

Verifiable Delay Functions (VDF)

Erdoğan Öztürk

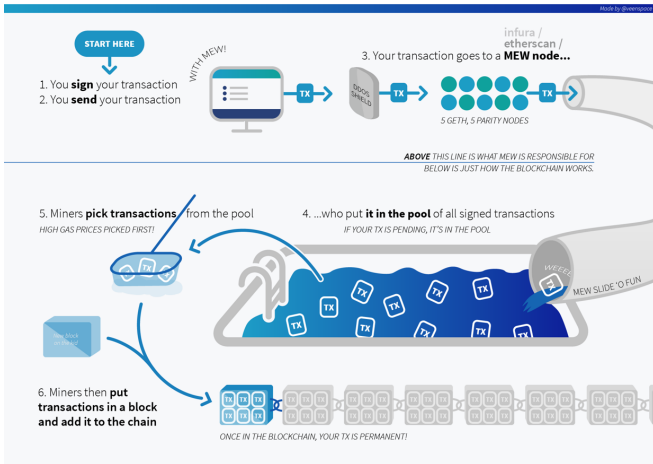
9.12.2019

Sabancı
Universitesi

Ethereum



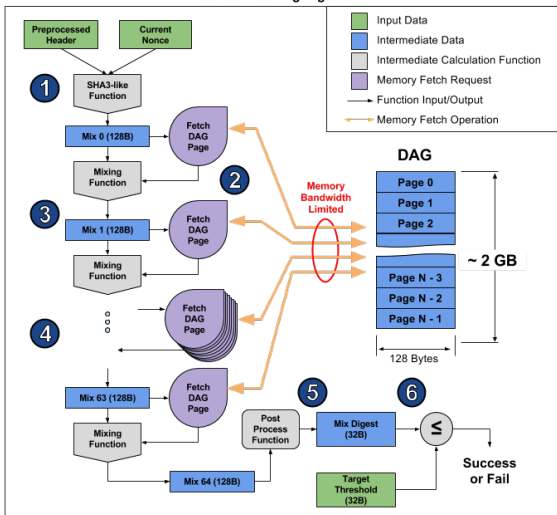
MyEtherWallet Behind-The-Scenes



URL: <https://kb.myetherwallet.com/en/transactions/what-is-gas/>

Ethereum Mining

Ethash Hashing Algorithm



Ethereum 2.0 (serenity) I

Here is a description of each basic solution Ethereum is working on to upgrade the network:

- Proof-of-Stake (PoS) solutions like Beacon and Casper refer to switching how Ethereum is mined. This addresses how the system is secured and how new coins are created.
- Sharding in general is splitting a large database into smaller more manageable parts, same general concept for the Ethereum network. This addresses issues of scalability and transaction speed and stops one app from slowing down the network.
- eWASM allows code to execute faster among other things. It expands coding options and capabilities for the Ethereum Virtual Machine.

Ethereum 2.0 (serenity) II

- Plasma is an extra layer that sits on top of the network that can handle massive amounts of transactions. It is the Ethereum version of Bitcoin's Lightning Network.
- Serenity is an upcoming major upgrade that creates a Proof-of-Stake chain that combines many of the above ideas (PoS, eSWASM, sharding, etc) into a new chain that would run tandem with and be fully compatible with the existing Proof-of-Work chain. This scaling and mining solution would not only partly change the way Ethereum is mined but also in theory would allow for faster transactions (and thus would create a better environment for smart contracts and DApps). In theory, Serenity could increase scalability by as much as 1000x (hopefully).

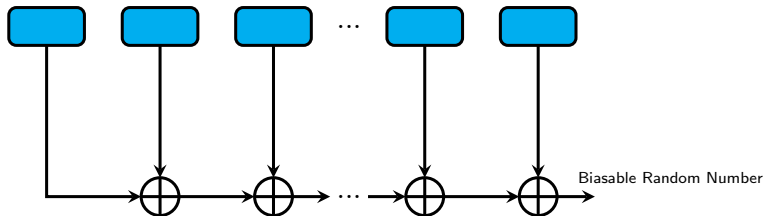
Randomness Beacon

Requirements:

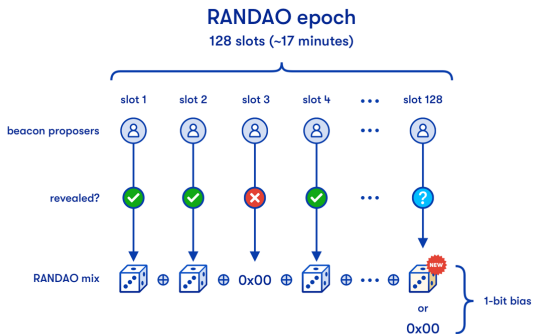
- Unpredictable
- Unbiasable
- Unstoppable

Problem: Generating Verifiable Randomness

Distributed Random Number Generation



RANDAO



URL: <https://quantstamp.com/blog/presenting-quantstamps-ethdenver-beacon-chain-implementation>

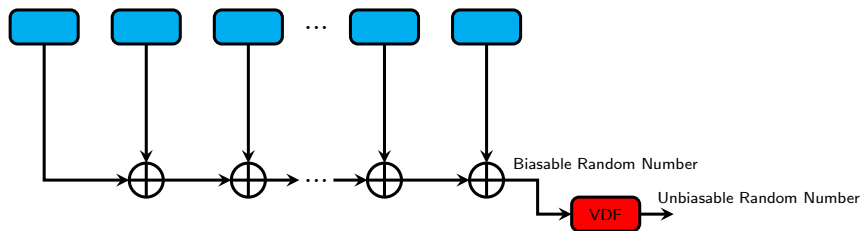
Randomness Beacon

Requirements:

- Unpredictable
- Unbiasable
- Unstoppable

Problem: Generating Verifiable Randomness

Unbiasable Random Number Generation



Dođrulanabilir Gecikme Fonksiyonları

Tanımı

Hesaplaması öngöröldüđü kadar sürmesi garanti olan, verilen girdiye karşılık tek bir sonuç çıkaran, yapılan hesaplamanın kolay bir şekilde dođrulanabildiđi fonksiyon ailesi.

Önemli ve Kullanılan Özellikleri

- Seri işlem içermesi
- İşlem sonucunun kesin olması

Doğrulanabilir Gecikme Fonksiyonları

https://vdfresearch.org

VDF Research Effort

Hello,

This is a collaborative effort to design and implement efficient VDF in software and in hardware, to make VDFs secure and usable in real systems.

What are VDFs?

Verifiable Delay Functions take a prescribed time to compute, even on a parallel computer, yet produce a unique output that can be efficiently and publicly verified.

Why do we need them?

VDFs have a wide variety of decentralized systems: *public randomness beacons, leader election in consensus protocols, and proofs of replication.*

Can we use them today?

Efficient VDF constructions exist today and can be implemented. However, if malicious actors have access to specialized hardware they can speed up their evaluation, breaking the security of the protocols that rely on VDFs :(

So, what's next?

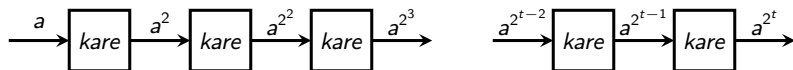
Ethereum Foundation, Protocol Labs, academic institutions and other collaborators are working towards designing and open-sourcing the fastest VDF hardware :)

- **Collaboration:** We are open to collaborate with academic institutions, manufacturers that can help improving our constructions and projects that want to participate in this effort.
- **VDF Competition:** We are organizing a competition to research the fastest VDF construction, get your maths and circuit optimization ready! TBA

Mevcut Tasarımlar

Time-lock tabanlı¹ : a^{2^t} hesaplama

- a^{2^t} işlemi için t defa kare almaktan daha kısa bir yol yoktur.
- t defa kare alma işlemi, paralelleştirilemez



¹R. L. Rivest, A. Shamir, and D. A. Wagner. *Time-lock Puzzles and Timed-release Crypto*. Cambridge, MA, USA, 1996.

Ethereum 2.0

- Ethereum Foundation, Protocol Labs, üniversiteler ve firmalar, mümkün olduğunca hızlı bir VDF donanımını açık kaynaklı bir şekilde tasarlamak ve üretmek için çalışıyorlar.

Ethereum 2.0'a dođru

VDF | FPGA Design Competition

Are you up for the challenge?

\$100,000 Prize to Forever Change Blockchain

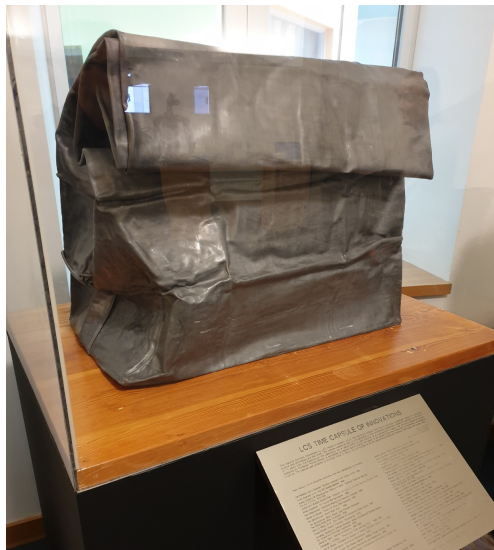
- ▶ **The problem:** Given 1024-bit input x , compute the verifiable delay function $h = x^{(2^t)} \bmod N$ as fast as possible.
- ▶ **Timeline:** The overall competition will run from Aug 1 - Dec 30, 2019
- ▶ **Prize:** The Ethereum Foundation, the Interchain Foundation, Protocol Labs, Supranational, Synopsys, and Xilinx are sponsoring a \$100,000 competition with support from AWS.

Read more

<https://www.vdfalliance.org/contest>



LCS35 Zaman Kapsülü



LCS TIME CAPSULE OF INNOVATIONS

This capsule contains innovations by LCS research leaders, which, the innovators believe, have had or will have a significant impact on computer science and technology and the world. The capsule, sealed as part of the Laboratory's 35th anniversary celebration, should be unsealed on the earlier side of 70 years from the inception of the Laboratory (on or about 2033) or upon solution of a cryptographic puzzle. The inherently sequential puzzle, prepared by Professor Ronald Rivest, is estimated to require approximately 35 years to be solved within the framework of expected technological progress. The capsule was sculpted by architect Frank O. Gehry, and symbolizes to us the Laboratory's motto of "forefront technology and human utility."

Sealed April 12, 1969
M. L. Dertouzos, Director
MIT Laboratory for Computer Science

There follows a list of innovators, innovations and year, alphabetically by innovator:

- Hal Abelson, Gerry Sussexin Scheme Language & MT Subject 6.001 1981
 Anant Agarwal, et al. The MIT Alewife Machine 1994
 Arvind, Gregory M. Papadopoulos, Rishiyur S. Nikhil Morenoon Dataflow Machine and the Id World 1978-1996
 Arvind, Larry Rudolph, Xaoxue Shen Computer Architecture via Term Rewriting Systems 1997
 Krste Asanovic TO Vector Microprocessor 1995
 Hari Babakrishnan Intentional Naming and Adaptive Transport 1999
 Bonnie A. Berger Theory of Virus Shell Assembly 1997
 Tim Berners-Lee World Wide Web 1989
 Tim Berners-Lee, Albert Vezza, Jean-François Abramatic The World Wide Web Consortium 1994
 Marc S. Blanc, et al. Zork: Earliest PC Interactive Fiction Game 1981
 Daniel Bricklin, Robert Frankston Spreadsheet 1979
 Sandeep Chatterjee, Shrinivas Devasdas MASC: Architectural Building Blocks for Networked Information Appliances 1999
 David D. Clark Internet Architecture 1981-1989
 Fernando J. Corbató Timesharing, CTSS and MULTICS 1963, 1969
 Jack B. Dennis Principles for Support of Modular Software Construction 1997
 Michael L. Dertouzos Information Marketplace 1979
 Michael L. Dertouzos, Joel Moses, Gerald L. Wilson Project Athena 1983
 Julie O'Brien Dorsey Stimulating Weathering and Appearance 1996
 Jon Doyle, Drew McDermott Reason Maintenance, Nonmonotonic Logics, and Reasoned Assumptions 1976-1983
 Peter Elias Convolutional Coding 1955
 Robert Fano Project MAC 1963
 Stephen Garland Tool Support for Formal Methods in Software Engineering 1991
 David Gifford The Boston Community Information System 1983
 James R. Glass, et al. SUMMIT: A Segment-based Speech Recognition System 1989
 Shafi Goldwasser, Silvio Micali Zero-Knowledge Interactive Proofs 1985
 Shafi Goldwasser, Silvio Micali Probabilistic Encryption 1982
 Philip Greenspun Toolkit for Building Online Communities 1998
 John Guttag Larch 1993
 Daniel Jackson Nitpick Specification Analyzer 1996
 Frans Kaashoek et al. Exokernel Operating Systems 1994
 David Karger, Lynn Stein Haystack 1997
 Alan Kotok Chess Program 1962
 Raymond Lau "Stuffit" Compression Algorithm 1987
 F. Thomson Leighton The Global Hosting System for Content Delivery on WWW 1998
 Charles Leiserson Hardware-Universal Interconnection Networks 1991
 J.C.R. Licklider Man-Computer Symbiosis 1960
 Barbara H. Liskov, Stephen Zilles Programming with Abstract Data Types 1974
 William Long Heart Disease Program 1980-1999
 Nancy Lynch Distributed Algorithms, Impossibility Results, Models and Proof Methods 1979-1999
 William J. Martin, Joel Moses MACSYMA for Symbolic Mathematics 1969-1983
 Leonard McMillan Image Based Rendering 1995
 Robert M. Malcafe Ethernet 1973
 Albert R. Meyer Polynomial-Time Hierarchy 1973
 Martin Rinard Credible Completion 1998
 Rivest, Shamir, Adleman RSA Public-Key Cryptography 1977
 Jerome H. Saltzer Making Project Athena Work 1984-1988
 Jerome H. Saltzer, David D. Clark, David P. Reed End-to-End Arguments 1980
 Robert W. Scheffler, James Gietty X-Window System 1983
 Stephanie Samet Probabilistic Hierarchical Language Modelling 1992
 Michi Sudrajat, Guruswami List Decoding of Reed Solomon Codes 1998
 Peter Szokovits Guardian Angel Patient-Centered Health Information Systems 1994
 Seth Teller City Scanning 1998
 David Tenenhouse Its Time to Get Physical, Real, and Out 1998
 Chris Terman RSM Circuit Simulator 1980
 Albert Vezza The Scout Project 1991
 Stephan A. Ward NuBus 1979
 Joseph Weizenbaum Eliza 1966
 Victor Zue, et al. Jupiter and other Spoken Dialogue Systems 1980-1999
 William H. Gates # Original Altair Basic 1975

LCS35 Zaman Kapsülü Kripto Bulmacası

- $2^{2^t} \bmod n$
- $t = 79685186856218$ (~ 80 trilyon)
- $n =$

63144660830728888937993571261312923323632988183308
41375588990772701957128924885547308446055753206513
61834662884894808866350036848039658817136198766052
18972678101622805574753938383082617597132189266686
11776954526391570120690939973680089721274464666423
31918780683055206795125307008202024124623398241073
77537051273444941695011809752418906679638587548563
19805507273709904397119733614666701543905360152543
37398252457931357531765364633198906465140213398526
58003419919039821928447102124648874593888535820703
18084289023209710907032396934919962778995323320184
06452247646396635593736700936921275809208629319872
7008292431243681 (616 digits)

LCS35 Çözümü

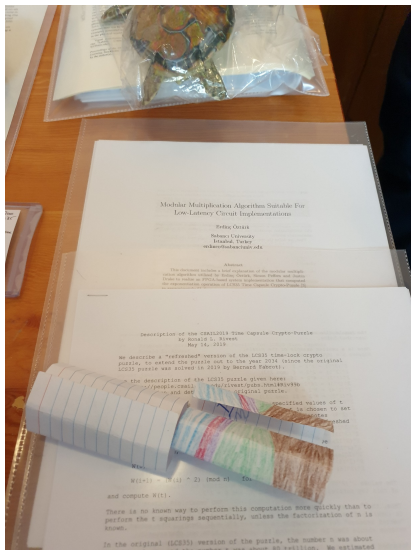
- $O(\log n)$ devre derinliğine yatkın Algoritma tasarımı
- FPGA tasarımı:
 - kare alma işlemi için ortalama 66ns
 - LCS35 bulmacasını ~ 2 ayda çözdü
- En hızlı yazılım (GMP kütüphanesi):
 - kare alma işlemi için ortalama ~ 1100 ns
 - LCS35 için gereken süre ~ 33 ay



Kapsül Açıldı!



Kapsül Tekrar Kapandı!



- $2^{2^t} \bmod n$
- $t = 2^{56} = 72057594037927936$

- $n =$
47480975472720128661750341306167738850512607449200564448671061963607104245581476
54252707604941012311775892012567579064620536874633385055919001167621577710311366
07205702942170513568430393481139013793780209643316395921689235118482669118001605
51988667965362300855232006835490669956721558390422829555915684946030611132920390
44753843846484807112228389204239581712931108919820250218586352043897306238872025
37819314111150742631144461349873631561421830476173554162699783903651772800068839
40156106181797688683420703951001476202956166958344408942411479055655678082981490
24668527045239650145862092904119412874007763041042314287604772876861294417664020
83279620913558718182645823558000382582372423580085016028485080973720098370355217
93546918638760444433778224398340793135780290856580785757312902447785956152294724
11326831502667425768520006371752963274296294506063182258064362048788338392528266
351511304921847854750642192694541125065873977 (925 digits)