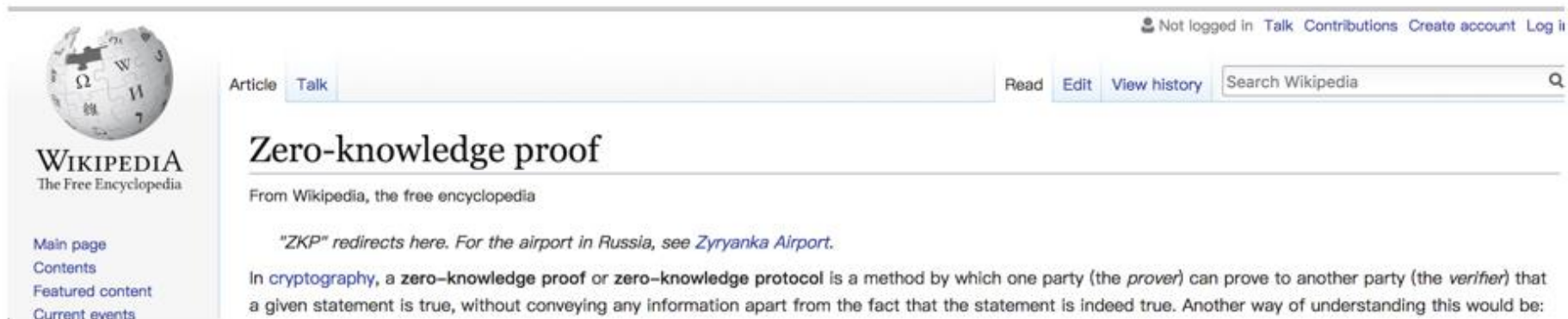


# 零知识证明

# 零知识证明是什么



The image shows a screenshot of the Wikipedia article for "Zero-knowledge proof". The page layout includes the Wikipedia logo and navigation links on the left, a search bar and user options at the top right, and the article content in the center. The article title is "Zero-knowledge proof" and it includes a redirect note for "ZKP" and a definition of the term in cryptography.

WIKIPEDIA  
The Free Encyclopedia

Main page  
Contents  
Featured content  
Current events

Not logged in | Talk | Contributions | Create account | Log in

Article | Talk

Read | Edit | View history

Search Wikipedia

## Zero-knowledge proof

From Wikipedia, the free encyclopedia

*"ZKP" redirects here. For the airport in Russia, see Zyryanka Airport.*

In **cryptography**, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true. Another way of understanding this would be:

零知识证明是指一方（证明者）向另一方（验证者）证明一个陈述是正确的，而无需透露除该陈述是正确的外的任何信息。

# 同态隐藏

- 如果 $x, y$ 不同，那么它们的加密函数值 $E(x)$ 和 $E(y)$ 也不相同。
- 给定 $E(x)$ 的值，很难反推出 $x$ 的值。
- 给定 $E(x)$ 和 $E(y)$ 的值，我们可以很容易地计算出某些关于 $x, y$ 的加密函数值。
  - 同态加法：通过 $E(x)$ 和 $E(y)$ 计算出 $E(x + y)$ 的值
  - 同态乘法：通过 $E(x)$ 和 $E(y)$ 计算出 $E(xy)$ 的值
  - 扩展到多项式

# 例子

- Alice 想要向 Bob 证明她知道一组数  $x$  和  $y$  使得  $x + y = 7$ , 同时不让 Bob 知道  $x$  和  $y$  的具体数值。

# 简单的版本

- Alice把 $E(x)$ 和 $E(y)$ 的数值发给Bob
- Bob通过收到的 $E(x)$ 和 $E(y)$ 计算出 $E(x + y)$ 的值  
(利用了性质3)
- Bob同时计算 $E(7)$ 的值，如果 $E(x + y) = E(7)$ ，那么验证通过，否则验证失败。

# 盲签方法

- 用户A提供SerialNum，银行在不知道SerialNum的情况下返回签名Token，减少A的存款
- 用户A把SerialNum和Token交给B完成交易
- 用户B拿SerialNum和Token给银行验证，银行验证通过，增加B的存款
- 银行无法把A和B联系起来。
- 中心化

# 零币和零钞

- 零币和零钞在协议层就融合了匿名化处理，其匿名属性来自密码学保证。
- 零币(zerocoin)系统中存在基础币和零币，通过基础币和零币的来回转换，消除旧地址和新地址的关联性，其原理类似于混币服务。
- 零钞(zerocash)系统使用zk-SNARKs协议，不依赖一种基础币，区块链中只记录交易的存在性和矿工用来验证系统正常运行所需要关键属性的证明。区块链上既不显示交易地址也不显示交易金额，所有交易通过零知识验证的方式进行。