NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 14: Blockchain Elements - II

CONCEPTS COVERED

- Block Generation Cost
- Transactions in a Block
- Bitcoin Scripts

KEYWORDS

- Hash Generation Rate
- Transaction Input and Output
- Bitcoin Script

Block Generation Cost

- Energy efficiency ~0.098 J/GH = ~100 J/TH
- ASIC Hardware for bitcoin can perform about 750 TH/s
- Hash rate approx. 120M TH/s!! Many actually go waste ▮▮
- Network consumes about 80 TW-hours of electricity annually. Figures vary between sources and are some form of estimates
- Average household in Germany of four people consumes approx. 4,000 KW-hours of electricity per year.
- Can power about 20,000 households
- Concept of Pooling is used (https://btc.com/)
- What ensures tamperproof operation in terms of honest nodes??

Blockchain Replicas

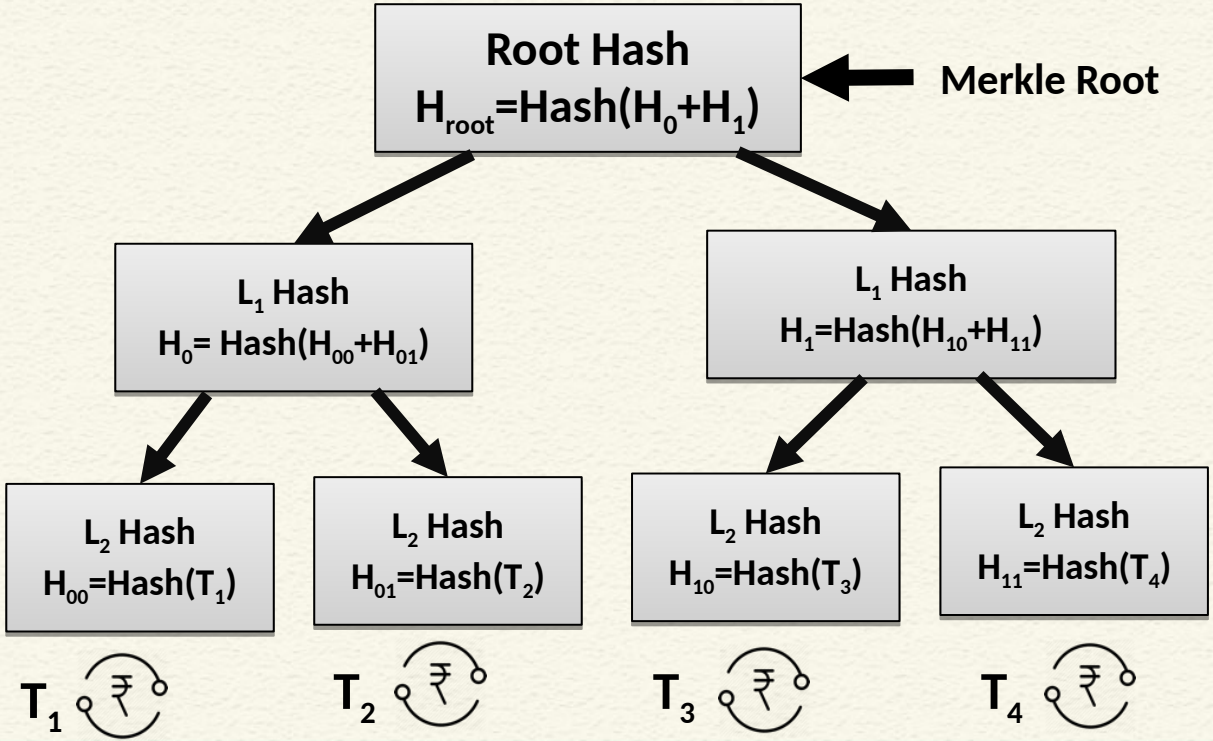
- Every peer in a Blockchain network maintains a local copy of the Blockchain.
- Size is just about 351 GB ⏪
- As a new user joins the network, she can get the whole copy

- **Requirements**
  - All the replicas need to be **updated** with the last mined block
  - All the replicas need to be **consistent** – the copies of the Blockchain at different peers need to be **exactly similar**

Transactions in a Block

- Transactions are organized as a Merkle Tree. The Merkle Root is used to construct the block hash
- If you change a transaction, you need to change all the subsequent block hashes
- The **difficulty** of the mining algorithm determines the **toughness** of tampering with a block in a blockchain

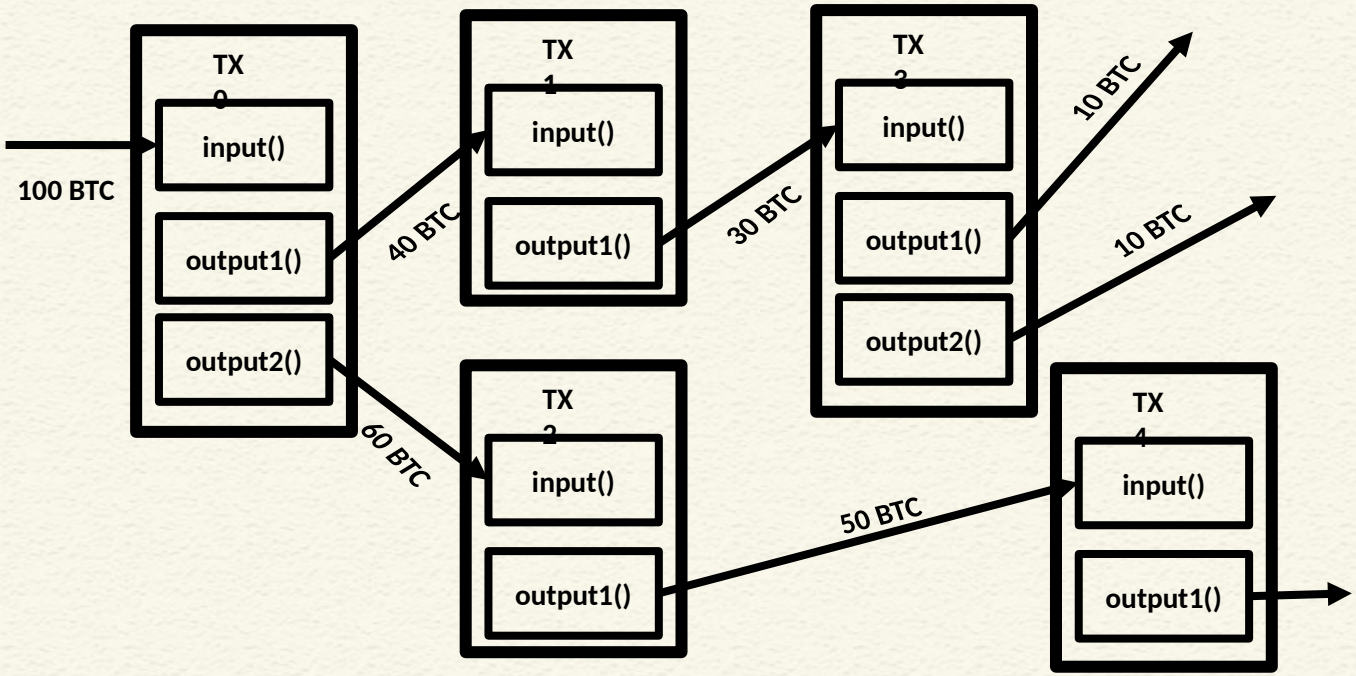
Merkle Tree – A Quick Recap



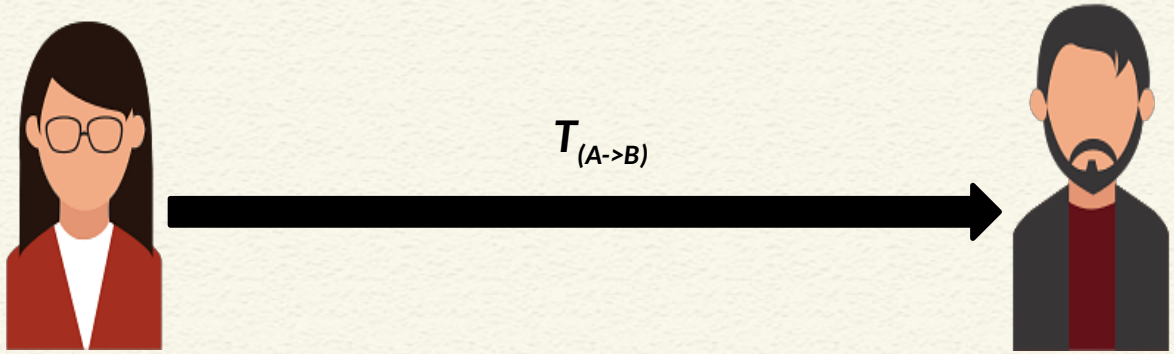
Transactions in a Block

Block Source: https://btc.com/btc/blocks

Bitcoin Transactions and Input and Output

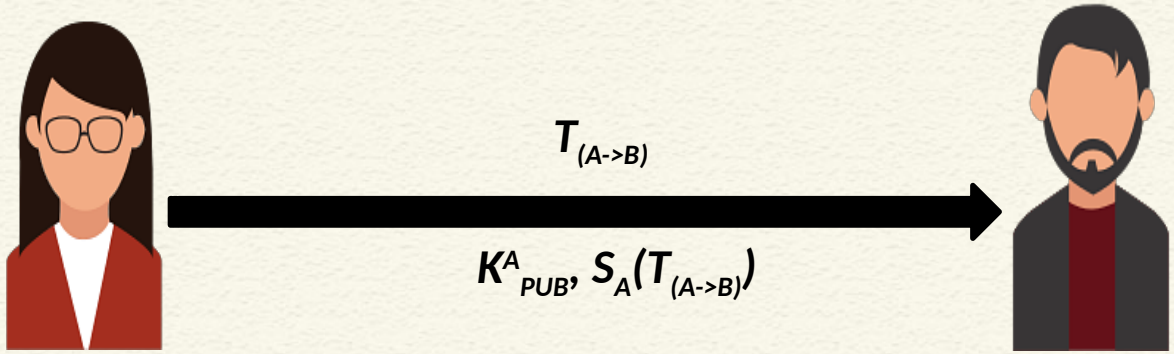


Bitcoin Scripts – A Simple Example



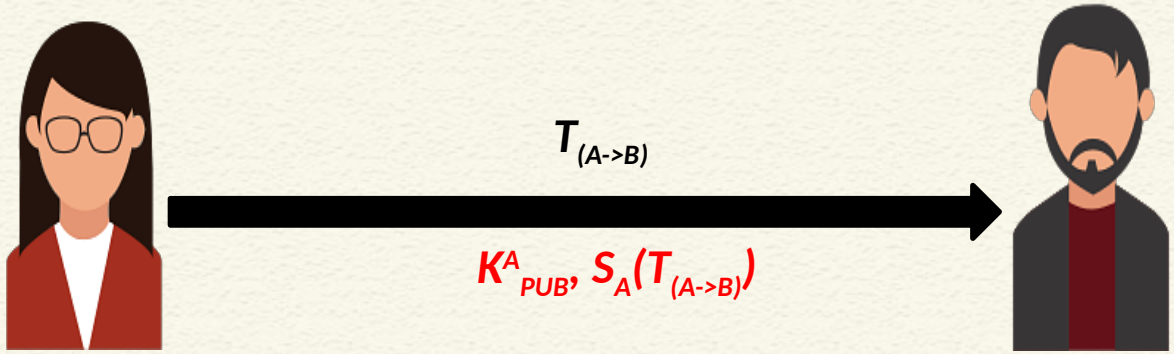
How Bob will verify that the transaction is actually originated from Alice?

Bitcoin Scripts – A Simple Example



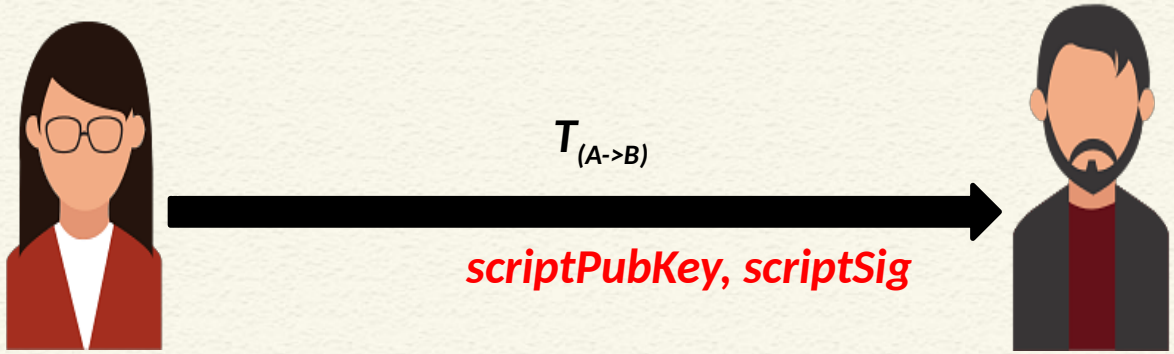
Send the public key of Alice along with the signature -> Bob can verify this

Bitcoin Scripts – A Simple Example



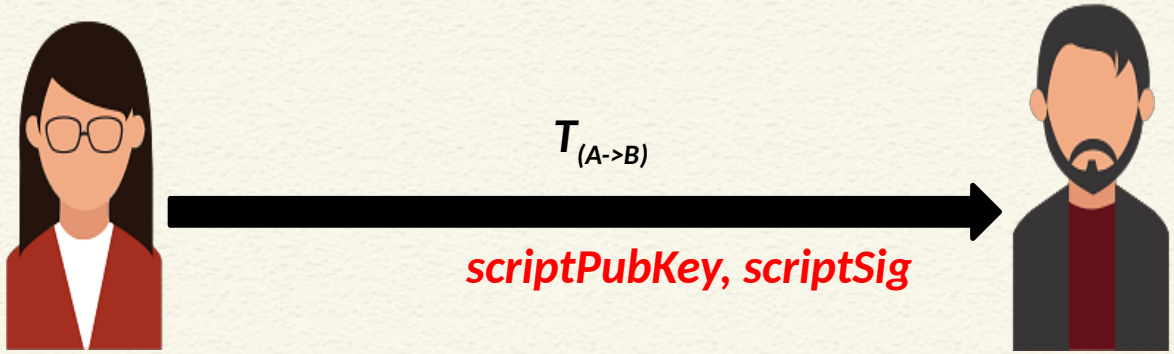
Bitcoin indeed transfers scripts instead of the signature and the public key

Bitcoin Scripts – A Simple Example



Bitcoin indeed transfers scripts instead of the signature and the public key

Bitcoin Scripts – A Simple Example



Bob can spend the bitcoins only if both the scripts return `TRUE` after execution

Bitcoin Scripts

- Simple, compact, stack-based and processed left to right
  - FORTH like language

- **Not Turing Complete** (no loops)
  - Halting problem is not there

Bitcoin Scripts

- With every transaction Bob must provide
  - A public key that, when hashed, yields the address of Bob embedded in the script
  - A signature to provide ownership of the private key corresponding to the public key of Bob

CONCLUSIONS

- Discussed the cost of block generation
- How transactions are included in blocks
- Use of scripts for making and claiming payments

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Any other standard textbook on blockchain/bitcoin


Thank
you