**Chapter 5**

**LIMITATIONS AND FUTURE WORK**

**5.1 Limitations**

Limitations of the Merkle scheme:

* it is stateful
* it uses CRHF (whereas we know how to construct CRHF from specific assumptions such as DLA or the hardness of factoring, we do not know how to construct them with the weaker assumption that OWF exist)
* we must know in advance the number of messages to be signed
* the length of the secret key is too long (it is proportional to the number of messages to be signed)

It is not certain at all how fast Merkle computing can really become, and whether it will mainly be used for a subset of computing goals (rather than replacing all computing with these additional auditing capabilities). It also not certain whether putting it into a networking layer like IPFS makes sense. Bandwidth might limit effective ability to propagate computing. For example, Ethereum is very slow, currently, compared to other computers. State changes are enforced at 15 second intervals, and is currently not faster than a single computer. Sharding & the use of state channels could improve the speed radically.

It remains to be seen how it will all evolve now that we have invented Merkle computing & computational courts. It will be interesting to explore its full potential in the coming years.

For humans, opting into computational courts means it has to be better than our current social courts. We can now create a market for courts, and we are exploring how to make better courts with this technology. It’s likely that the first use of these courts will be around systems that want global enforcement, where global courts don’t reach atm (or ever will):

However, in an only machine-to-machine economy, the only courts are computational courts. Empowering machines to coordinate without humans, and adding in scalability of AI to make decisions about markets faster and better than humans will cause some crazy, weird things to happen and potentially huge amounts of economic value.

Decentralized, virtual worlds (and simulations) will also not have access to social courts. Experimenting in this layer could have useful implications for how our current courts work and run.

**5.2 Future Work**

21st century is an era of Internet and IT infrastructures. Since 1994 it is well known that if anyone can build a large enough quantum computer, he can break all most popular public key cryptosystems like RSA, DSA and so on. According to the physicists this may happen the next 20 years. And since security is the heart of cryptography, now we are standing in front of one of the most serious problems nowadays – the improvement of post-quantum cryptography and digital signatures – what kind of signatures should we use to avoid the advantages of quantum computers. As Merkle scheme does not rely on any number theoretic assumptions (like for example the RSA is based on the well known integer factorization problem), but requires only the existence of collision resistant hash functions, it is a perfect candidate for a post-quantum signature system.

However a number of additional problems also appear like key pair generation and larger secret keys. Solutions may be found, but the most important question still remains - how can one apply the Merkle scheme with its limited number of possible signatures. As it has already been seen in the thesis, nowadays there are a number of improvements of the classic Merkle signature, but this question still remains unsolved.

So that is why we still ask ourselves: Can anyone use the Merkle signature scheme for the modern applications at all?