

Proposta secA: **secure Algorithms**

Introdução

Esta proposta consiste na implementação de um automatismo de Multi Party Computation (MPC) para a blockchain E-BC. A blockchain E-BC é uma blockchain de um projecto que está em fase desenvolvimento. De momento estão a implementar-se as provas de conceito que permitem verificar que o foi desenhado no projecto funciona. A blockchain E-BC é uma blockchain cujos blocos são conhecimento que está validado/certificado. Esse conhecimento começa por surgir na internet em forma de conteúdo de sites, blogs, post em redes sociais etc.. que após um processo de uniformização em ficheiros xml são verificados e se for o caso são certificados e incluídos na blockchain. O objectivo é o seu uso por múltiplos agentes que necessitem conhecimento certificado: governos, instituições, pessoas, empresas, PMEs, plataformas de e-learning, etc.

A arquitetura da blockchain E-BC (Epistemological BlockChain) consiste de um conjunto de nós em que cada nó contém uma machine learning e um modelo lógico de arquitetura servidor-cliente. A construção de blocos é realizada pelos nós quando investidos no propósito de criarem um bloco. Quando nessa situação o nó passa a ser designado por NÓ construtor. Um NÓ construtor irá começar por convocar aleatoriamente um conjunto de outros NÓS, os nós convocados, para avaliarem a informação que pretende incluir no bloco. Os nós convocados enviam ao nó proponente as suas Learning Machines e os respectivos conjunto de teste/avaliação. O NÓ proponente recebe-as/os como Inputs num contexto de Multi Party Computation (MPC) e baralha o emparelhamento learning machines versus conjunto de teste para manter a privacidade dos inputs. Inicialmente o nó proponente começa por fazer uma avaliação sobre a capacidade dos nós convocados serem juízes de conteúdos. Essa avaliação é feita em MPC em que os Result Part (RP) lançam sucessões de questões sobre os Compute Part (CP) e estes processam e respondem às questões e à RP. Essas relações verificação prova é feita através de um algoritmo de Zero Knowledge, chamado Naive Zero Knowledge Proof (NZKP). Se a exatidão nas respostas for assintoticamente superior a 90% o painel de nós convocados é aceite como juízes de conteúdos. Após isso poderá deliberar sobre os conteúdos submetidos, as deliberações são aceites quando satisfazem em consenso o equilíbrio de Nash.

Neste projeto pretende-se implementar em C/C++ todo este mecanismo de MPC descrito com os respetivos algoritmos Zero Knowledge e do Equilíbrio de Nash. Os alunos já contarão com as respetivas provas de conceito do mecanismo programados em python. Terão também disponíveis as machine learnings de produção para os nós.

Tarefas a Realizar

1. Estado da arte (setembro-outubro)
2. Estudo da blockchain E-BC e das suas provas de conceito (outubro)
3. Implementação de alguns nós (novembro)
4. Implementação do equilíbrio de Nash (dezembro)
5. Implementação do algoritmo Naive Zero KNowledge (janeiro)
6. Implementação do protocolo MPC (janeiro, fevereiro)
7. Funcionamento integrado do sistema MPC com NZK e Equilíbrio de Nash (março).
Eventual implementação na cloud.
8. Testes (abril)

Área

Blockchain, segurança, privacidade e inteligência artificial

Referências

- Paulo Vieira, Paul Crocker, and Simão Melo de Sousa, 2019, elearning, Artificial Intelligence, and Blockchain, *ECIAIR 2019, European Conference on the Impact of Artificial Intelligence and Robotics*
- Barbosa, M., Brouard, T., Cauchie, S. and De Sousa, S.M., 2008, July. Secure biometric authentication with improved accuracy. In *Australasian Conference on Information Security and Privacy* (pp. 21-36). Springer, Berlin, Heidelberg.
- Ronald Cramer, Ivan Damgård and Jesper Buus Nielsen. Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015.

Contactos

Orientador: Paul Crocker PhD, crocker@di.ubi.pt

Co-orientador: Paulo Vieira PhD, paulo.vieira@ubi.pt Cloud Computing Competence Centre, UBI