Meet-up 2019 | Doctorants & Industrie

Multiparty computation (MPC) and Blockchains

Lucas BENMOUFFOK

Daniel Augot[1], Kalpanah Singh[2]

INRIA Saclay, Palaiseau, France[1], IRT-Systemx, Palaiseau, France[2]

1. CONTEXT

Blockchain technology has changed the way we deal with information. Everything is public on it, and it is hard to handle private data for computation purposes on a blockchain. Thus, the use of multiparty computation protocols could be a solution.

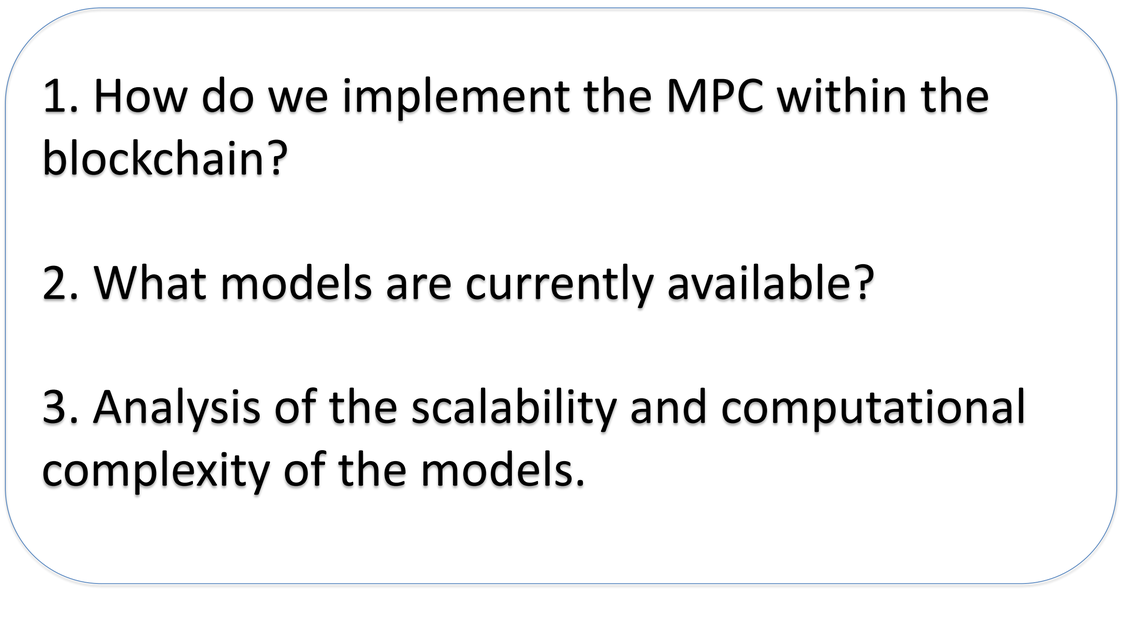
2. RESEARCH QUESTIONS

1. How do we implement the MPC within the blockchain?

2. What models are currently available?

3. Analysis of the scalability and computational complexity of the models.

3. RESEARCH METHOD



4.APPLICATION

1. Auctions within the blockchain (IPO, absolute…).

2. Computation on sensitive data (medical data, financial data…).

5. RESULTS

1. State of the art.

2. Key properties that defines the models.

3. A new model.

6. FUTURE WORK

1. Studying the different blockchain technologies such as ethereum, hyperledger in order to perform MPC efficiently.

2. Design and develop a new Secure, privacy-preserve MPC over Blockchain which achieves scalability and availbility.

REFERENCES

1. Fabrice Benhamouda, Shai Halevi, and Tzi-pora Halevi. Supporting private data onhyperledger fabric with secure multipartycomputation.

2. ShaFabrice Benhamouda, Shai Halevi, and Tzi-pora Halevi. Supporting private data onhyperledger fabric with secure multipartycomputation. i Halevi (IBM) Tzipora Halevi (Brook-lynCollege)CharanjitJutla(IBM)Yacov Manevich (IBM) Fabrice Ben-hamouda (IBM), Angelo DeCaro (IBM)and Qi Zhang (IBM). Initial public offering(ipo) on permissioned blockchain usingsecure multiparty computation

3. https://www.hyperledger.org/projects/fabric 4. https://www.ethereum.org/ 5. https://www.unboundtech.com/

ED STIC
Université Paris-Saclay
Benmouffok Lucas