Blockchain, Challenges and Solutions

Ojasvi Aggarwal
Indraprastha Institute of Information Technology, Delhi
ojasvi17033@iiitd.ac.in

Contents:

- **Introduction**
- **Motivation**
- **Challenges and solution**
- **Conclusion**
- **Future work**

Introduction

Blockchain:

- **A global ledger**
- **Stores data publically**
- **Globally consistent**

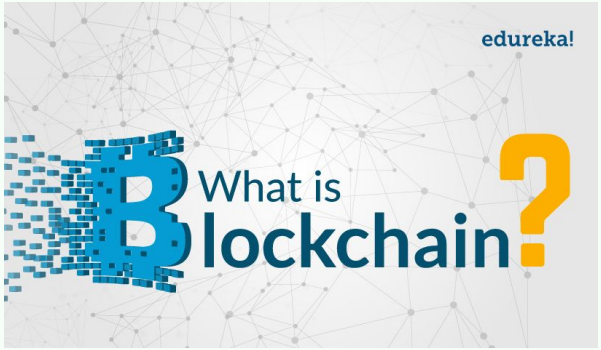

Fig 1: Blockchain [4].

Motivation

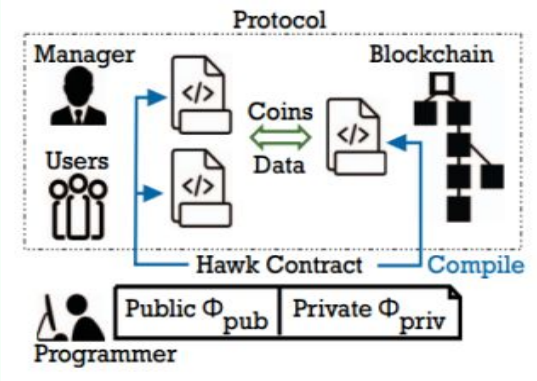

Fig 2: Smart Contract [3].

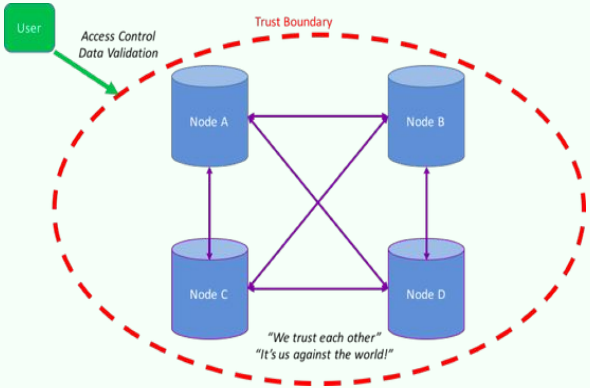

Fig 3: Distributed Ledger [5].

Fig 4: Digital Identity [8].

Challenges and Solutions

51 percent attack

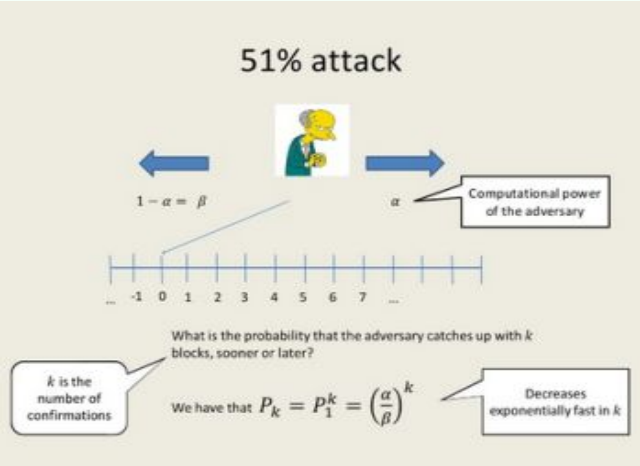

Fig 5: 51% attack [6].

Solution:

- **Increase minimum number of required confirmations**

Double spend attack

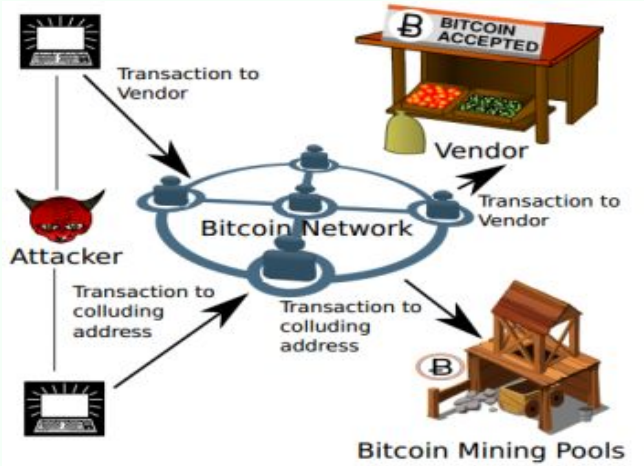

Fig 6: Double spend attack [2]

Solution:

- **Decision depends on how full nodes communicate**

Selfish mining attack

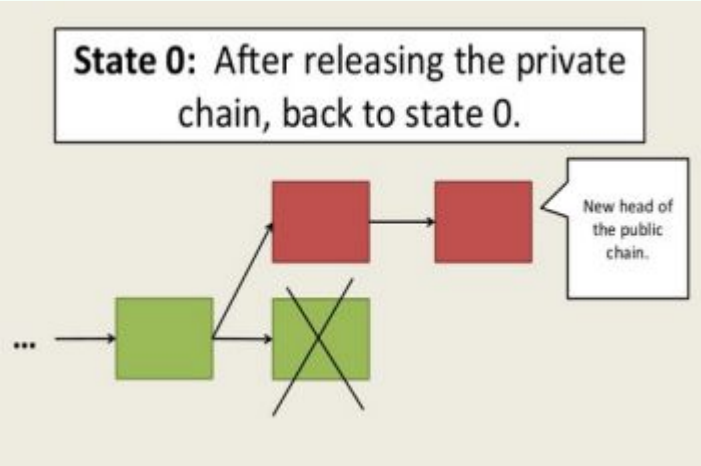

Fig 7: Selfish mining attack part 1 [6]

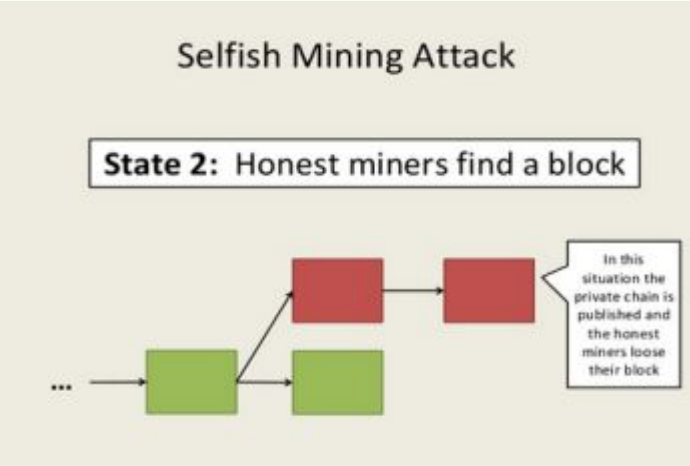

Fig 8: Selfish mining attack part 2 [6]

Solution:

- **Finding pending transactions in network and then blocking the nodes.**

Network Delay

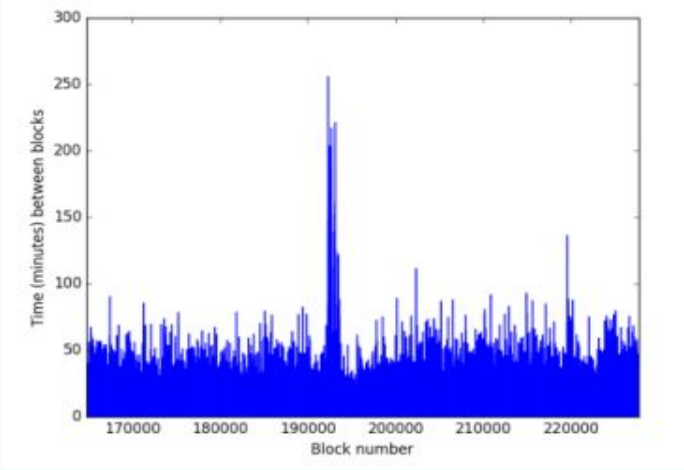

Fig 9: Graph showing network delay [1].

Solution:

- **Introduce more number of stable nodes in the network.**

Transaction Cost

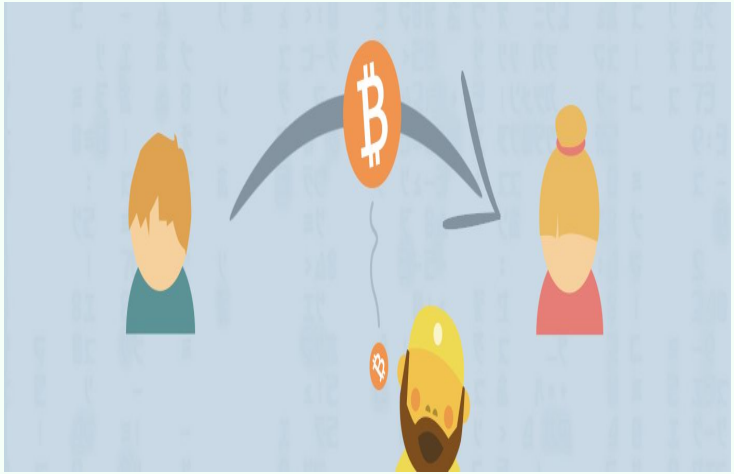

Fig 10: Transaction fee problem [7].

Solution:

- **Add a layer of lightning network over distributed ledger.**

Challenges of blockchain	Solutions
51 percent attack	Increase minimum number of required confirmations
Double spend attack	Decision depends on how full nodes communicate
Selfish mining attack	Finding pending transactions in network and then blocking the nodes.
Lack of privacy of users	Secure multiparty communication
Network Delay	Introducing stable nodes in the network.
Transaction Cost	Lightning network layer over distributed ledger

Conclusion and Future work

- **Discussed till now**
  - Motivation for blockchain
  - Purposes
  - Challenges and solutions

- **Conclusion**
  - Many challenges arrive with time
  - Temporary impact
  - Developers overcome with time

- **Future work**
  - Blockchain Will Protect Self-Driving Cars
  - Ensuring a Secure Internet of the Future

References

[1] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains.” in USENIX Annual Technical Conference, 2016, pp. 181–194.

[2] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 906–917

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in 2016 IEEE Symposium on,Security and Privacy (SP). IEEE, 2016, pp. 839–858.

[4] S. Dayananda, “Demystifying bitcoin and blockchain technologies,” 2017. [Online]. Available: https://www.edureka.co/blog/what-is-blockchain/

[5] R. G. Brown, “On distributed databases and distributed ledgers,” 2017. [Online]. Available: https://gendal.me/2016/11/08/on-distributed-databasesand-distributed-ledgers/

[6] P. Camacho, “Analyzing attacks,” 2017. [Online]. Available: https://www.slideshare.net/philippecamacho/analyzing-bitcoin-security

[7] E. Resende, “Why are bitcoin transaction fees so high?” 2017. [Online]. Available: https://medium.com/@ed_resende/why-are-bitcoin-transaction-fees-so-high-f6dea69e7db7

[8] T. Finanser, “Can blockchain bring trust factor to digital identity concept?” 2017. [Online]. Available: https://www.newsbtc.com/2016/05/25/ can-blockchain-bring-trustfactor-digital-identity-concept/