Branch: **master** ▾   Find file   Copy path

ethereum-analyses / README.md

amiller minor

`9fbdccf`   on 7 Jul 2015

1 contributor

Raw   Blame   History

108 lines (74 sloc)   7.08 KB

Ethereum Analysis: Gas Economics and Proof of Work

Overview

From January through March of 2015, Least Authority, conducted an analysis of Ethereum's Gas Economics and Proof of Work, in a consulting capacity with DEVolution, GmbH. The two analysis topics are independent and presented here as separate documents comprising this report:

- GasEcon.md : An analysis of the Ethereum Virtual Machine (EVM), its use of "gas" to compensate miners for the computational costs of verification, and the resulting economic effects. Includes an examination of contract composition and defensive programming strategies.

- PoW.md : An analysis of "Ethash", the Proof-Of-Work function which makes it difficult and expensive to attack Ethereum's consensus algorithm. We examine its goals ("GPU-friendly, ASIC-resistant"), compare it to existing techniques in the password-hashing literature, and discuss how it will need to evolve as conditions change.

- 2H Xȩ l ắủm l 'H ḳőĥ ĥ Ḧủ''Nủ ấẫmj mẳ ȩk H.HẺXI ḳẳȩ\XI XẫẫX ẫenj''őHḤXH.'' ủm

ŸXü ĖXḳőẼḧ

õ ḳ t \''ȩ''ĥ ẵ ḳ

- t ủ X HҚő ĥ m̧k m̧j ḳṇ ḳ ửkm X ̆ĥ ẤḠẫéX Ėử m̆ ĥ XXm̆ằḳ H.Hẳ̂ Ḧ ủ nj' Ḻ̇'HXȩ 6 ẵẳ enj\'' ĥ HẺXŰ m̆Hȩ ḳ \m̆ẳȩ ḳ ṬŰẳẺX ĥ ẫẫẫmj m̆ȩ nj\XHm̆ ȩ k Xȩẵ Ė'' Nủ X HI ẵ X m̆m \ẳểĥ
- bŰ ȩnj Xk Ṭ ẳẼ6X ȩXXI XI ẳȩ m̆ủX Nủ ủő HXĥ ṬŰȩ m̆ủX ửkm X ĥ nḤṬk ȩl nj ḳ NXXk HXHẺ\X 6Ẻ̆ \ẳểḤXṬ HIk ḳ m̆ủX HHẳ̂ Ḧ ủ ẳȩ\'' ĥ XNḦủ ĥ ẳȩ XHḳĥ
- b''ȩmH l m̆k'̆ '̂/̂6X\''ĥ H''ḳXI ĥ ố ủm̆k NXŰ\'''' HXH m̆ẳ ȩ 6XmṬXXȩ ĥ őm̆ő Ḛử ẵ m̆ḧ ḳ m̆ẳ enj H HẳX ṬẳẼ Xĥ őẳủX \ HXNửẺkm̆ő l ü ȩl Hẫnj' H ố k I XNXȩ ḳẳ X HḦ nHĥ ĥ ẳ enjĝ'' ĥ X\Ű ȩnj Xk m̆ m̆ủX t ẳm̆ő Ė̂ \ Űẳ ȩX \''őẺ 6Xĥ I Xm̆ẳ̂ H.H't Xm̆ủXk NXŰ̂''NủủXk X\''ĥ H'ḳẳ̂ẵ ȩkĥ ȩl ŰẳnjŰXủẺXt XẺ ȩ Ẻ̈kẳ m̆''Ḻ̇ ĥ ốkm̆6X I Xt XẺ HXI ĥ ḳŰXHḦ nHĥ ĥ ẳ enj XŰ ĥ HẺXk ẳȩ\Ẻ̂I XI ẳȩ ḳXHHXȩm̆ ȩl Nủ ȩl ẳȩ m̆ủX Ṭ ẳẼ HXNẺṬXI ȩl ẳȩ I Xĥ ő m̆XNḦHI Xĥ ''ȩkm̆Hm̆ ȩnj 6Xḳm̆HH \m̆ẳ Xkĥ
- KŰX\ốẺXm̆Ű m̆t Ẻ̂XHXĥ ẳȩk Ṭẳẫủm̆ủXHXḷẳḄXȩm̆őH'ȩ XŰ\XHẳ ȩṇ̆ẳk H Hẳẵ ốẺ̇HḚ̈ ḳő HHẳ̂k ẳ enj ȩl I ẳm̆m̆Ủ őẺm̆ Ṭ''Hẳ̇ HốȩI ĥ Ŷ XŰẳnjŰẺ̈ HX\''ĥ ĥ Xȩl \Ű ȩnj ẳ enj m̆ủẳk m̆ n̆t Ẻ̂X HXt XHm̆km̆ m̆ủX kXȩl XHőH'ȩ XŰ\XHẳ ḝ ȩĥ

t ủ ḳŰ ẼḤ'' Nủ'' Nủ̂Ŷ '' Hẳ́e

- t ủ X HҚőĥ ẳȩHHI ő\Xḳ ȩ''t XẺ c̆l̆d̆'Ğḋ ẼḤ''Nủ Nủ̂Ŷ ''Hẳ́e Ẻmj' Hẳ̂ ửĥ ĥ
- Aẳ ŰẳnjŰẺt XẺ Xḳẳ ȩnj' Ḻ̇m̆ḳőĥ ĥ Hẳ̂XI ḳ m̆ṕ Ėń őN̆ḥẳXȩl Ẽ̆m̆ĥ 2ğAẼ̂őḤXk ẳ̂Xm̆ȩm̆ HX HX ḳ''ȩ 6Ẻ̂X m̆Ṭ HIk \ŰẳXt ẳ enj ẳ̂ḳ ẳ enj XȩI XI X\''ȩ''ĥ ẵ XNXWk m̆ĥ
- t ủ ḳŰẳ̆ḳ6 ḳXI ''ȩ HȩI ''ĥ H m̆ủ̆k ''t XH NŰ̂XI HX I ẳ''ȩẺ̈I m̆kXm̆ĥṬŰẳ̆Űẳ̆k \Ẻ̂kXẺ̂ HXẺ̂mXI m̆ H.Hẳ̂HṬ''Hẳ́ẳȩ \ I Xĥ ẳ Ẻ̆m̆XHm̆ő HX''ȩ ĥ Xĥ ''Hủ̂ố''őȩI ẼḤ''Nủ Nủ̂Ŷ ''Hẳ́eHő'WWẺ̂Xk ȩl ''ȩXẼ ḳkṬ''HI § ḳŰẳ̆enj b''ĥ HXmẳ̂ẳ ȩ Nử Ẻ̂Xĥ
- KŰX\ốkm̆ĥ HȩI ''ĥ ẳW̆ẳ enj Nử̆ḷ \m̆ẳȩ ḳ őḳXI HXȩ''ȩốkm̆ȩl HI ȩl I ẳm̆m̆Ủ őẺm̆ \Hử̆H m̆ȩ Ė̂WXĥ6őm̆ủXü Ű'Ẻ̂ őHm̆ ḳẳ̂ HẺXkm̆mẳ̂m̆ẳ̆ Ė̂ Xḳm̆ĥ
- KŰX\''ȩl HXmX H Hĥ XmXHẳ̂W̆mẳ̂ ȩ ẳk Ẻ̈'' HX ḳ''ȩ 6Ẻ̂X6 ḳXI ''ȩ''őH ȩ ȩ Ẻ̈kẳ̂ ''NủőHHXȩm̆Ẻ̂ t ẳ̆6Ẻ̂X Ű HIṬ HXĥ
- KŰXHX ẳ̆ ḳ'' \ẳ Ė̇''ȩm̆H l m̆ĥ m̆Hȩ ḳẳm̆ẳ ȩ Ṭ ü Nḥ̆Hĥ ẼḤ''Nủ Nủ̂Ŷ '' Hẳ́e Ẻ̂m̆nnjXm̆ủ̆XĥN̆ủ̆Hủ̂X H HXẳ̆NḦHẳ enj nj' Ė̇'Nủ ẳẳ̂ enj kHXẳ̆ẳ Ẻ̂WXI Ű HIṬ HXI Xt XẺ̂Hĥ XȩmX\''ȩ''ĥ ẵ Ė̂ ẳ̆NXŰ ḳẳ̂őẺXĥ
- ŶX HX\''ȩl XHẺXI 6''őm̆ủX ḳ\ŰXI őẺXI I m̆kXm̆nḤṬ m̆ủĥ Ŷ X6XẺ̂Xt X m̆ủ̆ẳ̆k ĥ X\Ű ȩẳ̂ẳk ẳȩ XNXWk m̆ẳ̂X m̆ \Űẳ̆t ẳ enj ẳ̂ḳ ẳ enj Xȩl XI XNXWk m̆ĥ6őm̆ȩ'' mm̆XHm̆ẳ̂Ẻ̈ Ű Hĥ NủẼ̈ĥ

^ \ẳ enj HH őȩl

t ủ X HҚő ĥ

[illegible text]