17th International Workshop on Algebraic and Combinatorial Coding Theory,
October 11-17, 2020, online, Bulgaria, pp. 77-82

2020 Algebraic and Combinatorial Coding Theory (ACCT) | 978-1-6654-0287-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ACCT51235.2020.9383361

Research Incentivization based on Smart Contract Platform

Jivko Jeliazkov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Sofia, Bulgaria
jivko@math.bas.bg

Biser Tsvetkov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Sofia, Bulgaria
biser@math.bas.bg

Hristo Kostadinov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Sofia, Bulgaria
hristo@math.bas.bg

***Abstract*—The boom of public blockchains and smart contract platforms opened new approaches to solve existing issues. These new approaches addressed successfully some weaknesses of previous processes and created some new classes of problems that need solutions. In this paper we explore distributed system based on smart contract platform with a low-entry barrier designed for direct incentivization of results of scientific research. The proposed system relies on transparent interactions between organizations and individual scientist defining hard computational problems with others that are willing to invest time and efforts searching for computational solutions.**

***Index Terms*—public blockchain, distributed ledger technology, zero-knowledge proof, hard computational problems**

I. Introduction

An explosion of new ideas and technologies followed the success of Bitcoin network [1] as decentralized financial systems. It proved that a stable system can be build and operated there was how distributed systems could enhance and replace existing technologies. Ethereum [2] showed that smart contracts add to blockchains abilities that are make it flexible and programmable which led to a bunch of new decentralized applications (dApps) based on a set of related smart contracts running on the public blockchain. It took some more years and the third generation of public blockchains got traction adding sophisticated new methods for reaching consensus, reducing the transaction costs and improving network accessibility. The expected explosion of dApps did not happen as fast as expected. Public blockchains got swarmed by various games, gambling and decentralized exchange apps. Being a new technology public blockchains took major share of the technological research efforts. This brought many technologies in the spotlight such as zero knowledge proofs, advanced security protocols, analysis of consensus algorithms, and various distributed ledger technologies based on directed acyclic graph instead of blockchain.

Apart for the indirect boost to various science branches and technologies public blockchains have the unique ability to offer medium that is visible, immutable and decentralized. All these properties are desirable by most science research activities. Can we build a system that could help different scientific entities to better define the problems that they put their efforts? A system that is visible so even an external or anonymous participant could contribute to solution of a specific tasks by automatically incentivizing achievements of researchers.

Let's think about one practical example that is in the area of medical research: The protein folding [3] is a physical process by which a protein chain acquires its native 3-dimentional structure. The primary structure of a protein as a linear amino-acid sequence fully describes the protein's content. The secondary protein structure is the first step from the folding process for the protein to finally fold into its native structure. Secondary structure consists of sets of alpha helixes, beta sheets and connections between them. Their final single-protein structure is reached after tertiary structure get the secondary structures fixed in the 3-dimensional space. The quaternary structure describes formations of already-folded proteins assembled into bigger structures. Getting from the deterministic primary structure to the final 3-dimentional protein structure takes from microseconds and minimizes the structures Gib's free energy. Since the full information for the protein is a string of amino acids finding the native protein structure could be defined as energy-optimization problem (Fig. 1). When we have a stable low-energy solution that do not fit what we expect and does not match the structure observed in practice we could assume that the native protein structure is different.

A task to search for a matching structure that minimize protein's Gibbs energy could be an important step in the research of various proteopathy diseases [5] such as Alzheimer's disease, Parkinson's disease, amyloidosis and many others.

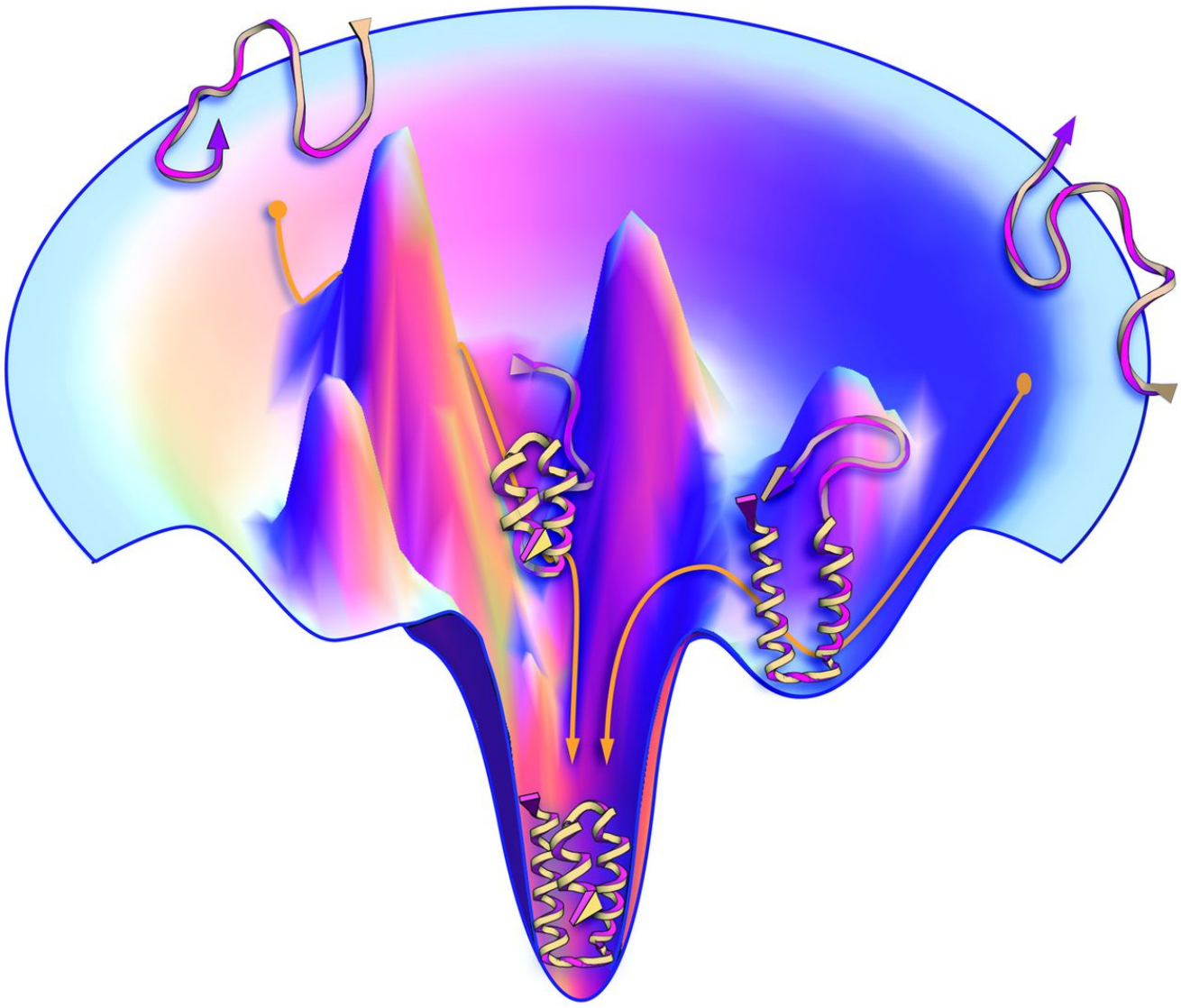

Fig. 1. Optimizing Gibbs energy during protein folding [4]

Although this computational challenge is easy to state, it is hard to solve, and the effectiveness of proposed solutions are easy to compare based on their calculated Gibb's energy values.

In this paper we describe a decentralized system based on public blockchain for incentivizing measurable and provable achievements in various research fields. We address the question if searching for solutions of such computational problems can be incentivized using a system based on smart contracts running on a public blockchain. In Section 2 we describe the overall process and all major participants in it. The types of tasks that the system could handle are described in Section 3. Key components of the systems are shown in Section 4. Some important factors for proper use of the system, some attack types and defense against them are described in Section 5. The final chapter 6 contains the conclusion of the research of the decentralized research-incentivization system.

II. Main Parties Involved in the Incentivization Process

Understanding the roles of the participants and their interactions with the system is the first step for analyzing such system. Due to the specifics of the systems not all participants need to actively communicate to the system. It is expected that for some participants will threat the system as read-only source of information and other may interact only indirectly. Based on their functions several groups of people are involved in incentivization for research topics.

Framework Providers are typically organizations or individual developers that create and maintain the distributed coding for the supported frameworks in the smart contract platform. Their responsibility is also to maintain them by providing improvements and fixes when needed. For example, a group could offer a module to the system for calculating Gibb's energy for a specific 3-dimentional structure of a

protein. Using this module, the system could automatically compare two or more different folding solution for a single protein and calculate that some of the proposed solutions are not the natural one due to their higher energy state. The provided coding makes sure no one could get the reward except the one that supply the best solution in the given timeframe. Thinking about architecture - there could be many different frameworks supported by the system. Different frameworks do not compete with each other but enhance their scopes and, in some cases, they could even share reward pools. And, since they all share the same smart contract platform based on public blockchain, they indirectly improve each-others security and immutability.

Reward Providers are the next important participants. Unlike Framework providers, the Reward providers does not have to be experts in the software or blockchain development. They need only to have scientific domain knowledge for the researched topic. For example, researchers investigate specific protein that is involved in specific prion disease. Knowing the protein's 3-dimensional shape is essential for determining its function and properties. Setting a reward for providing the best energy-efficient folded structure matching the protein's sequence of amino acids may lead to finding vital information for researching methods for treatment of the illness. Some initial monetary (in public blockchain sense) reward will be set for the entity that provides proper solution to the defined problem. Having the computational problem set and initial reward structure supplied to the system is all the Reward provider needs to do to have the problem defined and open for accepting possible solutions.

Reward Contributors are optional participants in the incentivization, but they may have a key role to focus attention to specific research problems. They could be either organizations or individuals that want specific problem(s) to find a solution. Reward contributors are not required to have domain or technical knowledge to contribute in the process. In our example Reward contributors could be organizations investing in finding cures for the specific prion decease. Their role is to contribute financially to the rewards for finding solution for one or more problems they choose.

Researchers are again organizations or individuals that work for finding solutions to the defined and modelled in the system computational problems. Once they have a fitting solution, they submit their proposed solution to the system. After validation, depending on the configurations, the reward could be either transferred immediately or at a previously defined moment in time to allow further (and possibly better fitting) submissions. The reward in this case is the accumulated currency rewards up to the moment the price is transferred, and the problem's state is considered solved according to the configured boundaries set by the Reward provider.

Read-only / Off-chain Participants are essential part of the proposed system. Sharing the information for the frameworks, research problems, and available reward in the media is important part of the overall process. The category of Off-chain Participants also includes researchers that compete for the reward or collaborate off-chain. The system is used as a medium for sharing problems and incentivizing research. In many cases this may happen, and it should happen with no on-chain traces.

In the perfect case all participants need to participate accordingly for the system to contribute for the successful scientific research. At the end of each full process and behind every reward given there could be significant research breakthrough.

III. Classification of Incentivization Tasks

TABLE I
SEVERAL TYPES OF SUPPORTED TASKS

ID	Task	Private	Allow	Allow	Typical	Examples
1	G_{8_2}	2	2	384		
2	G_{8_6}	6	2	5760		

Some of the task types are given in Fig. 2. The tasks that are set for the system may vary by their defined duration – they may either be set in the system for indefinite interval or could have a predefined duration. The indefinite time tasks assign their full reward the first time a solution matching defined parameters is supplied to the system. The limited time tasks are more flexible. They may assign the reward to the first fitting solution or they may wait for all submissions to accumulate and reward only the best one after the end of the period of competition.

In some cases, sharing the results for the winning solution may not be desirable due to security or financial reasons. For example, if a strength of a security key is tested by rewarding possible successful attacks it may not be desired. Also, a complex task such as a space travel plan may lead to negative financial consequences if specific parameters (launch dates, supplies) become public too early. For this kind of tasks solution submission should be possible in such form that only the Reward Provider could read the solution. This approach will require additional handshake between supplier of the solution and the Reward Provider. One effect of this complication is that these scenarios should not allow additional reward contributions as any Reward Contributor will not have access to the winning solution due to its private nature.

One very important aspect of the task lifecycle is the situation when no reward is won. This happens when a task is either cancelled or it reaches the end of its active period without valid solution to be submitted. In this case the accumulated reward has to be returned to the Reward Provider and all Reward Contributors.

IV. Architecture of the System

There are several basic elements of the proposed system (Fig. 3.) that will make it run. For the prototype we chose EOSIO as a public blockchain technology. Some of the reasons for choosing this third generation blockchain are its flexibility for development, efficient programming language C++, support for Ricardian contracts, use of replenishable/free resources such as CPU and NET for operations and very short

ID	Task Duration	Private results	Allow Contributors	Allow Cancelation	Typical tasks	Examples
1	Infinite	No	Yes	No*	Theoretical	Counterexample for a hypothesis
2	Infinite	No	Yes	Yes	Research	Protein folding (improvement)
3	Fixed	No	Yes	Yes	Research	Protein folding (initial), Space travel (public)
4	Fixed	No	Yes	No	Practical	Divisor of a big number (public)
5	Fixed	Yes	No	No*	Practical	Divisor of a big number (secret), Space travel

Fig. 2. Several types of supported tasks

block producing time - 0.5 seconds and block confirmation times - 99.9% in 1.5 seconds, 100% confirmation in 3 minutes. The choice of public blockchain such as Ethereum and EOSIO technology [6] brings additional benefit that participants does not have to invest heavy in own infrastructure as block producers are paid by block producing rewards or blockchain inflation. For comparison a blockchain network based on Hyperledger Fabric or Corda would require most or all key participants to maintain their own hardware resources raising the costs for operation.

User Management is a key module that keeps track of blockchain accounts that represent on-chain participants and their relations with supported Task frameworks, Tasks, Rewards and Solution submissions. In many cases there are option an account that is not yet known to the system to execute operations. For example, this could be an anonymous Task Contributor or Researcher which first interaction with the system is claiming a reward for finding solution of one of the defined problems. In these cases, no user registration is required for the system to be used but the blockchain account will be added to the User Management data after the interaction, being it successful or not. On-chain collaboration is also an option for several individuals or organizations to set clear reward boundaries by defining how rewards will be split on success. On-chain collaboration is an entirely optional feature which intention is mostly for sharing the visibility of participants for the achievement. If only monetary reward is concerned this could be achieved entirely off-chain as long as the partners trust each other for doing so.

Task Frameworks are a set public blockchain components that are open for contribution by developers.

The main parts for contribution are the Validation components and Task interfaces.

- **Validation components** are supplied and maintained by Framework Providers. It is important that they are stable and error-free contracts as they may be used for long time periods. Any changes to their interface have to be backward compatible to a large degree. It is strongly advisable that supported task frameworks are open source and could be validated by anyone involved.
- **Task interfaces** describe the technical parameters set by reward providers, as well as the format that the solutions are received. The period for which the rewards for finding a solution is a key parameter for such task. Another parameter is the type of competition. In some cases, the first validated solution may immediately receive the reward. In other cases, the problem may have many solutions and the first submitted solution may later be improved by other submissions. In this case the rewards are given to the best solution submitted in the configured period, if any.

Reward structure is a set of data that keeps track of the rewards offered for solutions of specific calculation problems and additional configuration data. A single reward may be as simple as one-to-one relationship between the token amount offered for problem's solution. They could also have complicated structure where one token amount may be assigned for a breakthrough in a variety of problems. Also, for each problems a variety of contributors may assign differently configured rewards. The native limitation is that the period of time for active secondary rewards (set by Task contributors that are not the original Task provider) should not extent the period of original task reward.

Reward type is a key parameter for the system that need

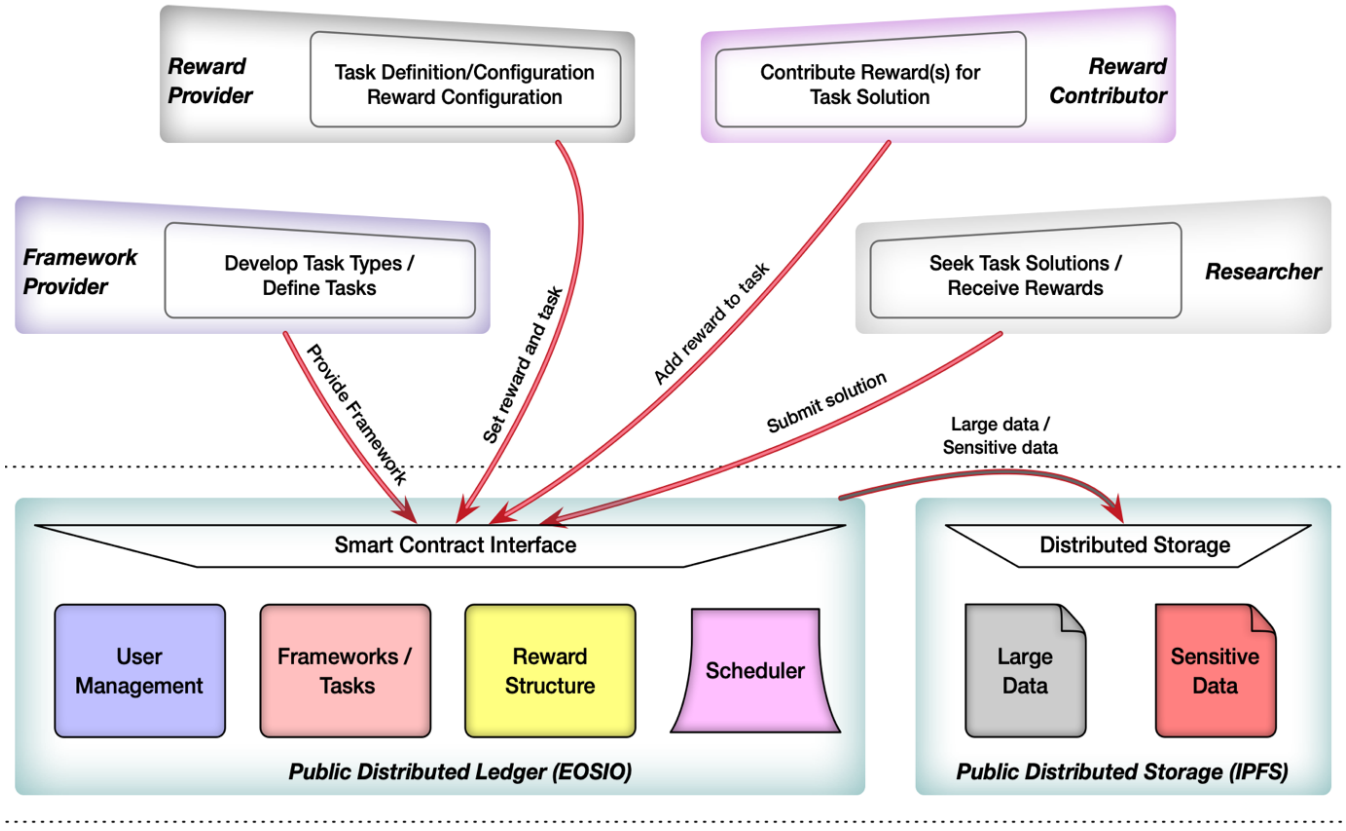

Fig. 3. Main actors and interactions for the system

to be considered. Each major public blockchain offers tokens as their default cryptocurrency. It is natural that rewards are offered and collected in blockchain's native currency. The main advantage for this approach is the simplicity for implementation and overall security.

The flexibility of modern public blockchains allows each dApp to offer and operate its own token. A solution with own currency attached may be used in addition to finance building and operating of such system. The drawback of such approach is the increased complexity of using the system by its users and additional fluctuations in its value.

Another approach is to set reward in a specific stablecoin is on the other side of the scale. Its rewards are independent of the fluctuations of the blockchain currency. Rewards set in stablecoin may be preferred due to the reduced risks of currency volatility.

The most complex approach is not to fix a single reward token and allow several tokens to be valid rewards. As this approach is most flexible and customizable it opens the system to new types of threads if no control is enforced on the allowed tokens for rewards such as custom malicious coding executed as part of normal token operations.

Reward target could be defined as flexible as the system allows. Each reward amount could be set for solving anyone of a predefined set of tasks. In their most flexible implementation, a single reward can be set for providing solution for problems defined in different task frameworks.

Scheduler component makes sure that rewards can be received after a predefined period of time. Its responsibility is to calculate and compare the submissions at the end of the configured period. In the specific case that there are no valid solutions submitted the rewards need to be returned to the Task provider and the Task contributors.

These are the key components for functioning of the system that are addressed in the EOSIO-based [6] prototype of the system.

V. Additional Factors to Consider

The proposed incentivization system differs from most "standard" dApps running on a public blockchain as the reward may be claimed with no restrictions. The monetary reward is "protected" by finding a solution to a puzzle that is clearly and openly defined. This difference makes normal public blockchain interactions vulnerable to specific attacks.

Denial-of-Service (DoS) type attacks could limit system availability and potentially prevent researchers from receiving their properly earned rewards. The natural solution for protection from DoS attacks is making sure all key resources for using the distributed system are provided by the participant that use the system functionalities. For example, these are the CPU, NET and RAM used for running an EOSIO-based system. Special case here is when the system tracks rewards

in several tokens. Without a maintained white list for allowed tokens in reward structure the system may be flooded with rewards in custom tokens that could be deprecated at any time. Setting pre-configured period for "receiving" the token rewards (claiming its RAM price) will protect the system's resources from being overwhelmed by unclaimed rewards.

Security/Protection of data. Interaction with public blockchains is typically done by sending signed message to a chosen blockchain endpoint. If one call is a solution to a problem, the submission theoretically could be intercepted at the endpoint, data from submission to be extracted and a new submission to be sent to blockchain, claiming the reward. Such man-in-the-middle attacks could be avoided by establishing a two-phase submission process. Initial call contains encrypted solution that set the time for submission. Once the system is set in "solution expected mode" the encryption key may be sent in separate calls potentially to several endpoints during the locked period for reward transfers. Timeout and costs for "locking" need to be chosen car

Private solutions. Sometimes the solution for which rewards are offered may not be public by nature. To address this case special handshake procedures, have to be established, based on zero-knowledge-proof, to make sure the key solution details are accessible only to the party/account that provides the rewards. Naturally, when solution's privacy is a requirement, the only Reward Contributor is the original Reward Provider as they are the only ones that may benefit from the solution.

Reward Cancellation/Expiration. Under some circumstances a reward(s) for specific problem can be canceled or its period could expire with no valid submission. Keeping information about who provided the rewards is essential in case the reward currency has to be returned to Reward Provider and Reward Contributors. A notice period for reward redraw should be in place to make the researchers know in advance that part or all of the rewards are canceled. The cancelation policy should be part of the initial task configuration to limit the possibilities for abusing the system. To avoid system abuse, certain small fees could be charged for removing parts or all of the rewards for solving a problem before the deadline is reached. This should not be possible for the original Reward Provider as various Researchers may have already invested significant efforts in finding a solution and possibly some Reward Contributors have already invested resources to incentivize the problem solution.

VI. Conclusions

In this paper we described and analyzed a distributed system based on public blockchain that can be used to incentivize research breakthroughs and collaboration. The proposed distributed system would allow many computational problems to be publicly shared. The rewards are set for every potentially anonymous participant that succeeds in providing their proper solutions. Some of the advantages of using the distributed application are its flexibility and transparency, by-design immutability, no-admin operations, as well as, its full traceability of both problem definition, reward structure and solution proposed. The developed EOSIO technology prototype covers the key roles and interactions for the proposed systems. In the paper was shown that even the simplest incentivization scenarios have to be built carefully to avoid many potential attacks specific for the third generation public blockchains.

Acknowledgment

The third author was partially supported by the National Science Fund of Bulgaria under Grant KP-06-N32/2-2019. The first and second authors were partially supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Bulgarian Ministry of Education and Science.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[2] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," 2014.
[3] Wikipedia: Protein Folding, 2020
[4] K. Dill and J. MacCallum "The Protein-Folding Problem," Science 338 (6110), pp. 1042-1046, 2012.
[5] Wikipedia: Proteopathy, 2020.
[6] D. Larimer, "EOS.IO Technical White Paper," 2017.