Миодраг Михаљевић

Математички институт САНУ, Београд

Неки изазови изградње безбедних система у дигиталном простору на бази *blockchain* технологије

Резиме:. *Blockchain* технологија је препозната као савремени приступ од суштинског значаја за обезбеђивање интегритета, аутентичности и контроле приватности у дигиталном простору са изузетно великим бројем могућих примена укључујући и примене у критичним информационо-комуникационим инфраструктурама.

Кључна компонента сваког *blockchain* заснованог приступа је протокол за постизање консензуса о тачности информационих блокова који се уланчавају. Такође, од кључног значаја су и криптографске технике које се користе у систему заснованом на *blockchain* технологији. Изградња система заснованих на *blockchain* технологији укључује и решавање низа изазова укључујући примену адекватних протокола за постизање консензуса и криптографских техника.

Сагласно наведеном, ово излагање приказује неке протоколе за постизање консензуса и неке криптографске технике погодне за одређене класе система на бази *blockchain* технологије којима се остварује жељени ниво информационе безбедности. Дискутују се: (а) неки консензус протоколи са становишта сигурности коју обезбеђују и њихове имплементационе сложености; (б) криптографске технике које омогућују ниско додатно оптерећење основне функционалности система због примењених механизама за остваривање информационе безбедности. Показује се како одређени резултати из области теорије кодова могу бити примењени за ојачавање криптографске сигурности компактних криптографских техника ниске имплементационе сложености чиме се постиже добар компромис између ојачања нивоа сигурности и увећања имплементационе сложености и енергетске потрошње. Дају се илустративни прикази ојачања криптографске сигурности у информационо-теоријском смислу и са становишта сложености израчунавања полазећи од разматрања декодовања после канала са синхронизационим грешкама у којима поред случајног комплементирања бита може да настане случајно брисање бита или/и уметање случајних бита у кодној речи.

Такође, укратко се дискутују примене разматраних протокола за остваривање консензуса и криптографских техника у одређеним системима заснованим на *blockchain* технологији.