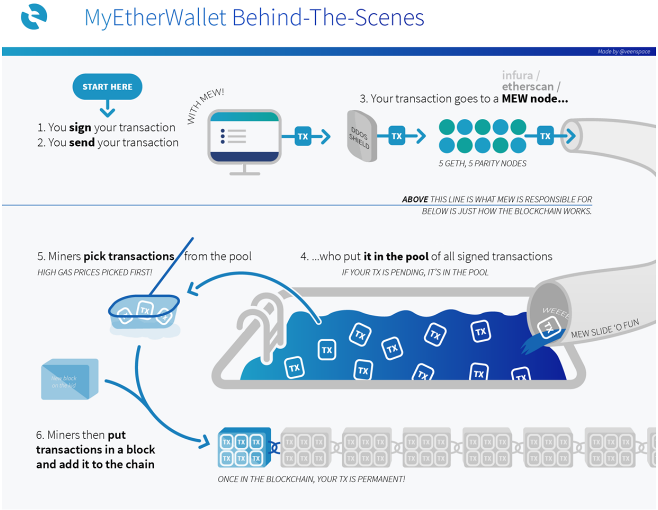
Verifiable Delay Functions (VDF)

Erdinç Öztürk

9.12.2019

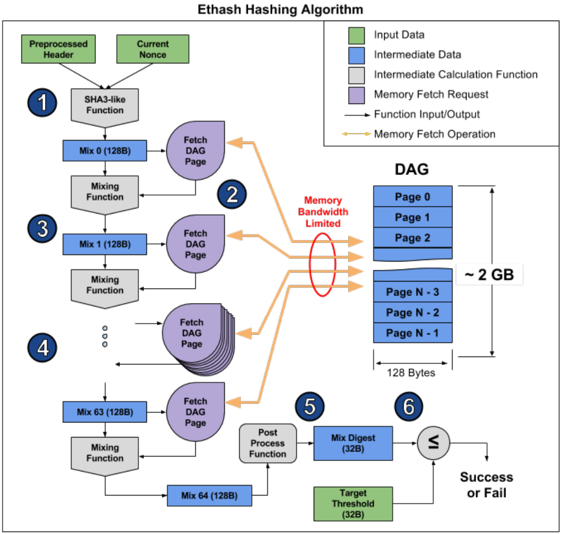
Sabancı Üniversitesi

Ethereum



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

Ethereum Mining



URL: https://docs.google.com/drawings/d/12yaGlsb5cz7IlWXcwgT6xXympFDVf84C6UrYkqHRipQ/edit

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 Lightening 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).

URL: https://cryptocurrencyfacts.com/ethereum-2-0-explained/

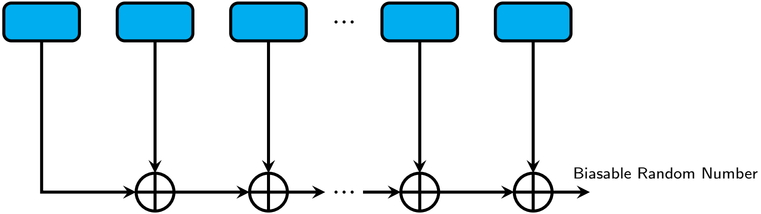
Randomness Beacon

Requirements:

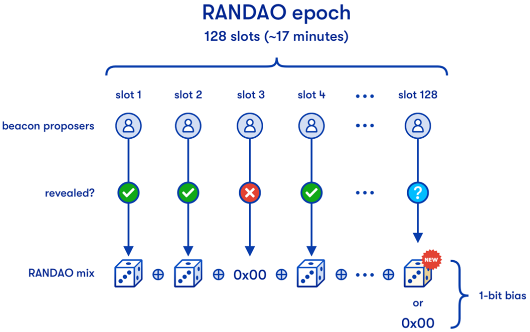
- Unpredictable
- Unbiasable
- Unstoppable

Problem: Generating Verifiable Randomness

Distributed Random Number Generation



RANDAO



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

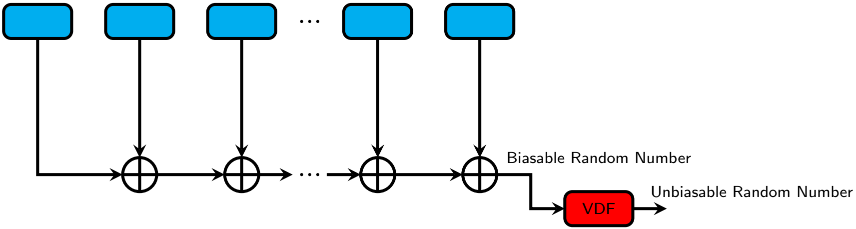
Randomness Beacon

Requirements:

- Unpredictable
- Unbiasable
- Unstoppable

Problem: Generating Verifiable Randomness

Unbiasable Random Number Generation



Doğrulanabilir Gecikme Fonksiyonları

Tanımı

Hesaplaması öngörüldüğü kadar sürmesi garanti olan, verilen girdiye karşılık tek bir sonuç çıkaran, yapılan hesaplamanın kolay bir şekilde doğrulanabildiği 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 :(

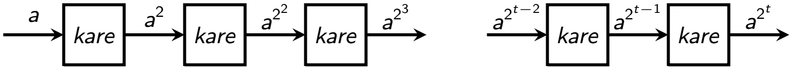
So, what's next?
Ethereum Foundation, Protocol Labs, academic institutions and other collaborators are working towards designing and open-sourcing the fastest VDF hardware :)

- **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 tabanlı[1] : a^{2^t} hesaplama

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

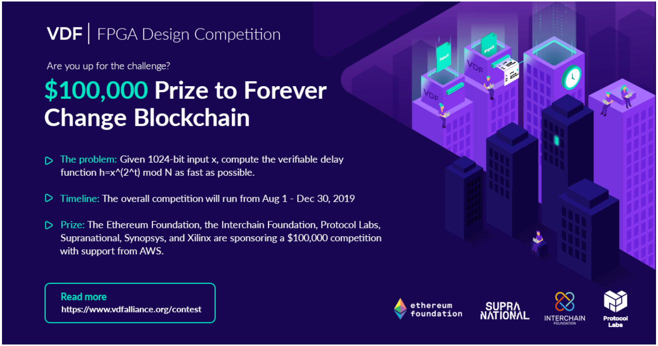


[1] R. L. Rivest, A. Shamir, and D. A. Wagner. *Time-lock Puzzles and Timed-release Crypto*. Cambridge, MA, USA, 1996.

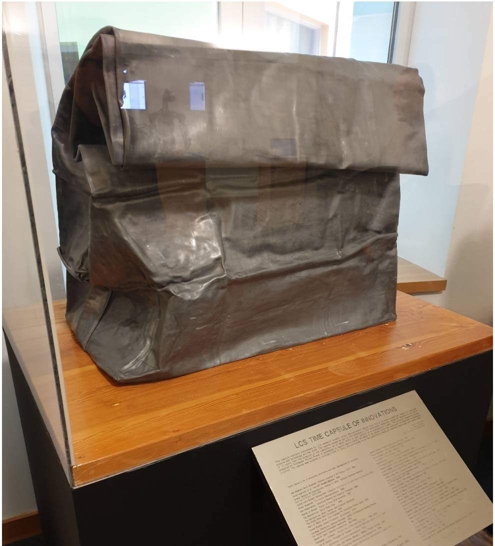
Ethereum 2.0

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

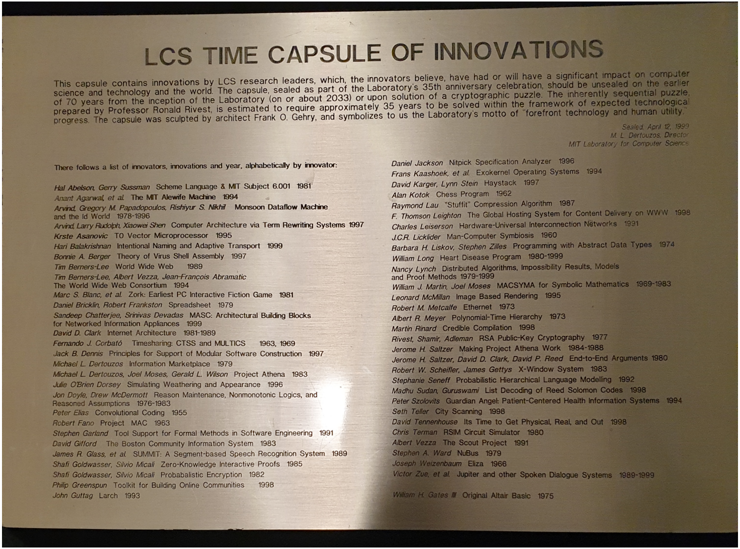
Ethereum 2.0’a doğru



LCS35 Zaman Kapsülü



LCS35 İçeriği



LCS35 Zaman Kapsülü Kripto Bulmacası

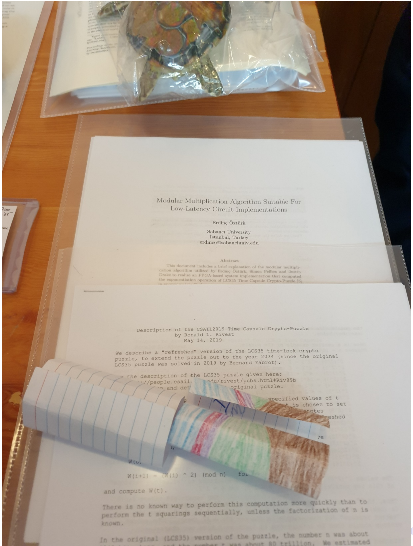
- $2^{2^t} \ mod \ n$
- t = 79685186856218 ($\sim$ 80 trilyon)
- n =
  6314466083072888893799357126131292332363298818330841375588990772701957128924885547308446055753206513618346628848948088663500368480396588171361987660521897267810162280557475393838308261759713218926668611776954526391570120690939973680089721274464666423319187806830552067951253070082020241246233982410737753705127344494169501180975241890667963858754856319805507273709904397119733614666701543905360152543373982524579313575317653646331989064651402133985265800341991903982192844710212464887459388853582070318084289023209710907032396934919962778995323320184064522476463966355937367009369212758092086293198727008292431243681 (616 digits)

LCS35 Çözümü

- O(logn) 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 ~ 1100ns
  - LCS35 için gereken süre ~ 33 ay

Kapsül Açıldı!

Kapsül Tekrar Kapandı!



Yeni Bulmaca

- $2^{2^t} \ mod \ n$
- $t = 2^{56} = 72057594037927936$
- n =
4748097547272012866175034130616773885051260744920056444867106196360710424558147654252707604941012311775892012567579064620536874633385055919001167621577710311366072057029421705135684303934811390137937802096433163959216892351184826691180016055198866796536230085523200683549066995672155839042282955591568494603061113292039044753843846484807112228389204239581712931108919820250218586352043897306238872025378193141111507426311444613498736315614218304761735541626997839036517728000688394015610618179768868342070395100147620295616695834440894241147905565567808298149024668527045239650145862092904119412874007763041042314287604772876861294417664020832796209135587181826458235580003825823724235800850160284850809737200983703552179354691863876044443377822439834079313578029085658078575731290244778595615229472411326831502667425768520006371752963274296294506063182258064362048788338392528266351511304921847854750642192694541125065873977 (925 digits)