**CONCLUSION**

It is clear that the Merkle signature scheme is existentially un-forgeable under adaptive chosen message attack and one can also present a forward-secure signature scheme from any cryptographic-secure pseudorandom bit generator, one-time signature scheme and hash function.

Having agreed on computing outcomes are useful, in that many applications can without requirement of arbitration connect with each other without human permission. Thus, something like Ethereum is useful: agreement on many applications in the same computing substrate.

Blockchain computers introduced Merkle computing. Currently the verification and enforcement are in the same system (blockchains).

On the edges, however, cheaper and more varied Merkle computing could open a much wider, more open, audit-able, shared & verifiable computing substrate.

Exploring more generic and varied Merkle computing with different styles of computational courts could lead to some very interesting, emergent applications.