



Haym @SalomonCrypto

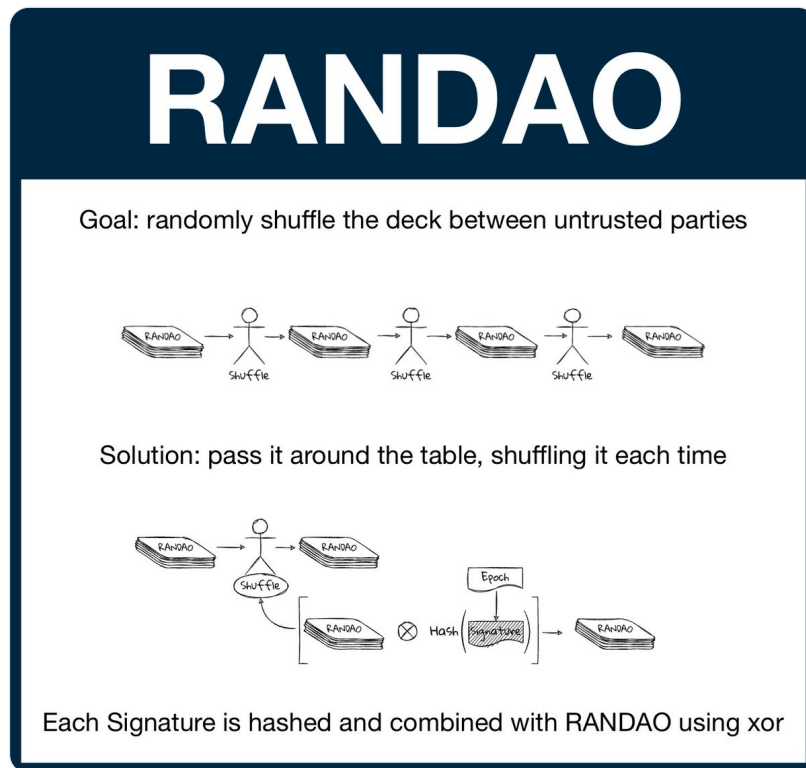
Oct 3 · 21 tweets · [SalomonCrypto/status/1576951211659390981](#)

Tr

(1/20) [@ethereum](#) Fundamentals: Randomness and RANDAO

Randomness is critical property for crypto and the World Computer. Unfortunately, computers are terrible at generating randomness without external input... and the EVM has no external input.

A guide to untrusted randomness.



(2/20) Randomness is a quality of unpredictability, an inability to foresee what comes next.

It is not a binary quality; some things can be more random than others. Weather seems random, but we can (try to) predict it; the lottery is (hopefully) completely random.

(3/20) In general, computers are supposed to execute in expected ways. The same input should generate the same output, every single time.

A computer that introduces randomness into execution would be practically unusable.

(4/20) And yet, there are clearly important applications that depend on credible randomness (for example, generating [@ethereum](#) private keys).

So where does this randomness come from? Computers (generally) rely on the concept of reasonably unpredictable external input.

(5/20) For example, a normal computer might use its users mouse movements as a basis of generating a random number. Mouse movements are very specific; it is very unlikely that two people will move their mice in the same way over a long enough period of time - intentionally or not

(6/20) [@ethereum](#) is the World Computer, a globally shared computing platform that exists between a network of 1,000s of computers, each running a local version of the Ethereum Virtual Machine (EVM).

Fortunately or not, the EVM is isolated from the outside world.



The image is a screenshot of a tweet from a user named Haym (@SalomonCrypto). The tweet is part of a thread, indicated by '(1/23)'. The text of the tweet describes Ethereum as the 'World Computer' and the 'future's internet-native global settlement layer', highlighting the Ethereum Virtual Machine (EVM) as its core. It includes a call to action to learn more about core \$ETH tech. The tweet features a large graphic with the text 'Ethereum Virtual Machine (EVM)' and a network diagram with the Ethereum logo in the center. The tweet was posted on September 27, 2022, at 4:33 AM. It has 375 likes and 21 replies. The interface shows options to 'Read the full conversation on Twitter', 'Reply', and 'Copy link'.

Haym
@SalomonCrypto · [Follow](#)

(1/23) [@ethereum](#) Virtual Machine (EVM)

Ethereum is the World Computer, the future's internet-native global settlement layer. The EVM is the core of Ethereum; it provides the world in which settlement and decentralized computation happens.

Read on to learn about core [\\$ETH](#) tech!



Ethereum Virtual Machine (EVM)

4:33 AM · Sep 27, 2022

[Read the full conversation on Twitter](#)

375 [Reply](#) [Copy link](#)

[Read 21 replies](#)

(7/20) One way to solve this issue is with oracles, a type of service that bridge information between the World Computer and the internet.

However, oracles are not native to [@ethereum](#). Relying on an oracle has external trust assumptions and can be very gas intensive (expensive).



The image is a screenshot of a Twitter post. At the top left is the user's profile picture, a small globe, and the name 'Haym' with the handle '@SalomonCrypto' and a 'Follow' button. To the right is the Twitter bird icon. The tweet text reads: '(1/20) @ethereum, Oracles and @chainlink: The Communication Layer of Web3'. Below this is a paragraph: 'How do smart contracts get info from outside the Ethereum blockchain? How can a protocol interact with a web2 service? How will The World Computer integrate with The Real World?'. This is followed by 'This thread has answers!'. The main content is a graphic titled 'Blockchain Oracles' in large blue letters. The graphic features a globe on the left, a black silhouette of a wizard with a staff in the center, and a blue geometric diamond shape on the right. Orange lines connect the globe to the wizard and the wizard to the diamond. A small 'Twitter: @SalomonCrypto' watermark is at the bottom right of the graphic. Below the graphic is the timestamp '3:44 AM · Aug 10, 2022' and an information icon. At the bottom of the tweet area is a link 'Read the full conversation on Twitter'. Below the tweet are interaction icons: a heart with '375', a speech bubble with 'Reply', and a link icon with 'Copy link'. At the very bottom is a rounded button that says 'Read 22 replies'.

(8/20) Instead, [@ethereum](#) relies on a RANDAO mechanism to create protocol-level randomness.

The RANDAO is a value maintained by the beacon chain; with each block, the proposer mixes in their own random contribution to the existing RANDAO value.

(9/20) Imagine you have a deck of cards you want randomly shuffled. One way to achieve credible randomness is to pass the deck around the table, with each person shuffling it in turn.

Even if one person tries to cheat, the cumulative result is still very random.

RANDAO

Goal: randomly shuffle the deck between untrusted parties



Solution: pass it around the table, shuffling it each time

(10/20) For [@ethereum](#), the chain maintains a RANDAO value. When a block proposer creates a new block, it adds in its contribution. You can see the contribution in the block (randao_reveal)

Each contribution needs to satisfy 2 properties: it should be unpredictable yet verifiable

Haym
@SalomonCrypto · Follow

(1/21) [@ethereum](#) Fundamentals: PoS Blocks

In less than 1 week, the Ethereum blockchain will Merge with the Beacon Chain and the World Computer will transition from PoW to PoS. The blockchain will never be the same.

A field-by-field guide to on-chain future.

10:28 PM · Sep 9, 2022

[Read the full conversation on Twitter](#)

481 [Reply](#) [Copy link](#)

[Read 37 replies](#)

(11/20) Early ideas for the RANDAO contribution had each validator create a "hash onion," a data structure built from hashing a random number repeatedly. However, this method is clunky and begins to fall apart with some edge cases.

Instead, [@ethereum](#) uses a different approach.

(12/20) A natural alternative became available when [@ethereum](#) changed its digital signature scheme to be built around BLS signatures

Tl;dr BLS signatures begin with external randomness used to generate private keys. These keys are used to sign messages, which are then aggregated

Haym
@SalomonCrypto · Follow

(1/12) Cryptography 201: BLS Digital Signatures

Digital signatures provide cryptographic assurance that a specific person sent a specific message. Their existence is critical, but traditional digital signatures are not scalable.

A manual for aggregation and acceleration.

BLS Digital Signatures

Public Keys
+
+
+
↓
Aggregate Public Key

Signatures
+
+
+
↓
Aggregate Signature

Aggregate Public Key + Message + Aggregate Signature → YES/NO

12:22 AM · Sep 29, 2022

[Read the full conversation on Twitter](#)

138 Likes · Reply · Copy link

[Read 7 replies](#)

(13/20) At the data level, an aggregate BLS key is identical to a single BLS key; they share the same size and use the same verification algorithm.

This property is extremely important for the consensus process, but it is particularly useful as a RANDAO function.

(14/20) With BLS signatures, every validator already has a closely guarded random number - their private key - achieving unpredictability.

Furthermore, every node can verify the RANDAO contribution just by verifying the BLS signature - achieving verifiability.

(15/20) Specifically, the RANDAO contribution is its normal BLS signature with the epoch number (think block number) as the message.

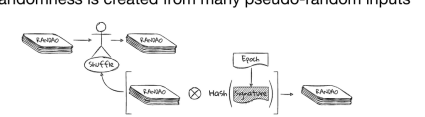
This contribution is both stamped into the block (randao_reveal) and mixed into the EVMs RANDAO value.

(16/20) In a RANDAO scheme, mixing is the process of combining the contributions; in our card metaphor mixing is shuffling the cards.

For [@ethereum](#), we first hash the BLS signature and then we mix this has with the previous RANDAO value using an operation called xor.

RANDAO Mixing

Randomness is created from many pseudo-random inputs



Each Signature is hashed and combined with RANDAO using xor

xor (exclusive or)

Compares two input bits:
- if they are the same, output FALSE (0).
- if they are the different, output TRUE (1).

Input A	Input B	Output
1	1	0
1	0	1
0	1	1
0	0	0

(17/20) Each time a new block is created, RANDAO is updated with just a little more randomness. And so, through the trustless contribution of every proposing validator, we generate a sufficiently random value.

This value is now available to both [@ethereum](#) consensus and the EVM.

(18/20) Practically speaking, if a dApp relies on true randomness, they are probably going to use a Verifiable Random Function (VRF) form an oracle like [@chainlink](#).

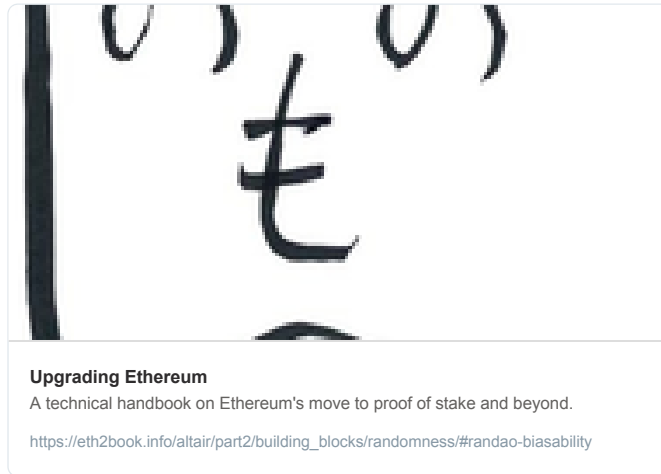
The true purpose of RANDAO is to provide randomness for consensus.

(19/20) A protocol that is fully predictable is very vulnerable. An attacker could:

- DDoS a proposer or a committee to attempt to halt the chain
- bribe an upcoming proposer
- attempt to register advantageous validator number to try to gain control over a committee
- etc


(20/20) [@ethereum](#)'s RANDAO isn't perfect, but it is very strong. For a deeper dive into some of the issues with RANDAO, check out this incredible resource.

But for us, RANDAO is good enough. Just think "RANDAO is random enough for Proof of Stake."



Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.

 **Haym**
@SalomonCrypto · [Follow](#)

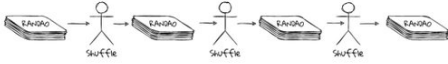
(1/20) @ethereum Fundamentals: Randomness and RANDAO

Randomness is critical property for crypto and the World Computer. Unfortunately, computers are terrible at generating randomness without external input... and the EVM has no external input.

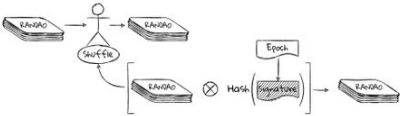
A guide to untrusted randomness.

RANDAO


Goal: randomly shuffle the deck between untrusted parties







Solution: pass it around the table, shuffling it each time



Each Signature is hashed and combined with RANDAO using xor

3:04 PM · Oct 3, 2022 

 [Read the full conversation on Twitter](#)

 3  Reply  Copy link

[Read 2 replies](#)

...