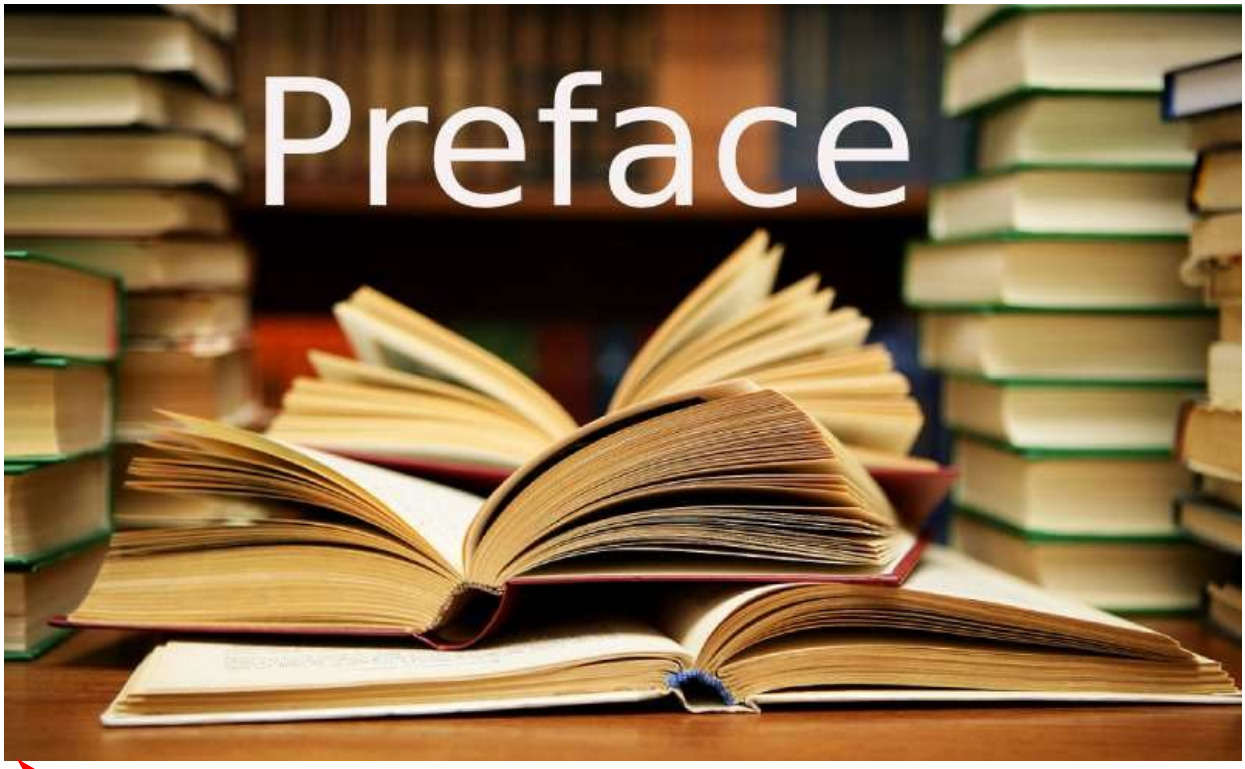
Daric (DAR)

Daric-coin.io

Contents



➢ Preface:

As the world becomes increasingly digital, cryptography is another natural step in the evolution of money. Daric is the first digital currency for everyday people to represent a major step forward in the adoption of cryptography around the world.

- **Our mission:** Create a cryptographic platform that is secure and managed by everyday people.
- **Our Perspective:** Create the World's Most Comprehensive Peer Market, Made by Daric, The Most Common Cryptocurrency Used in the World.
- **Disclaimer:** Since the Daric currency mission is as comprehensive as possible, we want to take this opportunity to introduce our blockchain network everywhere.

➢ Introduction:

Why cryptocurrencies are important ?

Currently, our day-to-day financial transactions rely on a trusted third party to keep track of transactions. For example, when you make a bank transaction, the banking system keeps its records and ensures that the transaction is safe and secure. Similarly, when Cindy transfers $ 5 to Steve using PayPal, PayPal maintains the original $ 5 record that is credited to Steve's account from Cindy's account and $ 5. Intermediaries such as banks, PayPal and other members of the current economic system play an important role in regulating global financial transactions.

The role of these trusted intermediaries also has limitations:

- **Unfair recording:** These intermediaries raise billions of dollars to create wealth, but they transfer almost nothing to their customers. Everyday people on earth, whose money drives a significant portion of the global economy. More and more people are going backwards.
- **Cost:** Banks and companies pay a lot of money to facilitate transactions. These costs often disproportionately affect the low-income population with the least choice.
- **Censorship:** If a trusted intermediary decides that you should not be able to move your money, it can impose restrictions on your money transfer.
- **Accessibility:** A trusted intermediary serves as a goalkeeper who can arbitrarily block anyone's presence on the network.
- **Nickname:** In a situation where privacy issues are urgently urgent, these powerful goalkeepers can accidentally disclose more financial information about themselves than you might want or force you to disclose information.

The Bitcoin system of "peer-to-peer e-cash", launched in 2009 by an unknown (or group) programmer Satoshi Nakamoto, was a time for freedom of money.
For the first time in history, people can exchange confidently without the need for a third party or a trusted intermediary. Paying in Bitcoin meant that people like Steve and Cindy could pay directly to each other, overcoming institutional costs, obstacles, and inconveniences. Bitcoin was, in fact, a currency without borders and power, and a link to the new global economy.

➢ Notice:

This Confidential Preliminary Product Whitepaper (this “Whitepaper”) has been prepared by Ronak DM, a Limited and private company based in Iran (“Ronak DM”), for use by purchasers to whom Ronak DM is offering the opportunity to purchase up to 20,000,000 of Daric, for the primary use in the Daric Platform (“Daric”)

Digital currency information (Daric)	
Main Unit	Daric
Subsidiary Unit	Sheqel
Symbol	DAR
Coins available	DAR 2,100,000,000
Saleable coins	DAR 20,000,000

➢ Coin story:

The Persian daric was a gold coin which, along with a similar silver coin, the siglos, represented the bimetallic monetary standard of the Achaemenid Persian Empire .

Cyrus the Great (550–530 BC) introduced coins to the Persian Empire after 546 BC, following his conquest of Lydia and the defeat of its king Croesus, who had put in place the first coinage in history. It seems Cyrus initially adopted the Lydian coinage as such, and continued to strike Lydia's lion-and-bull coinage .

Darius I (521–486 BC) introduced a new thick gold coin which had a standard weight of 8.4 grams, equaling in value 20 silver coins. The gold used in the coins was of very high quality with a purity of 95.83% and it bore the image of the Persian king or a great warrior armed with a bow and arrow. Their use ended with Alexander the Great's invasion in 330 BC, after which they were mostly melted down and recoined as

coins of Alexander. This is believed to be the main reason for their rarity, in spite of their widespread usage at the time .

Close to the end of the 5th century BC, the Persian satraps in Asia Minor decided to strike their own coins. Darius considered such encroachment a crime punishable by death since the right of coinage was treated as an exclusively royal prerogative. The numismatic evidence does not permit identification of the image on the darics and sigloi as anything but that of the king; it was adopted by Darius as a dynamic expression of his royal power expressly for his coin issues .

An Achaemenid daric, 4th century BC .

The coin is mentioned twice in the Hebrew Bible, where it is called the "adarkonim", as the Israelites came into contact with it when their Babylonian conquerors were conquered by Persia. The first Book of Chronicles describes King David as asking an assembly of people to donate for the construction of the Temple. The people gave generously "for the service of the house of God five thousand talents and ten thousand darics of gold, ten thousand talents of silver, eighteen thousand talents of bronze, and one hundred thousand talents of iron." Since David's reign is believed to be between c. 1048 and c. 1007 BC according to Old Testament chronology, the use of the daric is either an anachronism or a conversion by the writer into contemporary units.

“More than just a technological solution, Project Atlas offers a hopeful vision of humanity’s future .”

➢Transaction fee:

Similar to Bitcoin transactions, the costs on the Daric network are optional . Each block has a certain limit on the number of transactions in it . When there is no transaction, transactions are free . But if there are more trades, the nodes order them at the highest cost of trades at the highest cost, and only select the top trades to be included in the production blocks . This will open up the market. Execution: Costs are divided proportionally between nodes once a day . In each block, the cost of each transaction is transferred to a temporary wallet, from where it is distributed to active workers at the end of the day. This wallet has an unknown private key. Transactions inside and outside the wallet are forced by the consensus protocol of all nodes in the same way that consensus also disrupts the new Daric every day.

➢Economic model Daric:

We want to make sure that our users increase Daric because they help the network. Daric goal is to build an economic model that is advanced enough to meet these priorities while remaining intuitive enough for people to use.

- **Daric Economic Model Design Requirements :**

Simple: Create a visual and clear model .
Fair distribution: Allocate extensive access to the world's population to Daric .
Deficiency: To maintain a consistent price over time, create a sense of deficit .
Competent income: Help create and maintain a network

➢Formalization:

We use the perfect term to refer to nodes in a network that behave honestly and without error. In contrast, a defective node is a node that may be honest (due to information inaccuracies, administrative errors, etc.) or destructive .
We reduce the validity of a transaction to a simple binary decision problem: each node must decide on the information it received with a value of 0 or 1.

We define the collective process according to the following three principles:
1 (C1): Each flawless knot decides in a limited time .
2 (C2): All perfect knots reach the same amount of decision .
3 (C3): 0 and 1 are both possible values for all perfect nodes .
2.3 Existing Collective Algorithms: Much research has been done on algorithms that reach a collective agreement in the face of Byzantine errors .
Previous work has included the continuation of cases in which not all participants in the network are identified over time, and messages are sent asynchronously (there is no time limit for a separate node to reach a decision) and a definition between the concept process. There is a strong and weak mass.
The strength of a collective algorithm is usually measured in terms of the amount of defective processes it can withstand.
This proves that no error solution can withstand more than (n − 1) / 3 Byzantine error, or 33% of malicious network performance
. However, this solution does not require proper proof of the messages sent between nodes (digital signatures). If it is possible to guarantee that the messages are not forged, there are algorithms with much higher error tolerance in sync cases.
Several algorithms with greater complexity are presented to Byzantines in heterogeneous cases. FaB Paxos can withstand the Byzantine error

(n - 1) / 5 in a network of nodes, and this tolerance is 20% of the network nodes that encounter sabotage.

➢ The goals of formal consensus:

Our goal in this work is to show that the collective algorithm used by the Daric protocol in each open loop reaches consensus (even if the partial consensus of all transactions is rejected), and the partial consensus is obtained only with known probability, even in Facing Byzantine errors.

Since each node in the network only votes for suggestions from a set of trusted nodes (other nodes in its UNL), and since each node may have different UNLs, we show that There is only one consensus available for UNL membership. This goal is also referred to as preventing the "fork" in the network:
A situation in which two sets of nodes are separated and each reaches a consensus independently, and two different closed logs are observed by nodes in each node set.
Finally, we will show that the Daric protocol can achieve these goals in the face of errors (n - 1) / 5, which is not the strongest result, but we will show that the Daric protocol has several other desirable features to some extent. Too much increases its usefulness.