Projeto de Formatura – Turmas 2017

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema:

Gavel: Uma Blockchain Editável

Sobre a Gavel Blockchain

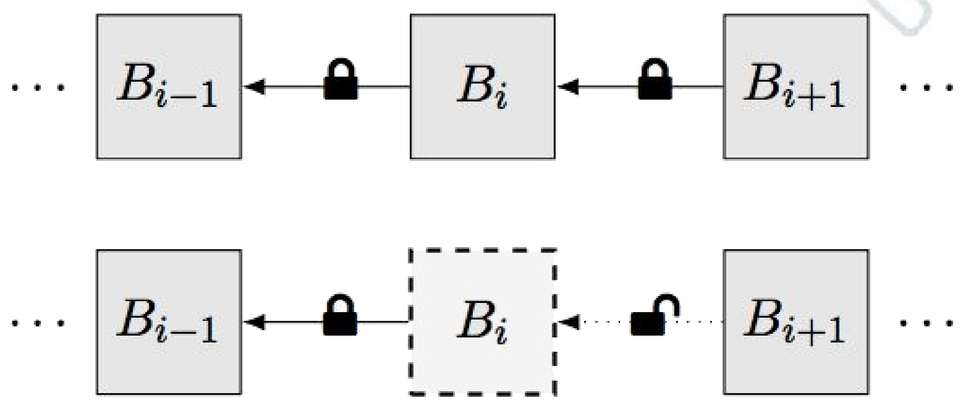
Blockchain é uma tecnologia usada para armazenar transações P2P sem a necessidade uma entidade central confiável.

Normalmente esses dados não podem ser alterados posteriormente. A Gavel no entanto é uma Blockchain que permite a edição de seus dados a partir do consenso de um grupo de usuários da rede, chamados de moderadores.

Como ?

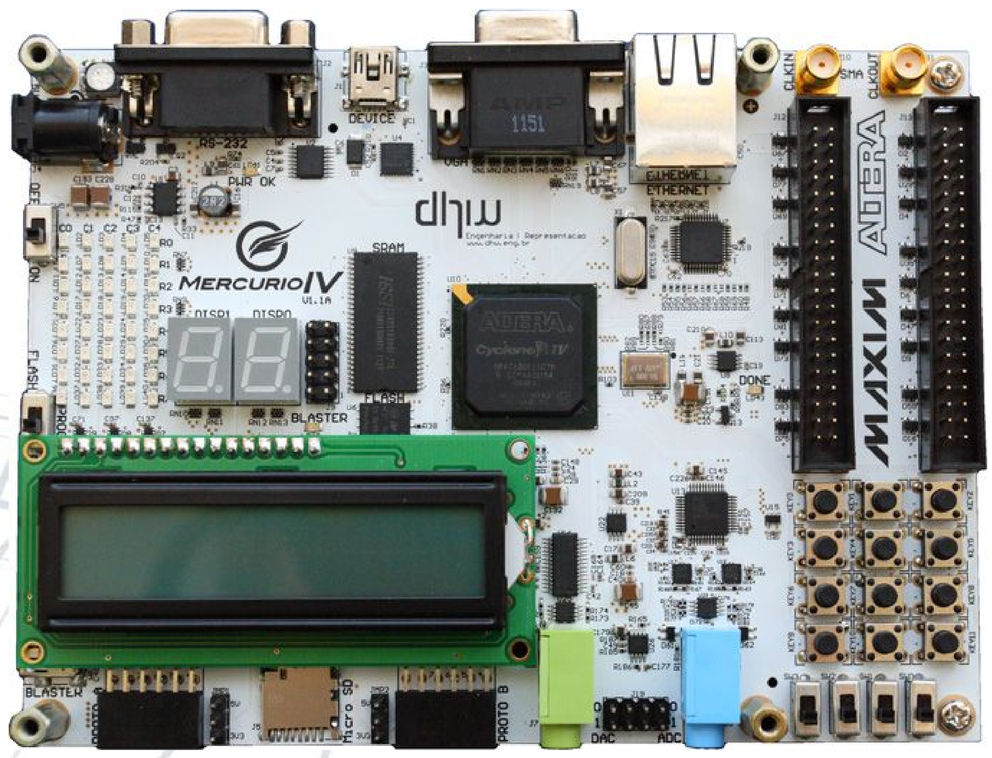
O Chameleon Hash é uma função que recebe uma mensagem a ser transformada e uma chave secreta, chamada de trapdoor.

Quando a chave secreta é conhecida, é possível encontrar colisões para um valor de hash.



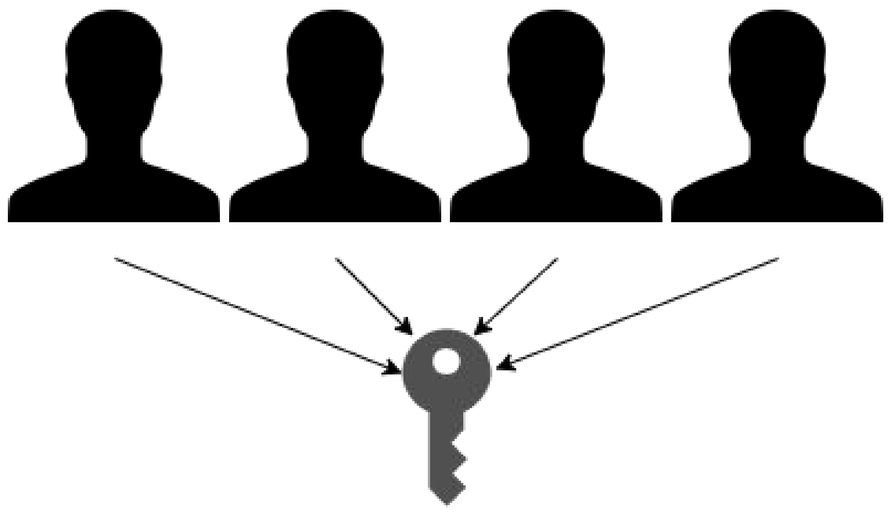
Hardware

Uma placa FPGA Macnica Mercurio IV foi utilizada para fazer o cálculo do Chameleon Hash e obter uma performance melhor em relação ao software.



Consenso para Edição

A chave para edição no Chameleon Hash é única, mas pode ser dividida em partes menores entre um grupo de moderadores para que a edição só ocorra mediante ao consenso.



Integrantes: Danilo Mendes Dias
Guilherme Livreri Stein Mamprin
Lucas Batista Gabriel
Manuel Conrado Puyol

Professor Orientador: Professor Dr. Bruno de Carvalho Albertini e Professor Dr. Marcos Antônio Simplício Júnior

Co-orientador: Professor Dr. Ewerton Rodrigues de Andrade