Know Your Assumptions.

A Treatise On Assumptions in Cryptocurrencies and DeFi.
Revision 0.1

Alexander Chepurnoy, Amitabh Saxena

July 17, 2022

Abstract

1 Introduction

This article is going to provide affirmative answers to few important questions which seem to be largely ignored in the cryptocurrency industry, despite the fact that the questions are very basic ones, and, in our opinion, existence of the industry is heavily relying on them. Also, we systematize knowledge about assumptions cryptocurrency and DeFi protocols are based on. We suppose that understanding explicit or implicit assumptions protocols are based on is critical for understanding security and degree of decentralizion of protocols properly.

- Traditional financial institutions are doing invasive checks known as KYC/AML practices. In bankless world of cryptographically powered decentralized finance it is natural to assume that now users are checking protocols for their properties, including cryptographic and other assumptions, however, there is no explicit notion of it in the wild. We would like to see Know Your Assumptions practices as an alternative to KYC/AML practices in the world of decentralized money and financial tools, where users of the protocols do have real power, not centralized entities enforcing users to comply with their always-changing rules.

- In traditional finance, an investment is always associated with not just a projected profit, but also with risk profile. In opposite, in DeFi only APY (estimated yearly interest rate at the moment, usually not averaged over long enough period and cleared from noise even) is being sold, while public is totally unaware about risks.

- As a consequence, it would be desirable for investors to quickly compare security of different protocols (from L1 blockchains to complicated DeFi stacks and inter-chain bridges) by assumptions they are based on.

- For protocol researchers and developers, it would be good to explicitly state assumptions their protocols are relied on in their papers and specifications.
- It is common, especially around so-called Bitcoin maximalists, to say, that, instead of trust in central authority, they trust math. However, we need to challenge that saying. Is Bitcoin protocol relies on math only?

We start with Bitcoin, the most known and probably simplest cryptocurrency. Then we consider Ergo case as well as some applications on top of it, such as ErgoDEX, SigUSD.

2 Assumptions in Cryptography

In cryptography, starting from around 1980s, it is common to require provable security for all the constructions, starting from theoretical primitives, like one-way functions and pseudorandom generators, to very complex protocols. Provable security basically means that security goals of a construction are defined formally, as well as assumptions the construction is relied on, and then there is a proof that goals are indeed satisfied while assumptions hold. A proven construction can be then used as an assumption for a higher level protocol. In the very core there are some assumptions we can not reduce to other ones, so modern cryptography relies on a belief that in the world we are observing some very basic assumption holds, but those assumptions are well tested and centuries of math have not disproven them.

3 Bitcoin As A Digital Gold

We do believe probably that Bitcoin is valuable commodity and

- Hash function SHA-256 is not broken. By being not broken we mean that known security properties of any hash function, namely collision resistance, second preimage resistance, and preimage resistance hold.
- Digital signature scheme is not broken. As digital signature scheme used in Bitcoin is vulnerable in presence of quantum computers, it means that the Bitcoin protocol relies on assumption that quantum computers capable to solve Discrete Log Problem for an elliptic curve of 128-bit security will not appear.
- Majority of mining hashrate is *honest*, i.e. following the Bitcoin protocol. This is the most tricky part, as the protocol is defined via a reference client implementation, and it is not very clear what modification of pretty massive client codebase could be considered as dishonest. The best thing we can do here is to work with simplified models. The most famous one is presented in GKL15 paper. For the first time in the space, the paper had

shown that the Bitcoin-like Proof-of-Work based protocol can achieve some formally defined properties under assumptions of hash function collision-resistance and also majority (or 33% for fairness property) of hashrate power being *honest*, and the protocol defines what does it mean to be honest: a peer must build on a longest chain, use protocol's validation and input contribution rules. Real Bitcoin protocol, however, is much more complex than the GKL15 model. Continuing longest chain could not be enforced by the Bitcoin protocol, for many years there was a tenet in the folklore that this behavior is just the most rational choice, but then some papers show that rational behavior could be quite different in some scenarios (see [], [], []). While in the real protocol following validation rules seems to be necessary indeed (otherwise, a mining node's block will be rejected by honest nodes), SPV mining was observed in the wild even [] (and, theoretically, is a big concern when talks about increasing block size happen, due to validation dilemma []). For input contribution, it is hard to say where honest behavior ends (especially for other protocols which are more feature-rich, where miners can profit a lot from reordering transactions and other games []). Please note that the field is still pretty green, so we do not know a lot about deviations from the protocol and how to react about them.

As you can see, even for Bitcoin assumptions are tricky, and then it is hard to say how successfully the protocol we have (in form of client code) may achieve security properties, as even basis is not fully understood yet. However, Bitcoin network works for more than 13 years to the moment of writing this treatise, many theoretical issues do not happen in practice (so maybe not of a concern), and issues that are not known likely are even more theoretical.

Note that Bitcoin has known emission schedule if assumptions hold. Thus Bitcoin as a digital gold can be better than physical gold, as for physical gold assumptions behind hardness of its production are less known.

Alex notes : fun facts, e.g. Bitcoin protocol is the code, but originally the code had unlimited emission.

4 Ergo

Bitoin assumptions, as shown above, are tricky, but for other cryptocurrencies situation is worse. They may have additional cryptographic assumptions (such as hard problems in pairing and trusted setup in ZCash), or more complex problematics of peers behavior.

For Ergo, since day one the focus was on achieving possible maximum from modest Bitcoin's set of assumptions. Main differences are:

- Ergo allows a node to have full security guarantees without storing UTXO set.