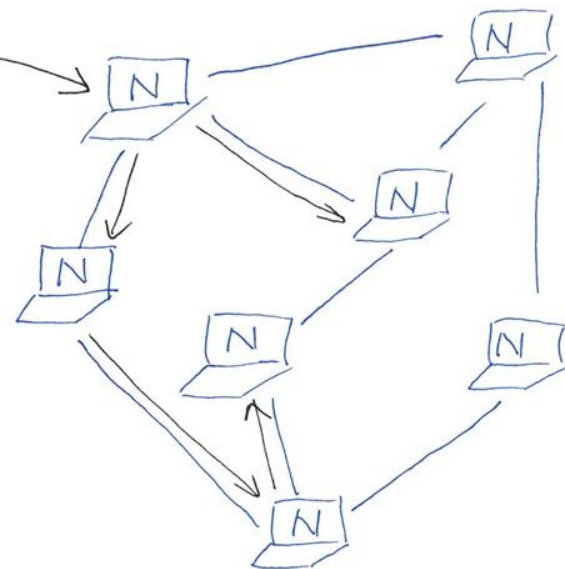
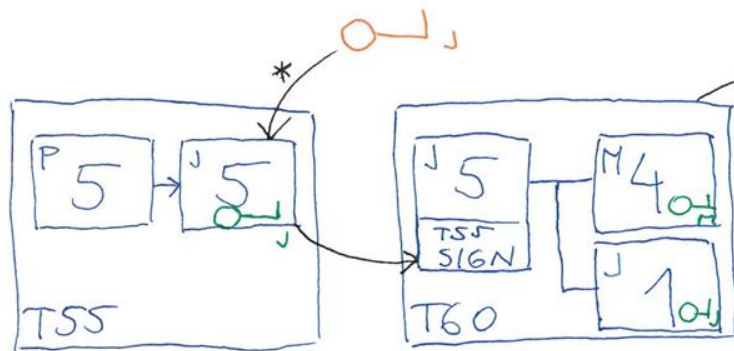
0.1

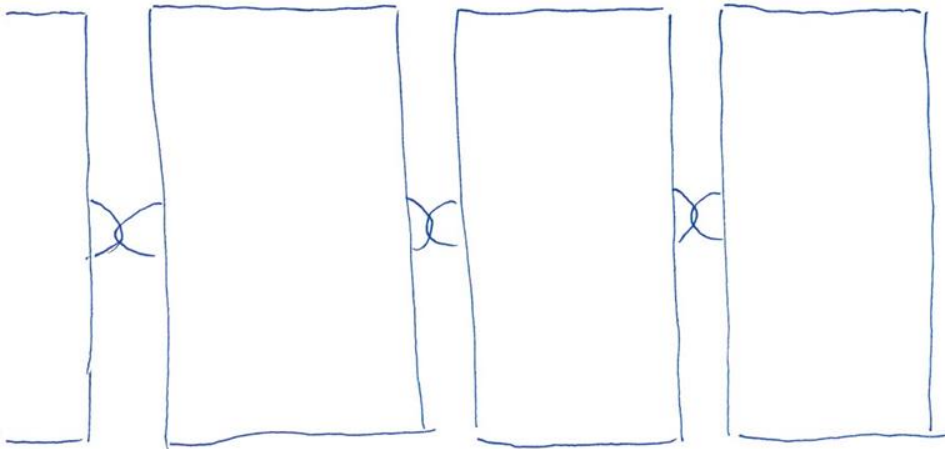
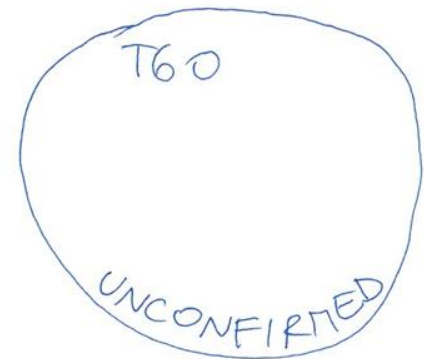
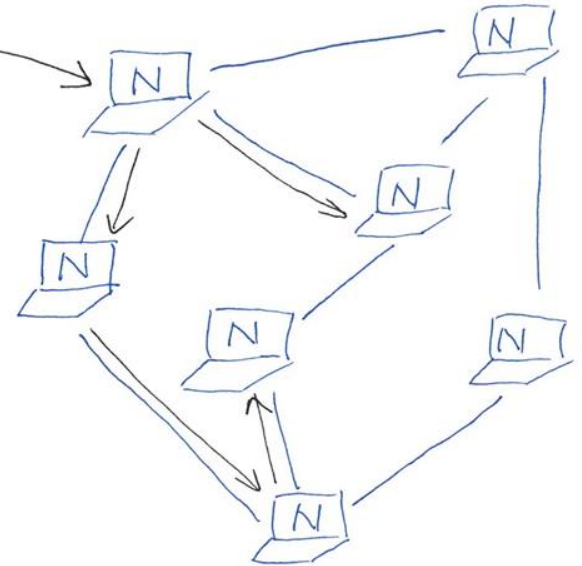
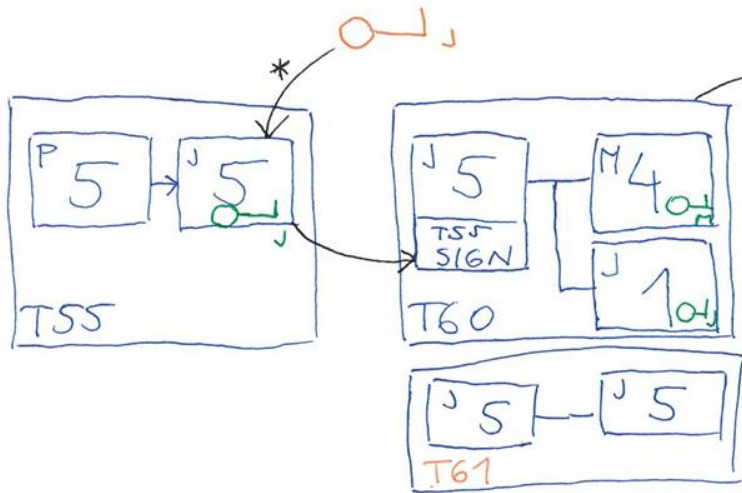


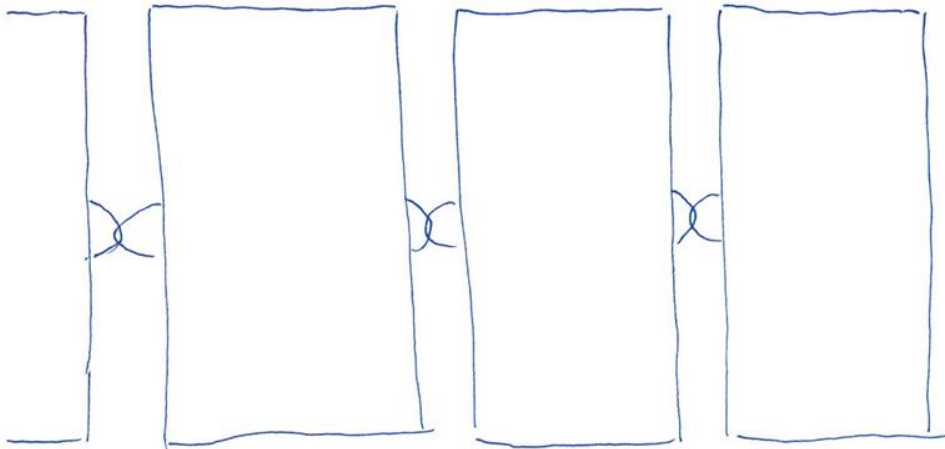
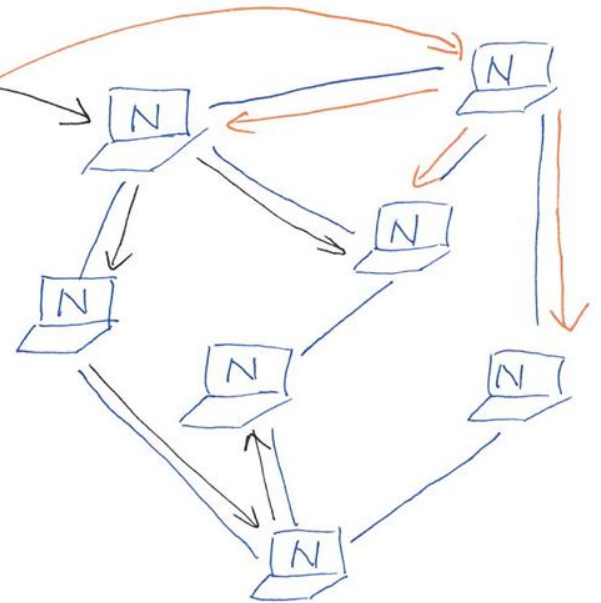
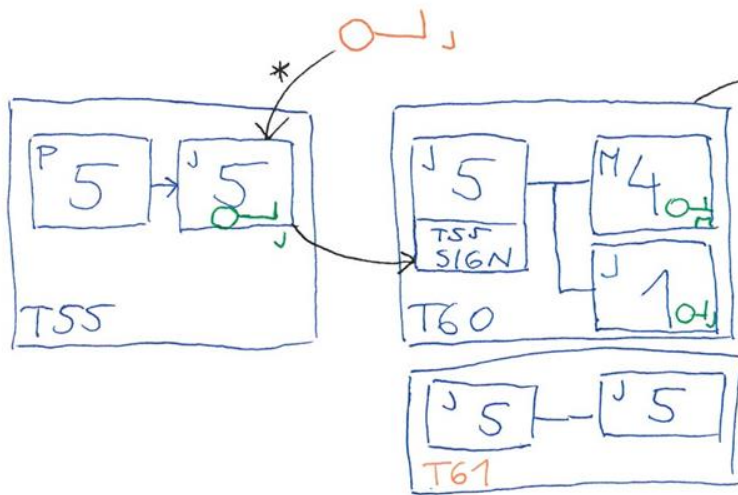


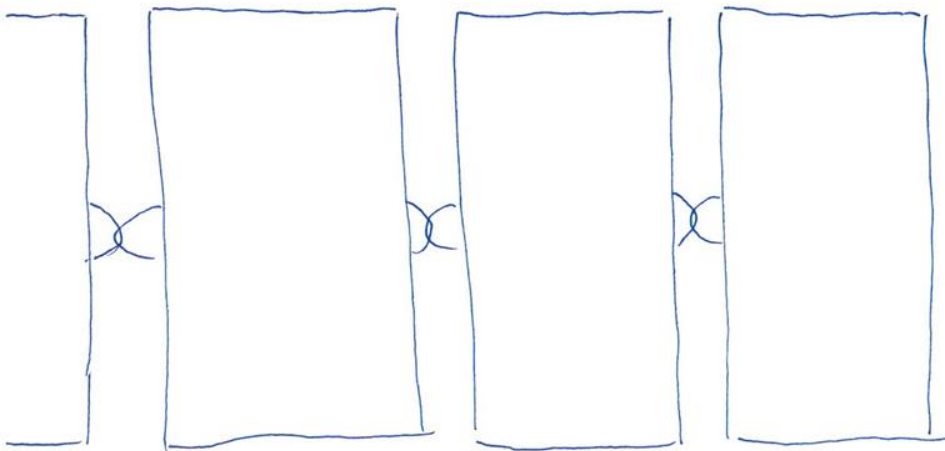
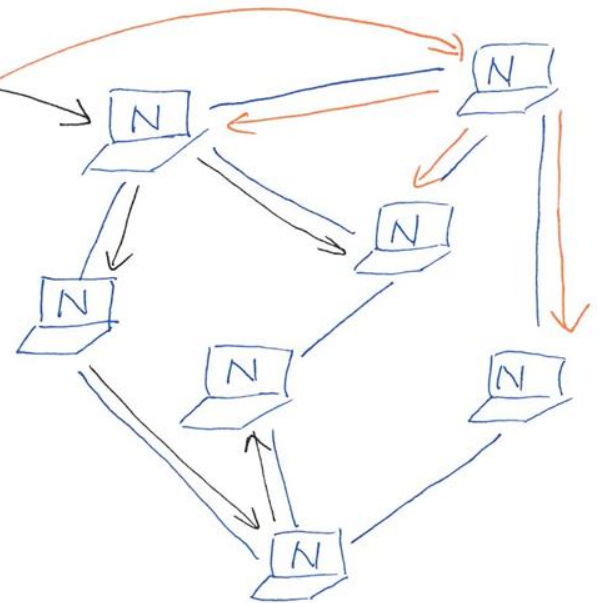
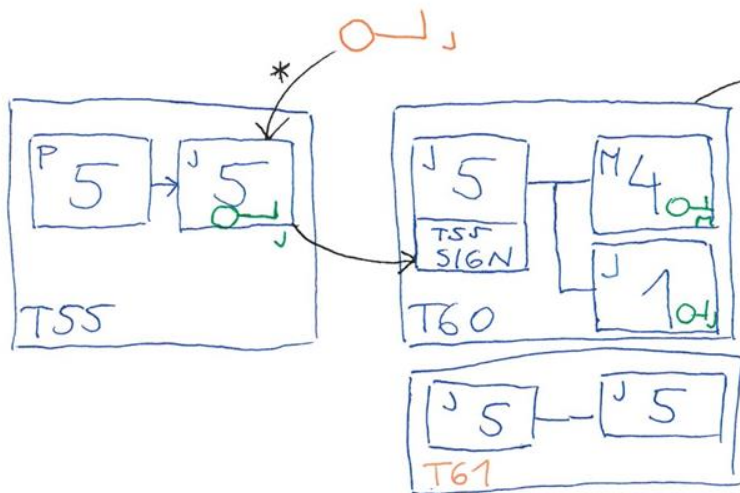


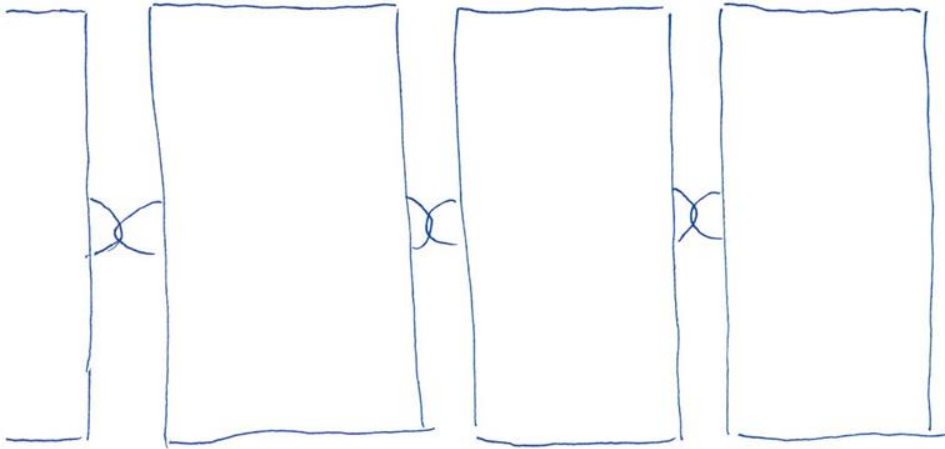
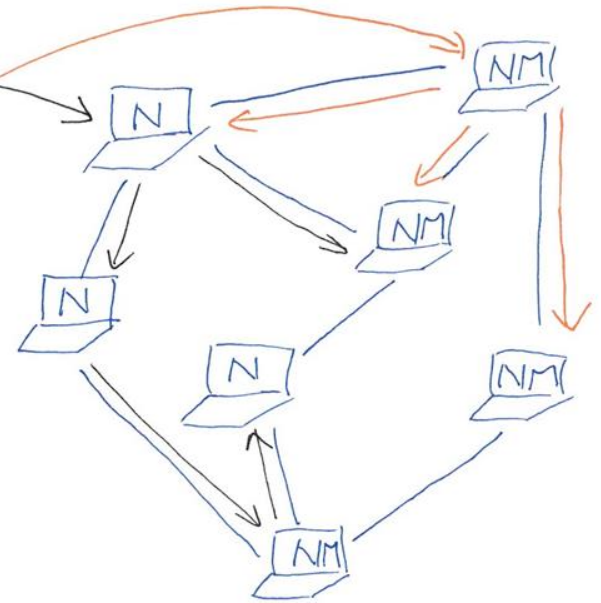
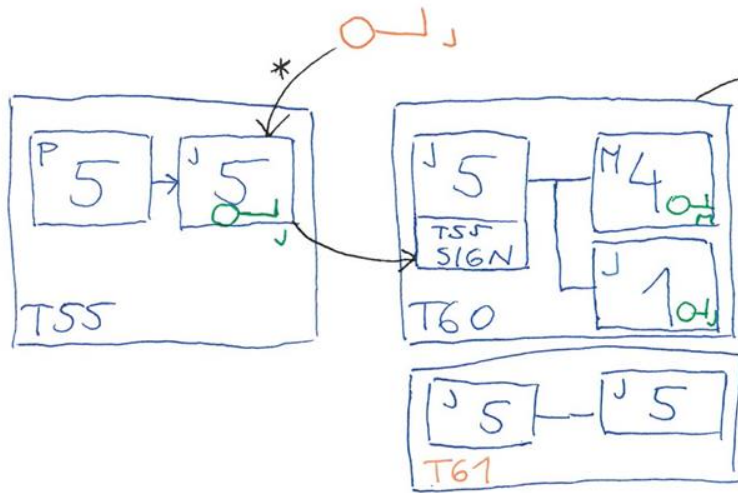


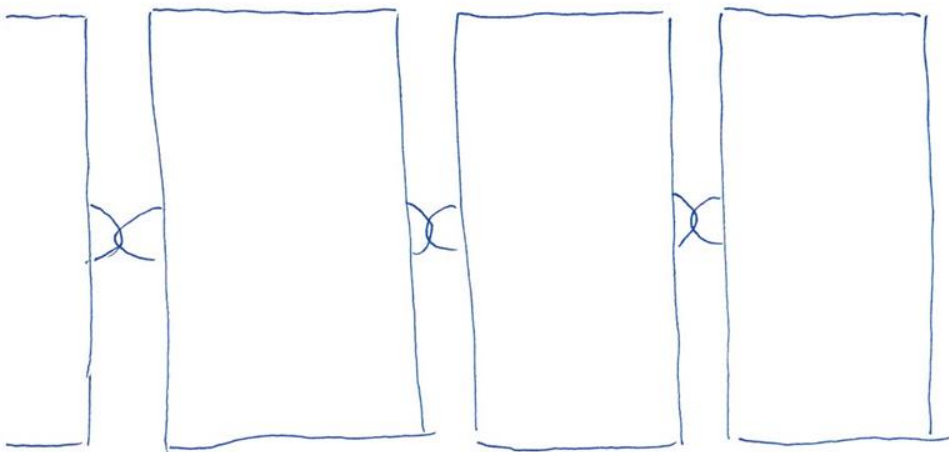
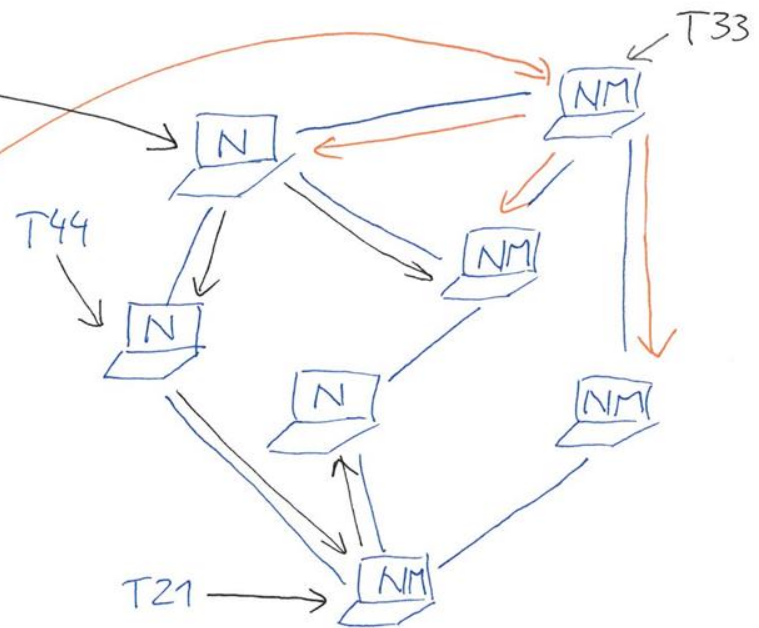
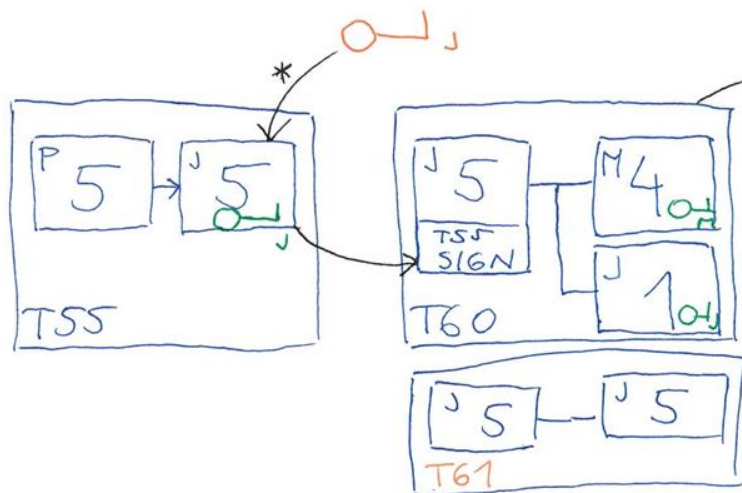












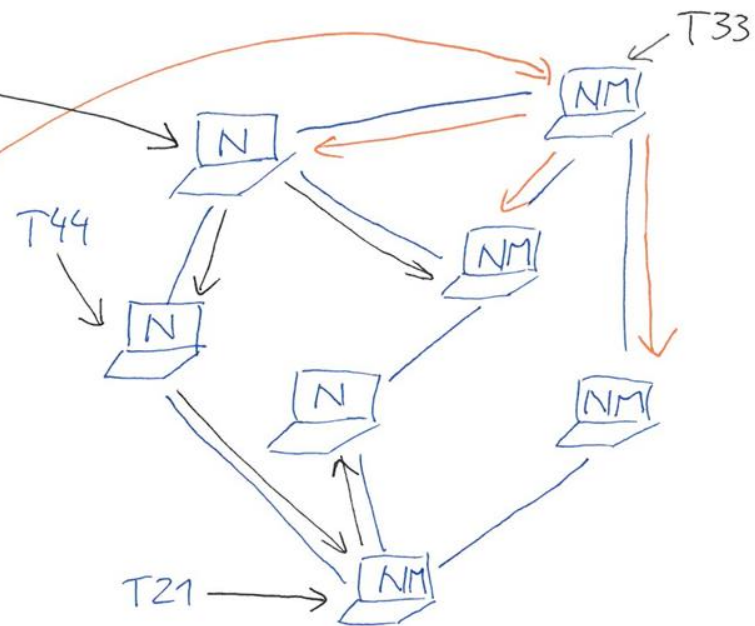


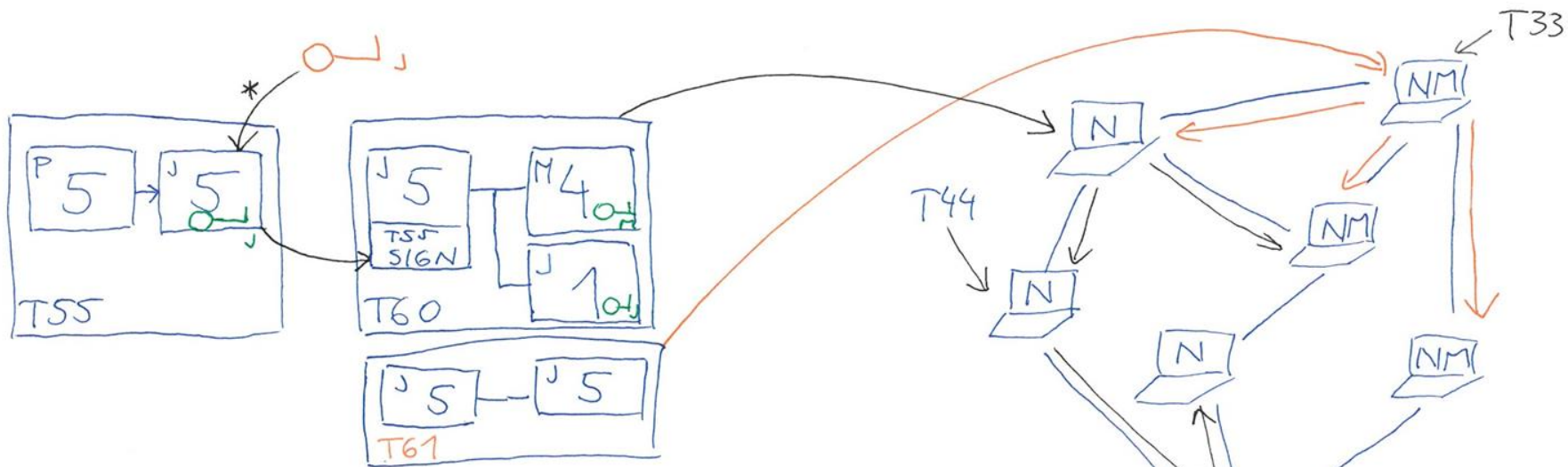
Diagram illustrating a linked list structure with three nodes (B108, B109, B110) and a pointer field labeled #.

The nodes are connected sequentially, with each node containing a pointer field (indicated by a bracket labeled #).

The pointer field for node B110 points to a structure containing the following elements:

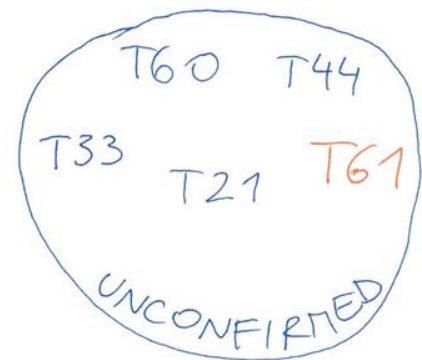
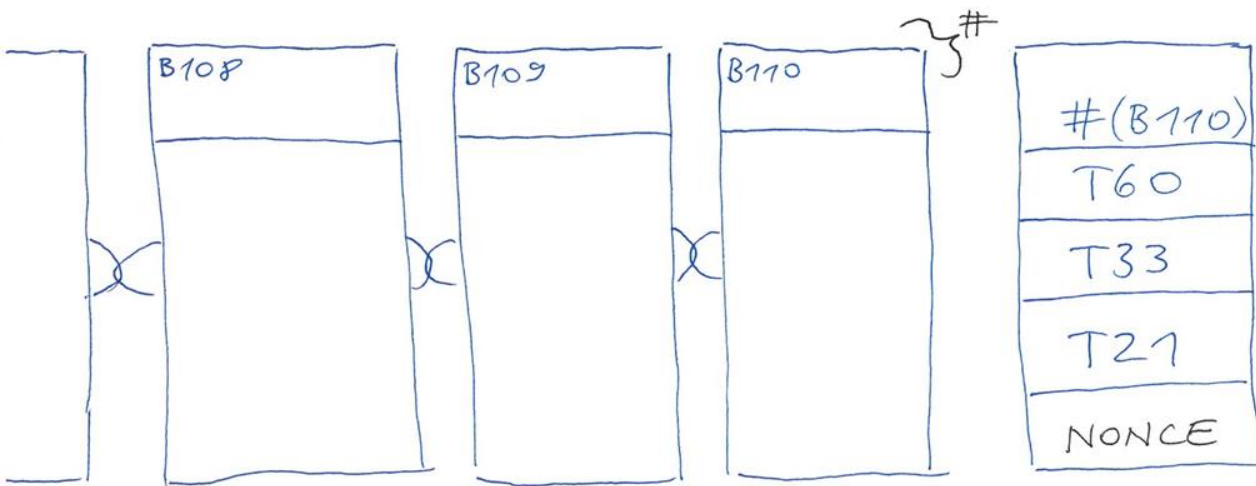
- #(B110)
- T60
- T33
- T21

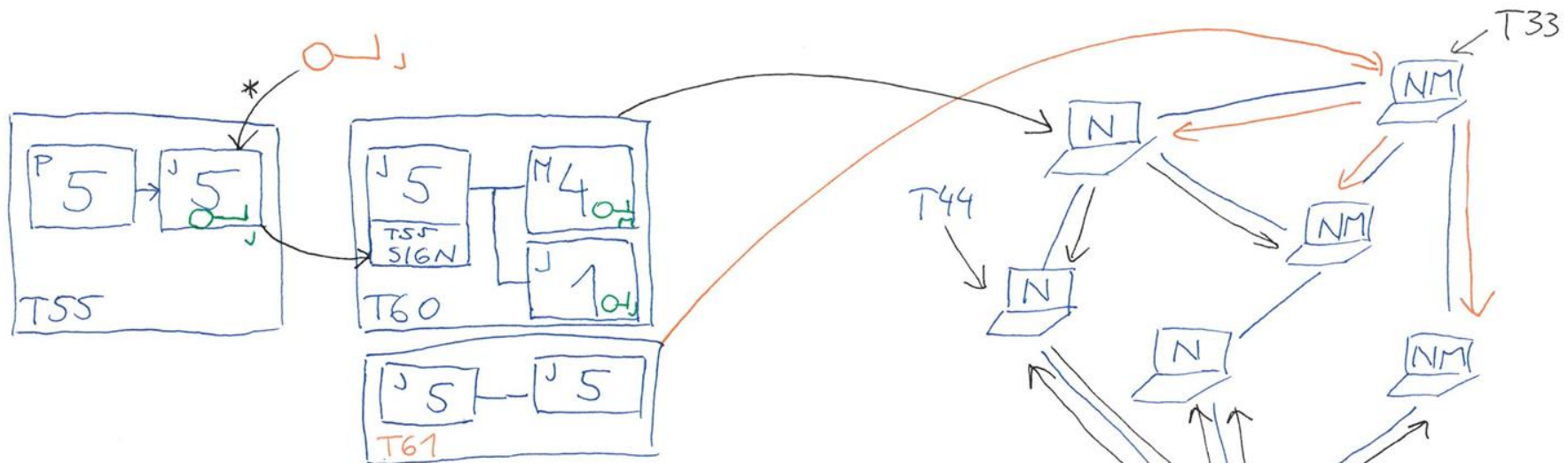




TRANSAKCIJE

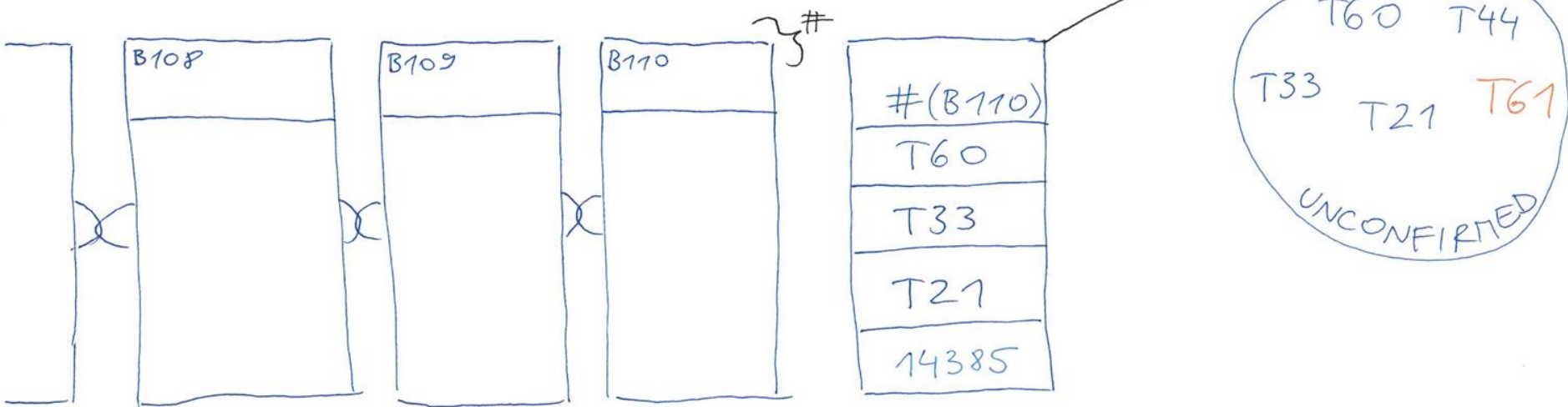
BLOKI

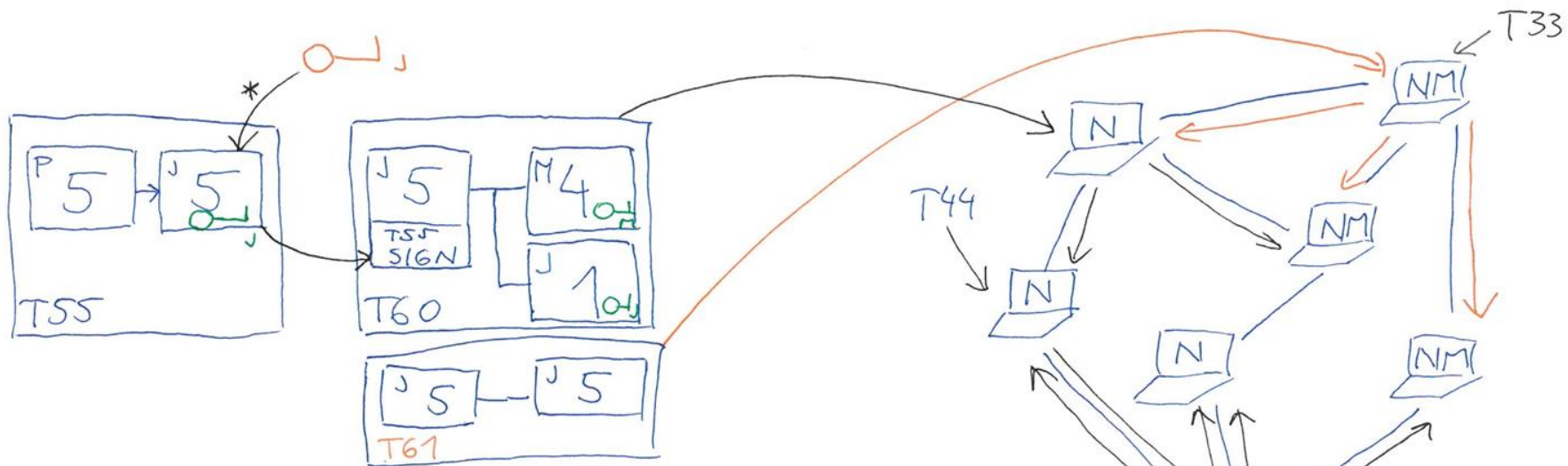




TRANSAKCIJE

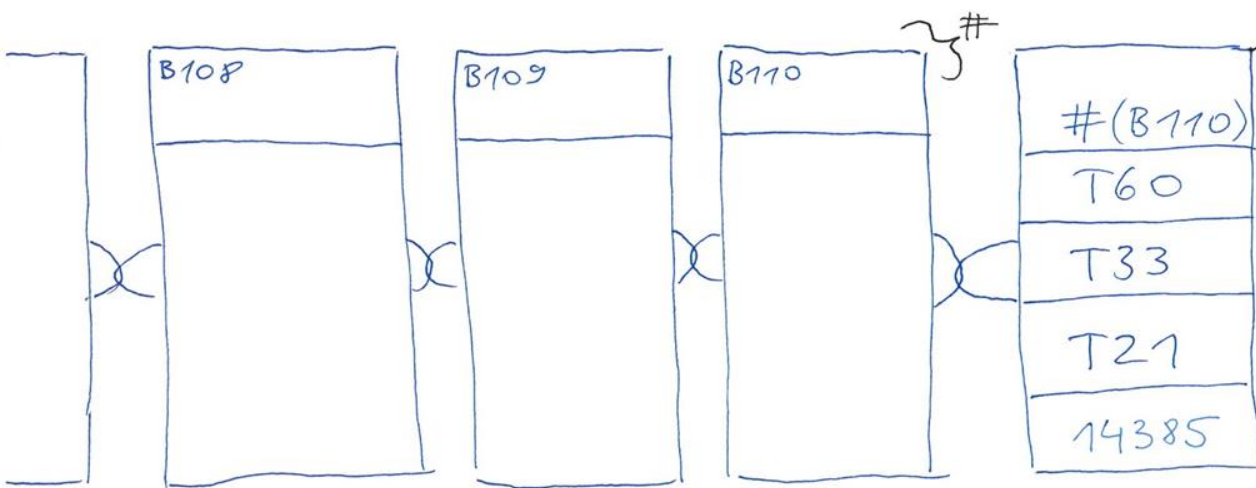
BLOKI

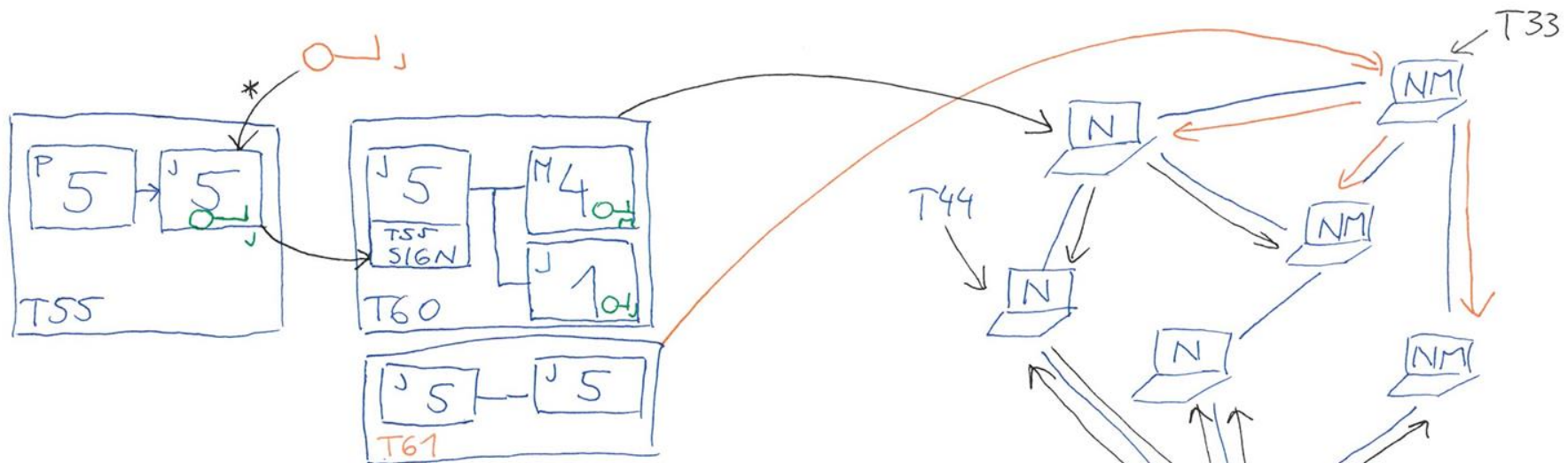




TRANSAKCIJE

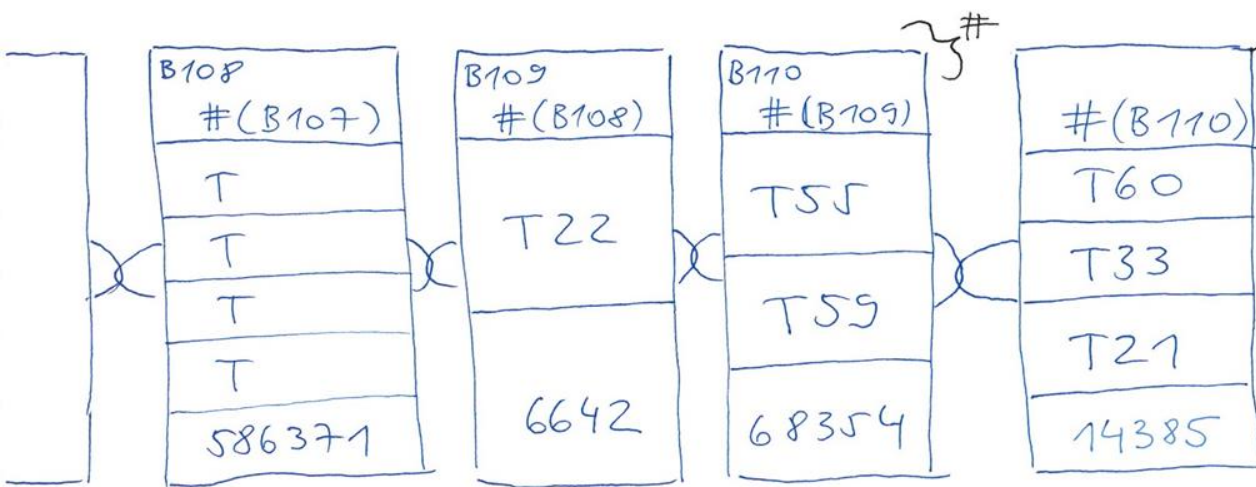
BLOKI

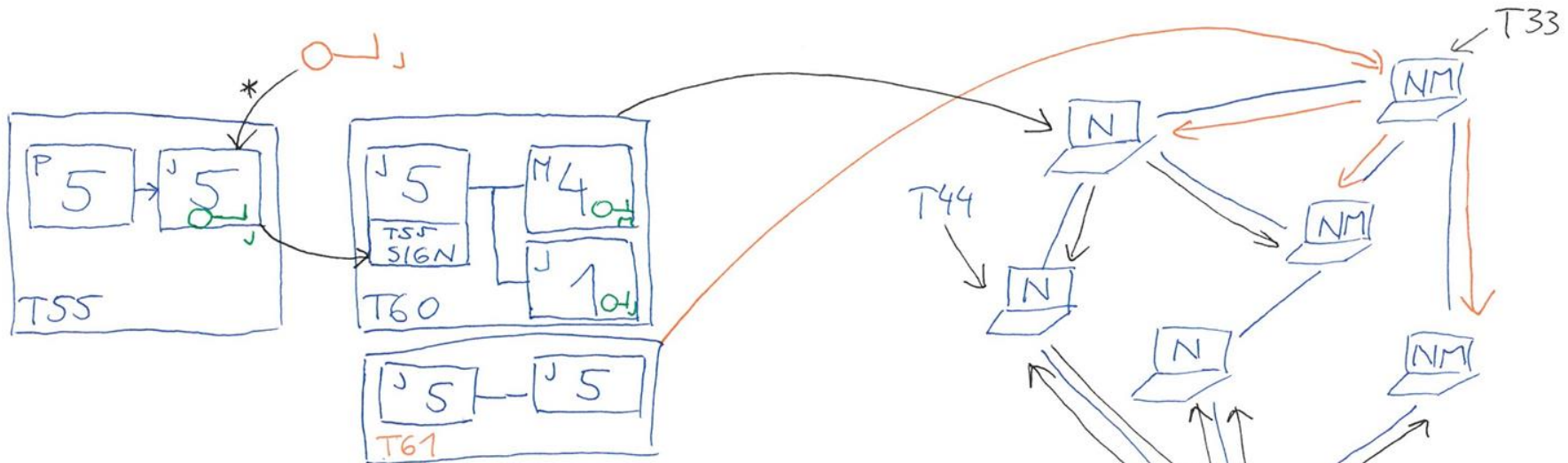




TRANSAKCIJE

BLOKI



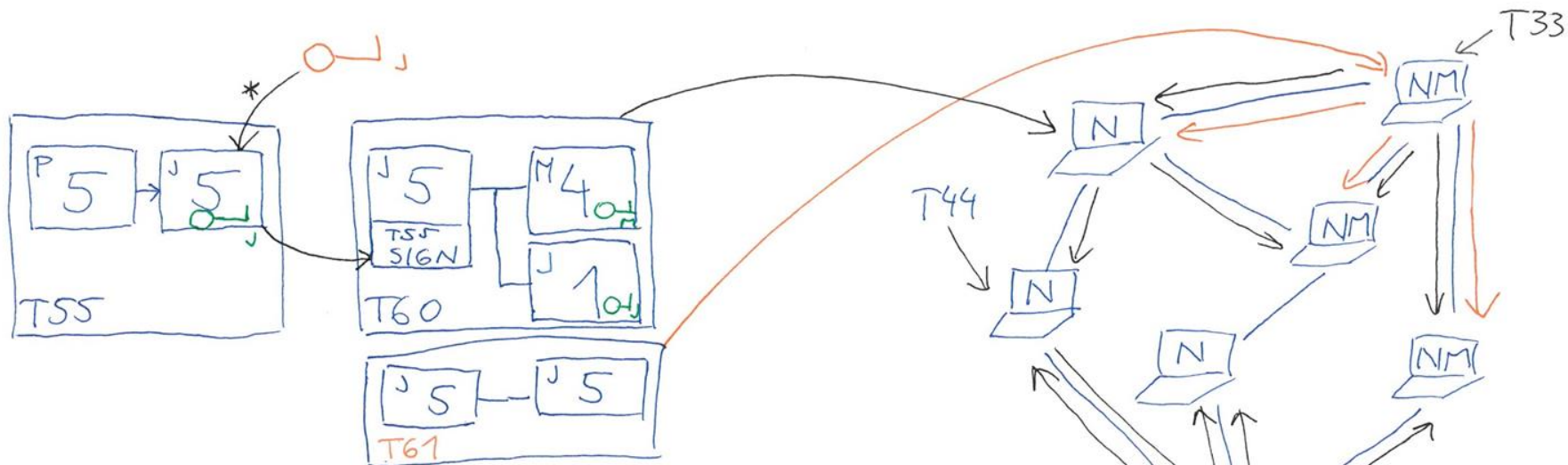


TRANSAKCIJE

BLOKI

	B108 #(B107)	B109 #(B108)	B110 #(B109)	#(B110)
	T	T22	T55	T60
	T		T59	T33
	T			T21
	586371	6642	68354	14385
				#(B110)
				T61

T60 T44
T33 T21 T61
UNCONFIRMED

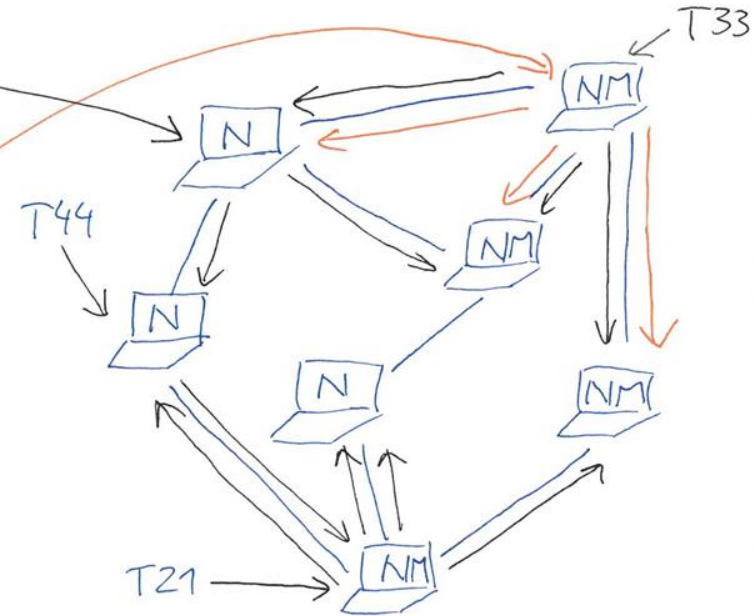
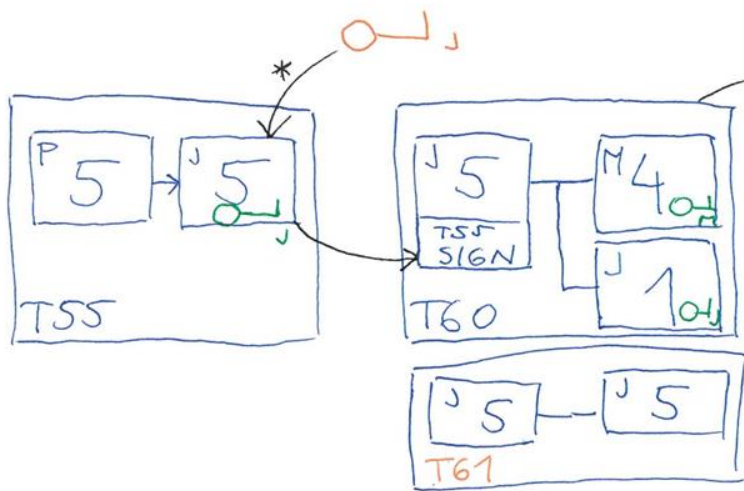


TRANSAKCIJE

BLOKI

	B108 #(B107)	B109 #(B108)	B110 #(B109)	#(B110)
	T	T22	T55	T60
	T		T59	T33
	T			T21
	586371	6642	68354	14385
				#(B110)
				T61
				3485267

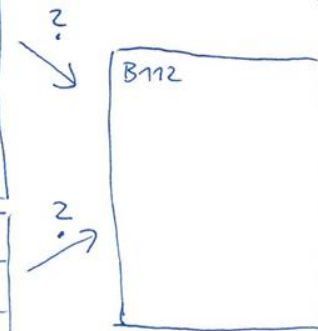
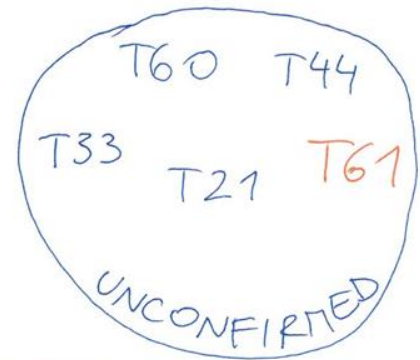


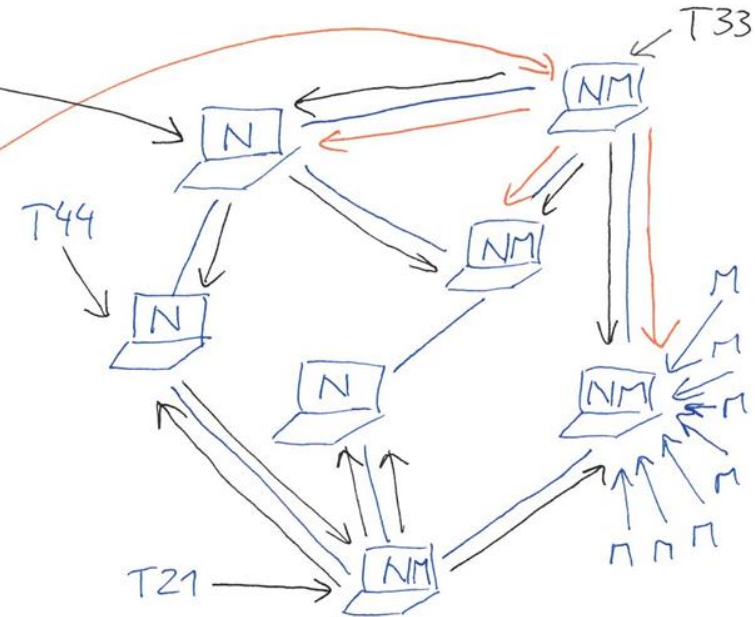
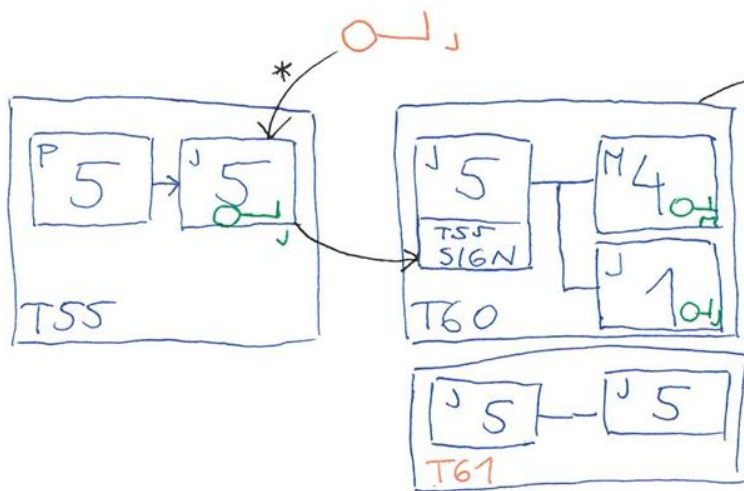


TRANSAKCIJE

BLOKI

	B108 #(B107)	B109 #(B108)	B110 #(B109)	B111 #(B110)
	T	T22	T55	T60
	T		T59	T33
	T			T21
	T			14385
	586371	6642	68354	#(B110)
				T61
				3485267

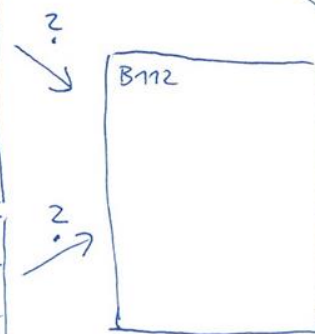
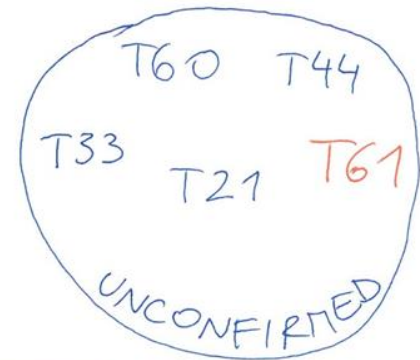




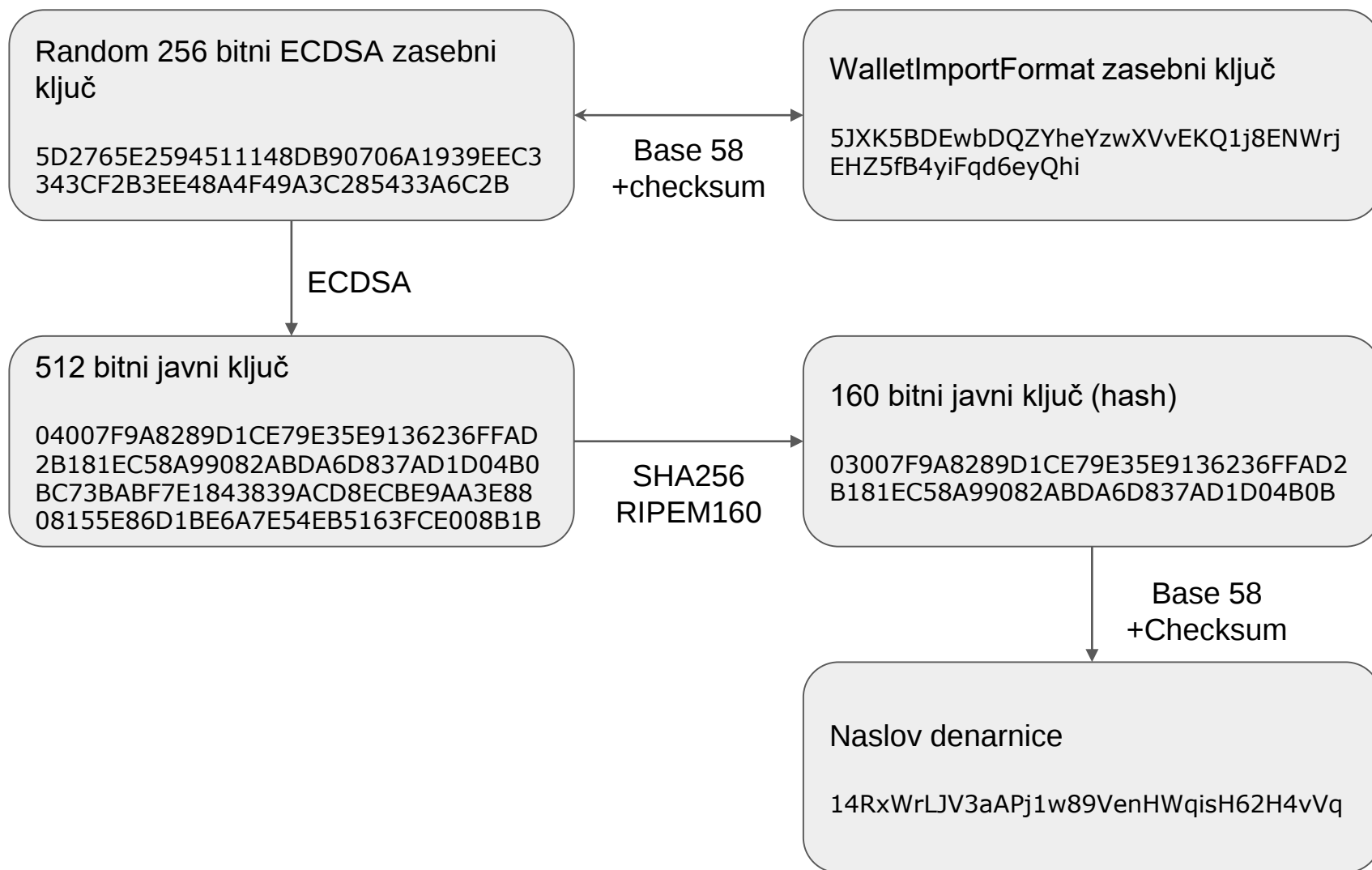
TRANSAKCIJE

BLOKI

	B108 #(B107)	B109 #(B108)	B110 #(B109)	B111 #(B110)
	T	T22	T55	T60
	T		T59	T33
	T			T21
	586371	6642	68354	14385
				#(B110) T61 3485261



Ključ & naslovi



Altcoins

Omrežje	Leto	Hash algoritem	Št.vseh kovancev	Čas blokov	Simbol
Bitcoin	2009	SHA-256	21 MIO	10 min	BTC
Litecoin	2011	Script	84 MIO	2,5 min	LTC
Ripple	2013	ECDSA	100.000 MIO	3,5 sek	XRP
Dogecoin	2013	Script	-	1 min	DOGE
Monero	2014	CryptoNight	18,4 MIO (+)	2 min	XMR
Ethereum	2015	Ethash	-	15 sek	ETH
Bitcoin Cash	2017 (razcep)	SHA-256	21 MIO	10 min	BCH

Bitcoin scaling & forks

