Andrew Poelstra

Je suis mathématicien et je travaille chez Blockstream, où j'analyse et conçois des protocoles liés à la preuve à divulgation nulle de connaissance et au consensus décentralisé et contribue au développement et à la mise en œuvre de ces protocoles; identifie et règle des sous-problèmes de mathématique associés à la mise en œuvre de conception et aux opérations de systèmes distribués ou cryptographiques; examine et comprend la documentation de pointe dans les domaines pertinents (p. ex. la théorie des nombres, la cryptographie, les crypto-monnaies, la sécurité informatique) et appuie les développeurs qui créent et optimisent la mise en œuvre; rédige des articles techniques examinés par les pairs où l'on décrit de nouveaux algorithmes et protocoles.

J'ai grandi à Cloverdale, en Colombie-Britannique. J'ai fait mes études à la Simon Fraser University, obtenu un baccalauréat en sciences avec spécialisation et été corédacteur de plusieurs articles techniques. Je me suis inscrit alors à la University of Texas à Austin, où j'ai obtenu une maîtrise en mathématiques, tout en participant à des projets de cryptographie à source ouverte dans mes moments libres. J'ai quitté l'école pour poursuivre mes intérêts en dehors de mes études, puisque la cryptographie appliquée était plus pratique à ce moment de ma vie que ma recherche universitaire.

IJe me suis intéressé tôt dans la vie aux mathématiques, en particulier la cryptographie, en apprenant qu'on faisait des efforts récemment pour déchiffrer les messages codés à l'aide de la machine *Enigma* dans la Seconde Guerre mondiale. J'ai obtenu un baccalauréat en mathématiques, période durant laquelle j'ai exploré de nombreux domaines. Vers la fin de mon premier cycle, j'ai découvert le mouvement *cypherpunk*, groupe d'activistes et de développeurs qui utilisent la cryptographie appliquée pour le mieux-être social. À cette époque, la crypto-monnaie Bitcoin venait d'être créée. Ce sujet comportait de nombreuses questions de recherche accessibles. Ma formation officielle en mathématiques a été fortement complémentaire à mon travail non officiel dans ce domaine. Selon moi, c'était une excellente application de mes compétences. Je travaille maintenant à temps plein en cryptographie appliquée.