Blockchain was introduced around a decade ago as a tool for dealing with a so-called "double spending" problem in a cryptographic currency called "bitcoin". It is currently believed that this technology has a wide range of applications much beyond the financial ones. One of the blockchain's key advantages is that it "distributes trust", i.e., its users are not required to trust a single entity, but instead they can rely on (weaker) assumptions such as "honest majority" or "honest majority of computing power".

One of the weaknesses of this technology is that (while reducing trust in *external* servers) it is very strongly based on the assumption that individual users can *internally* securely store data and perform complex cryptographic algorithms. Since blockchain users are typically identified by their public keys this makes the corresponding secret keys a very attractive target for cyber attacks. Moreover, there is a non-trivial risk that a user will forever loose access to his account due to secret key loss. It is estimated that the total amount of coins lost this way in the years 2011–2018 is equivalent to over USD 2 billion. In order to increase security, the secret keys are usually stored in so-called *blockchain wallets*, which are devices for storing cryptographic keys used for making transactions on the blockchain.

If a wallet is piece of dedicated hardware then it is called a "*hardware* wallet". Using hardware wallets comes, of course, at a price, since digital equipment is expensive. The need to handle additional devices also degrades user's experience. Therefore some users prefer to use the "*software* wallets", i.e., application executed on a general purpose computer (or a smart device). Another popular distinction is between "hot" and "cold" wallets. The former are connected to the Internet, while the latter are separated from it (via a technique call "air gapping"). Usage of wallets introduces additional trust assumptions. Understating them is important since, unlike in the traditional applications (such as on-line banking), blockchains, due to their distributed nature, pseudonimity, and irreversibility of transactions, are much more sensitive to cyber attacks.

The goal of this project is to develop new models and tools for secure blockchain wallets with *focus on the foundational aspects* of this field. Its main outcomes will be: new models and definitions in the area, and new provably-secure solutions. Our main focus is *theory* and *foundations*, but we expect the project to also have a *practical impact*. In our modeling efforts we will use formalism from theoretical cryptography. Formal approach is extremely important in the area of cyber security. This is because security cannot be proven "experimentally", or in other words there are no "experiments" that can serve as evidence that a given system is secure. Our constructions will use tools and methods from cryptography and distributed algorithms. We will also use techniques developed in the area of leakage- and tamper-resilient cryptography. Although the main expected impact of this project is theoretical, we may also work on prototype implementations that can lead to commercial products.