A digitális pénzrendszerek biztonsági kérdései

(Absztrakt)

E tanulmány célja, hogy széleskörűen és rendszerszemléletűen vizsgálja a létező digitális pénzrendszerek tulajdonságait, ezek között kiemelten az anonimitást, mint a személyes adatok védelmének eszközét, valamint a biztonság különböző aspektusait; továbbá hogy összegezze egy ideális rendszerrel szemben elvárható követelményeket. A digitális pénz séma mibenlétének meghatározása után a szerző áttekinti a Chaum kutatásaiból kiinduló evolúciós folyamatot, ennek főbb állomásait és jellemzőit. Ennek során számos, sokféle célra használható sémát és technológiát mutat be, köztük kreatív és új kriptográfiai primitíveket, amelyek alapvető építőelemként lehetnek jelen a sémákban, vagy pedig modulárisan biztosíthatnak kívánt tulajdonságokat. Hivatkozik a sémák tudományos publikációira és elemzi az összehasonlító művek által fontosnak tartott tulajdonságokat. Áttekint bizonyos lényeges tulajdonságokat, digitális pénz sémákat elemez. Ezt követően a szerző sorra veszi, hogy egy elképzelt ideális digitális pénzrendszernek milyen tulajdonságokat kell teljesítenie. Kiemeli, hogy megítélése szerint mely fő problémák nyitottak az egész kutatási terület előtt és szubjektív kitekintést ad a várható fejlődésről.