Ledger

Ethereum 2:
The Highly Anticipated Sequel
&
its Potential Impact on the DeFi Ecosystem

Jerome de Tychey

Ledger SAS
1, rue du Mail
75002 Paris - France

Ledger SAS
Parc Technologique de Sologne
Allée Georges Charpak
18100 Vierzon - France

Ledger Technologies SG PTE
9, Raffles Place,
Republic Plaza
Singapore 048619

Ledger Technologies Inc.
214 West 29th Street,
10001, New York, NY

About me

Ledger

Social media @jdetychey ; email: jerome.de-tychey@ledger.fr

March 2 - 4, 2021

Ethereum Community Conference 4

Maison de la Mutualité, Paris, France 🇫🇷

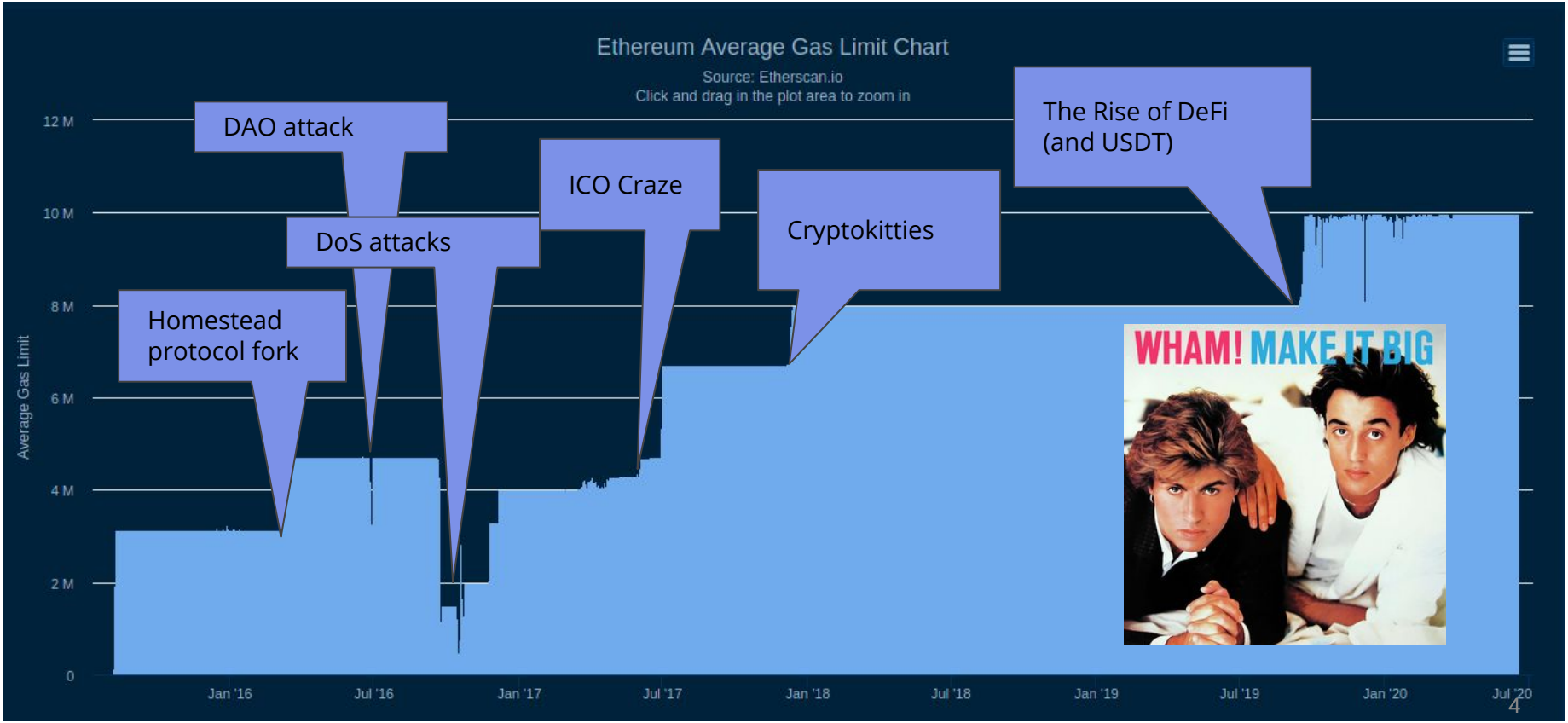
ethereum France

- Global Head of Client Success @Ledger
- Associate professor @CNAM in economics
- President of Ethereum France
- Hosting EthCC every 1st week of March

Previously on Ethereum

Ethereum 1.0

Ethereum so far, a great season 1



The EVM Franchise

Build on top, with or advertised as *better* than the Ethereum Virtual Machine

Ledger

EOS™

vechain

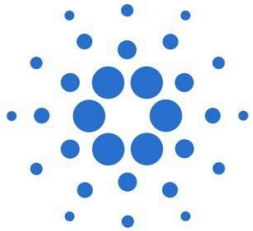
QuarkChain

QTUM

TRON

BINANCE CHAIN

tezos



CARDANO

HYPERLEDGER BURROW

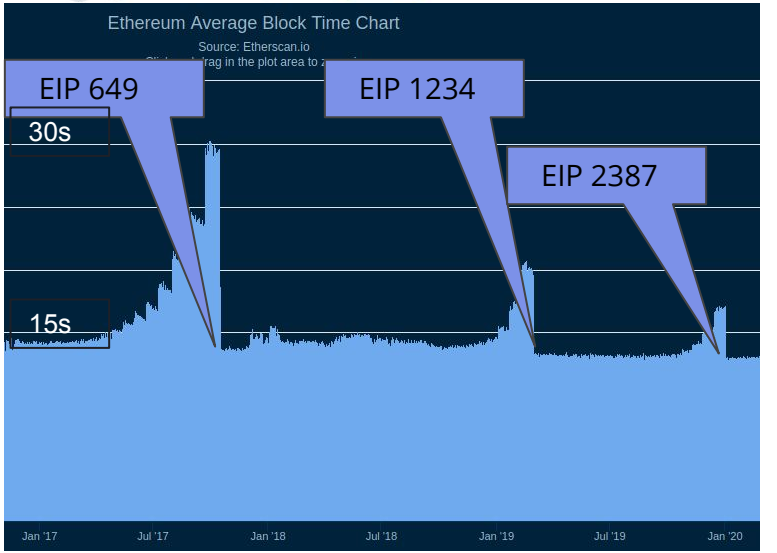
RSK SMARTER BITCOIN

NEO smart economy

The Delays.

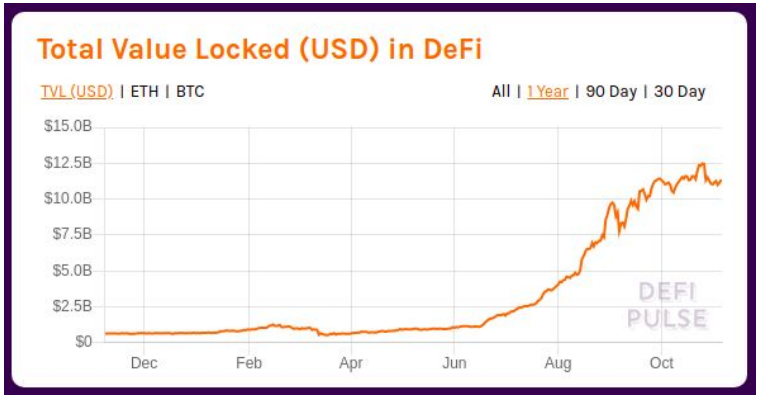
Short term goal, strong commitment and research dead ends

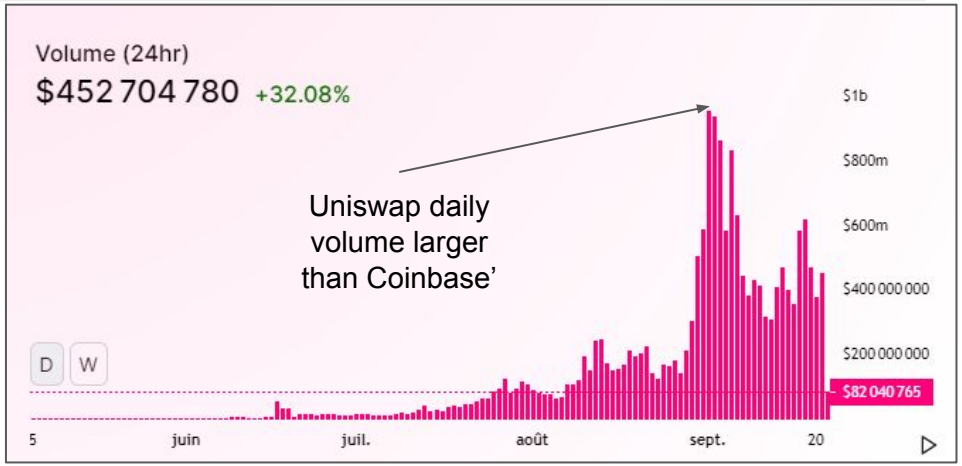
- **Proof of Stake transition was the target in 2014**
- **Difficulty Bomb / Ice-age introduced with Thawing Frontier fork (Sep. 2015)**
- **Push backs: Byzantium (Oct. 2017), Constantinople (Feb. 2019), and most recently Muir Glacier (Jan. 2020), next one ? July 2021.**
- **Vlad Zamfir: History of Casper (1,2,3,4 & 5)**
- **Ben Edington: Exploring Ethereum 2.0 Design Goals**
- **Eth2 specs stabilization in early 2020**



Meanwhile in DeFi

2020, a year full of DeFi





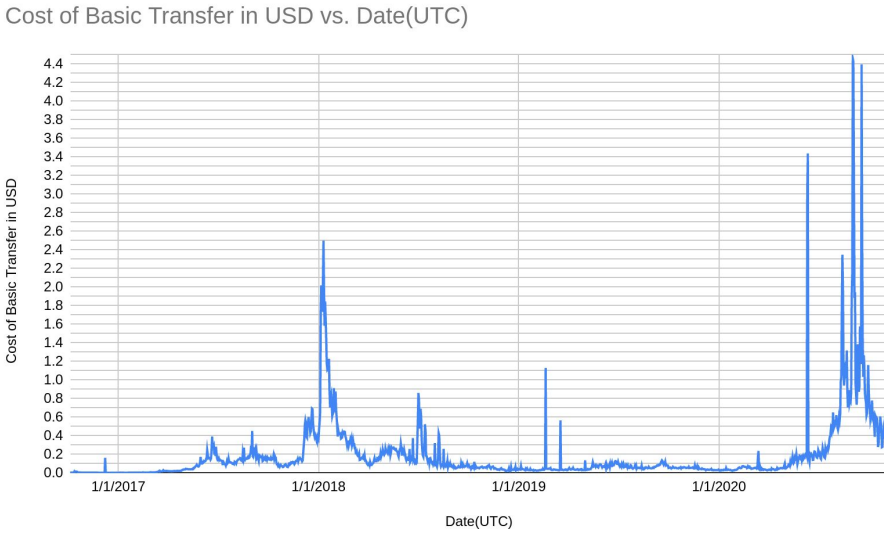
Key takeaways :

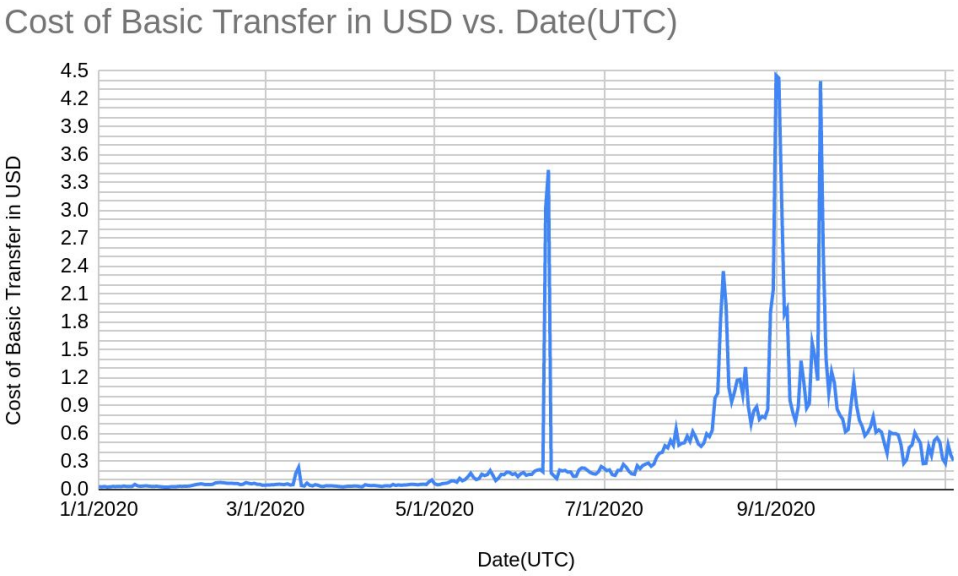
1. 11,3 Bn$ are locked in DeFi applications, "*everything"* is on Ethereum
2. **ICO Boon and Money Legos: ICO brought** tons of existing assets asking to be put at work + powerful well audited standards and easy to use mature tech stack
3. Lightning Network has 14,8M USD while 2.2Bn USD of BTC have been wrapped on Ethereum
4. DEX "can" technically handle big volumes - similar to centralized exchange
5. Several DEX are available (Uniswap, SushiSwap, 1inch…) and derivatives, lending, online court, predictive market, pegging...

Meanwhile in DeFi: Gas Guzzling

Ledger

Immediately correlated with huge gas price pump and overloaded network





Data: Etherscan + Kaiko

Key takeaways :

1. **The system is not broken**, many services emerged like relayers or gained in usage like gastoken
2. A technical improvement is being tested and soon implemented: EIP-1559

Ledger

~~Coming next:~~

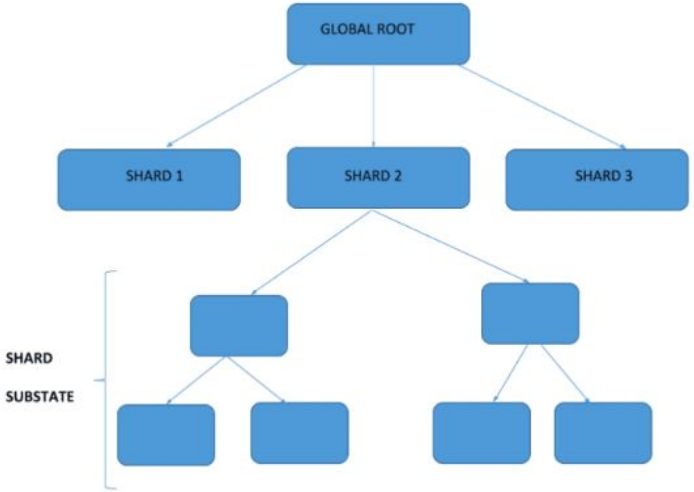
Available Now: Ethereum 2

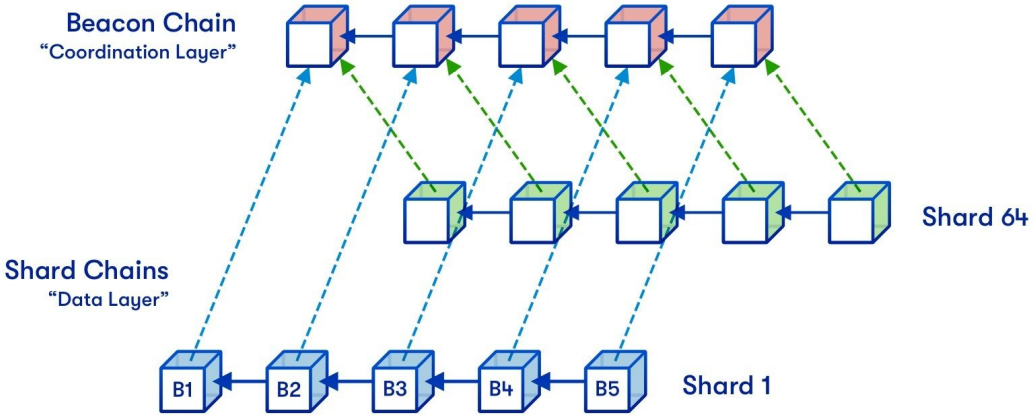
What's Ethereum 2?

Decentralization, Resilience, Security, Simplicity, Longevity.

64 Shards orchestrated by the Beacon Chain for cross-shard communication, finality and RNG.

Each shard with it execution environment.





What's Ethereum 2?

Ledger

The rollout

Phase 0 "Beacon chain"

- Deployment of the Deposit contract on the mainnet (Eth1 POW)
=> Done Yesterday!
- Genesis block and start of the Beacon Chain with POS consensus (Casper - Friendly Finality Gadget) for finality
=> Scheduled for Dec. 1st

Phase 1 "Shard chains"

- Launch of the first shard
- Cross shard communication
- Beacon chain locked Ether can move

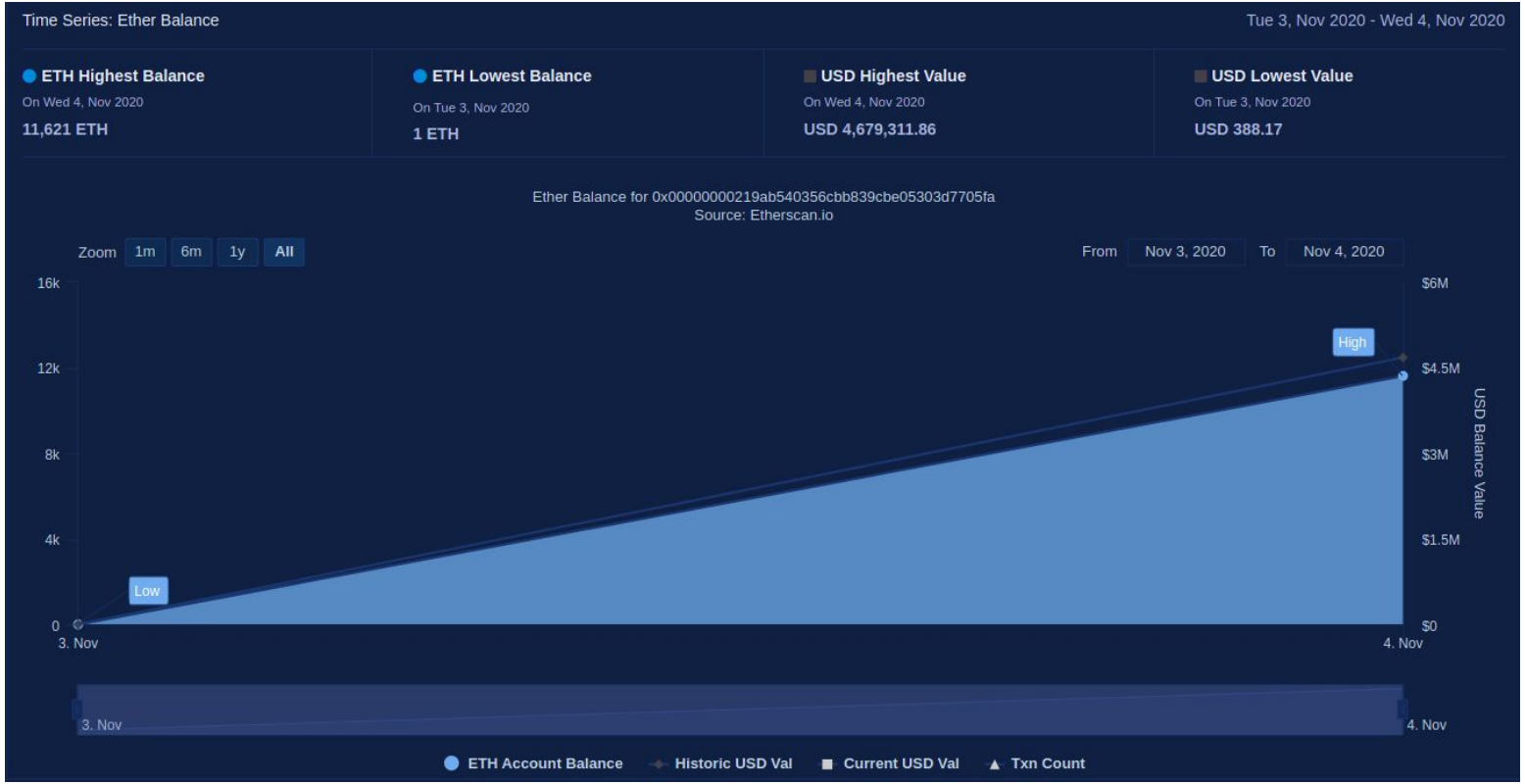
Phase 2 "State execution"

- eWASM on each shard
- High flexibility in the set up of new shards

What’s Ethereum 2?

Ledger

To start the beacon chain we need 524,288 ETH in the deposit contract (16,384 validators)



19,877 ETH deposited in the last 24 hours, at this rate we are done in 26 days

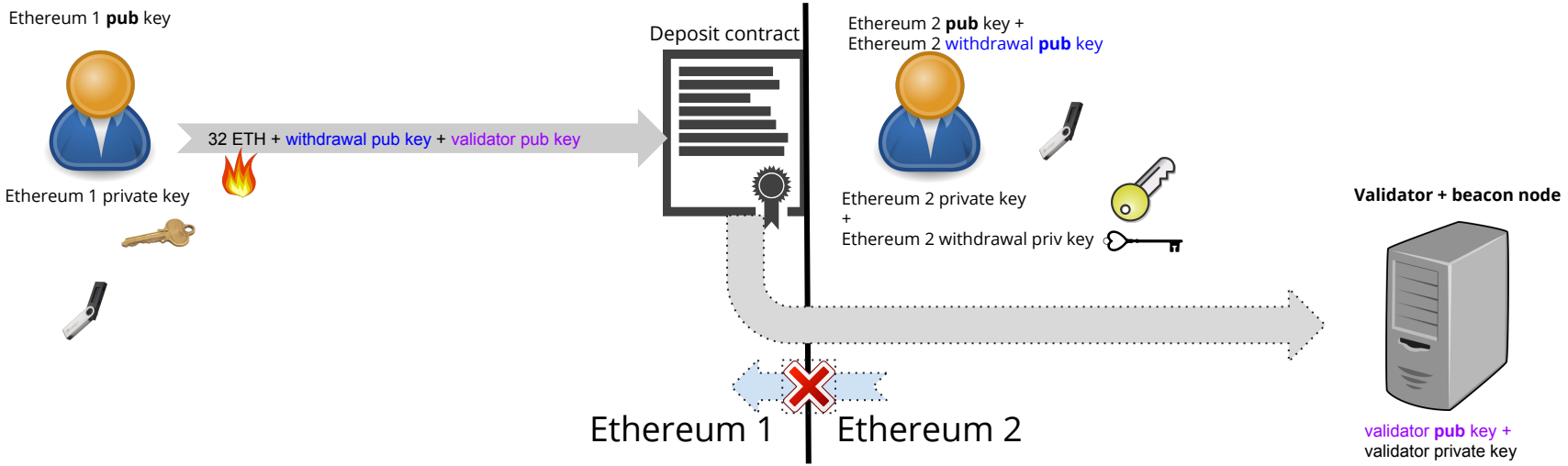
Getting ready for phase 0

Ledger

The Deposit contract

The deposit Function requires **32 ETH** and take 4 arguments

- ***Pubkey (bytes[48])***: a BLS Key that would be used by the validator, -Validating Key-
- ***Withdrawal_credentials (bytes[32])*** : the hash of a BLS Key that would be used to withdraw funds at later stage,
- ***signature: bytes[96]***: a BLS signature by Validating Key (aka ***Pubkey***) on the ***Deposit_data_root***
- ***Deposit_data_root (bytes[32])***: the hash of the deposit data.

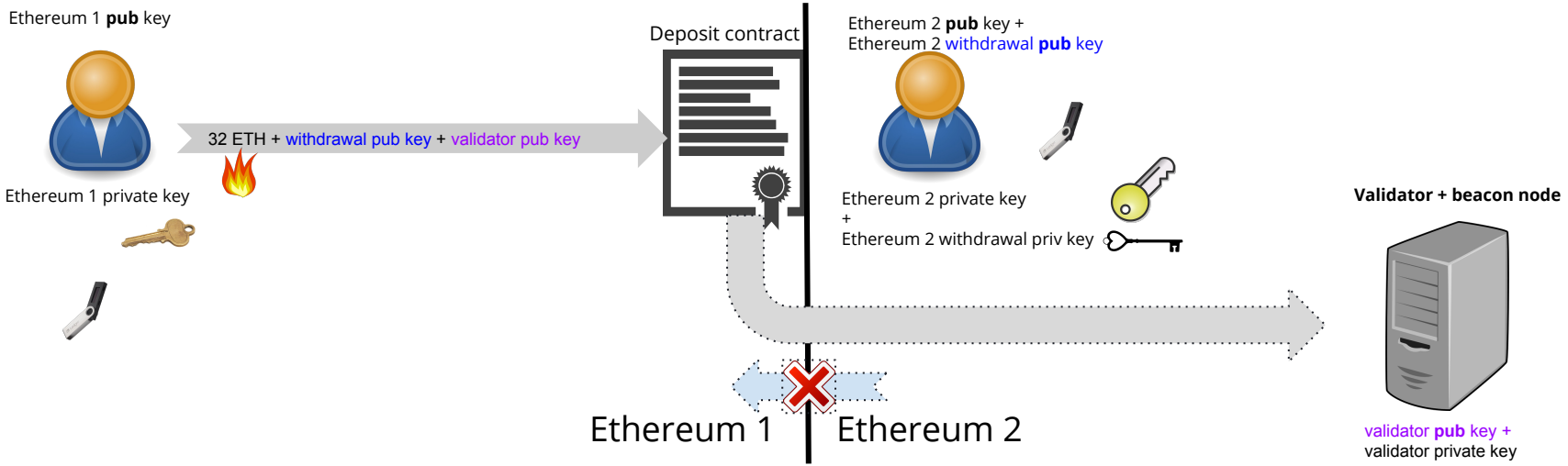


Getting ready for phase 0

Ledger

The Deposit contract

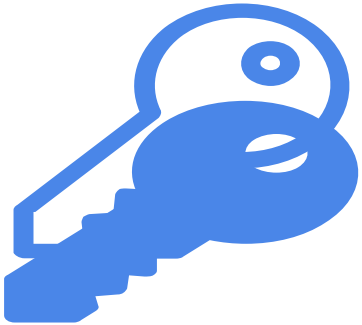
- **Users will call a *deposit contract* on Ethereum 1 to "transfer" their ETH to the beacon chain and several information must be provided (withdrawal pub key + validator pub key)**
- **ETH deposited appear on the beacon chain. They can't be retrieved on the POW chain**
- **Unlike other POS chain, user cannot delegate on Ethereum 2, in fact everything is designed to make delegation impossible**
- **To enjoy staking reward, users must "assign" their funds to an Ethereum 2 node, in other word the Ethereum 2 node will need to have access to the Validating Key (public & private), exiting the validation requires the validating key (!)**



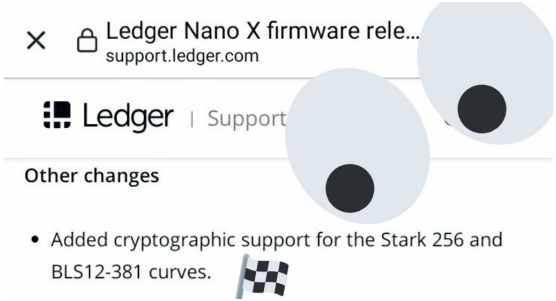
Getting ready for phase 0

Ledger

Securing the critical key pairs



Withdrawal key

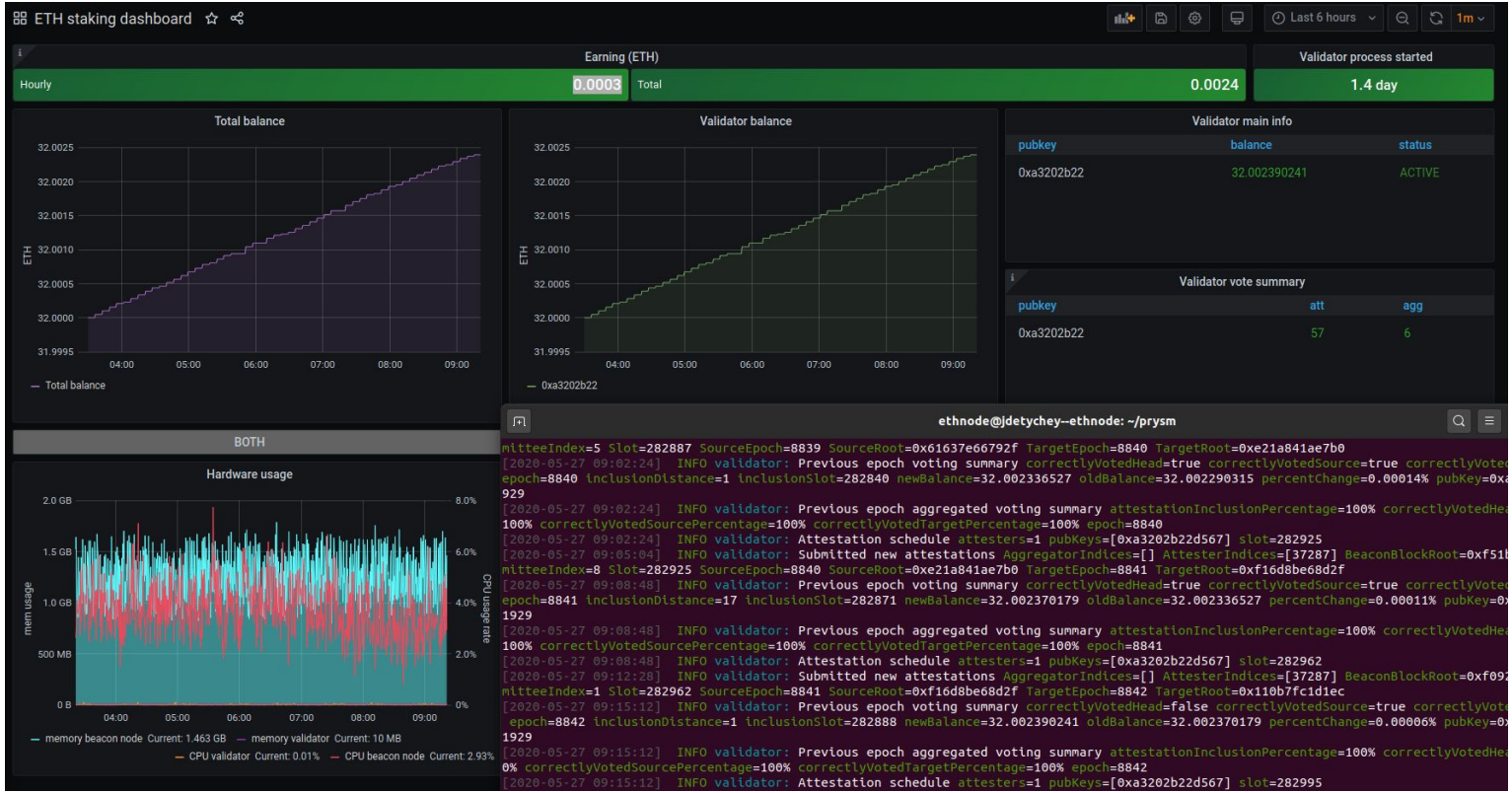


Validating key

Running a node

Ledger

It’s easy, seriously. It can run on Raspberry pi4 (8go RAM).



Core i9 9880H ; Bundle 16go DDR4 - 1TB M.2 SSD installed Ubuntu 20.04

Staking: get rewarded for bringing security and finality to the blockahin

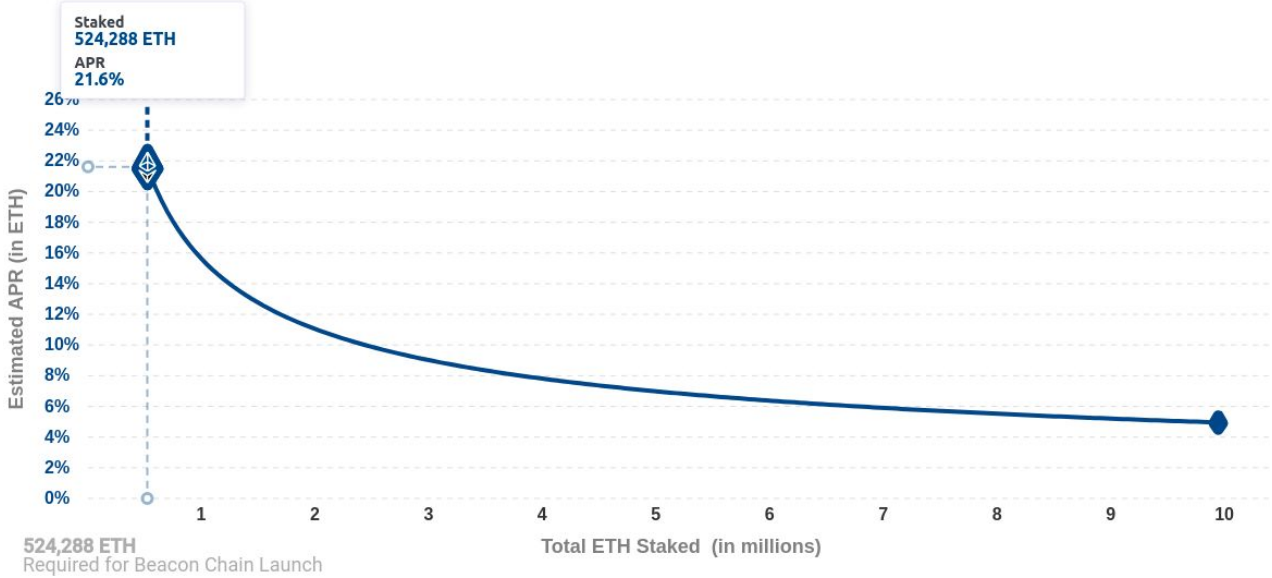
Ledger

https://launchpad.ethereum.org/

Staking and rewards

Validators get rewarded for proposing and attesting to blocks. The rewards are tied to the overall amount of ETH staked in the network.

Learn more about the economics of eth2 →



Timeline

Ledger

2020 (July / August/ Sep.)	2020 (October, November)	2021	2022
Beacon chain ***multi-client testnet***	**Beacon chain Main net launch**	**Phase 1 Shard Chains**	**Phase 2 State Execution**
Multi client testnet for Ethereum 2.0 is well tested.	Deposit contract is activated on Ethereum mainnet. ETH1 are being deposited as ETH2. Once the threshold of minimum staked ETH2 is reached, the network goes Live.	**July?**	

Ledger

What’s in it for DeFi?

What to expect?

Ledger

Short term:

- Lending rates for ETH can be expected to rise
- Less ETH on Centralized exchanges if they don't offer staking
- Staking pools: similar to PoW mining pools but for ETH2 at Stake => Wrapped ETH2 and return rate derivatives

Mid term:

- BLS allows for simple threshold signatures that can find application in DeFi

Long term:

- Massive Scalability with Cross-Shards communication
- Order book-based exchanges thanks to L2s and Scaling but will institutional liquidity come?
- Fixed rate borrowing and lending: currently the main loan instruments are floating rates.

Ledger

Discussion

DISCLAIMER

The information in this document does not constitute legal or investment advice and is not intended as a recommendation for buying or selling cryptocurrencies. Ledger SAS and all other companies mentioned in this document will not be responsible for the consequences of reliance upon any opinion or statement contained herein or for any omission.

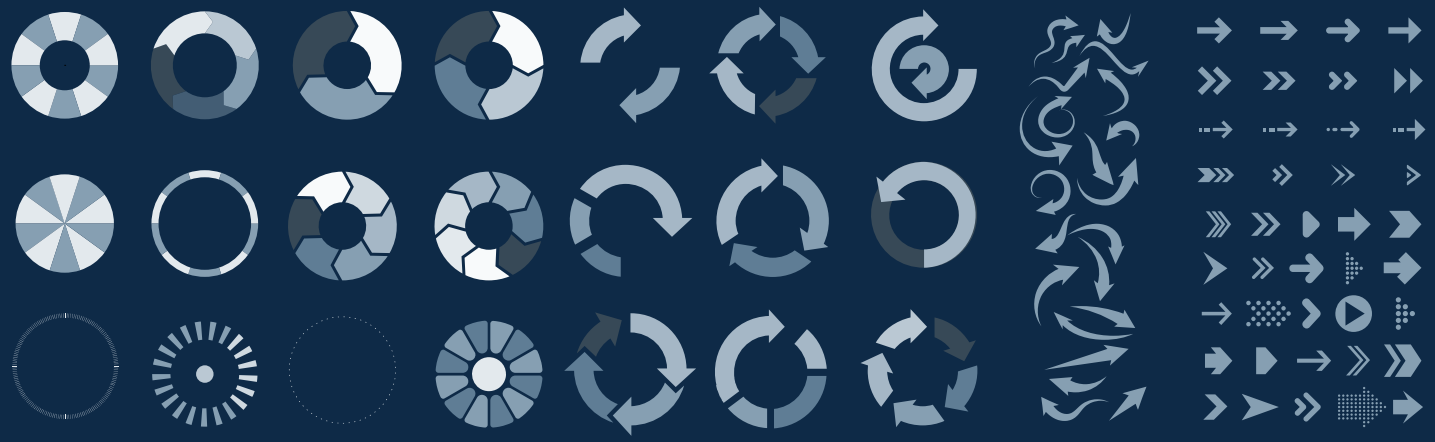
You must not rely on this document or any information therein as an alternative to seeking legal advice from your lawyer and/or other professional legal service providers.

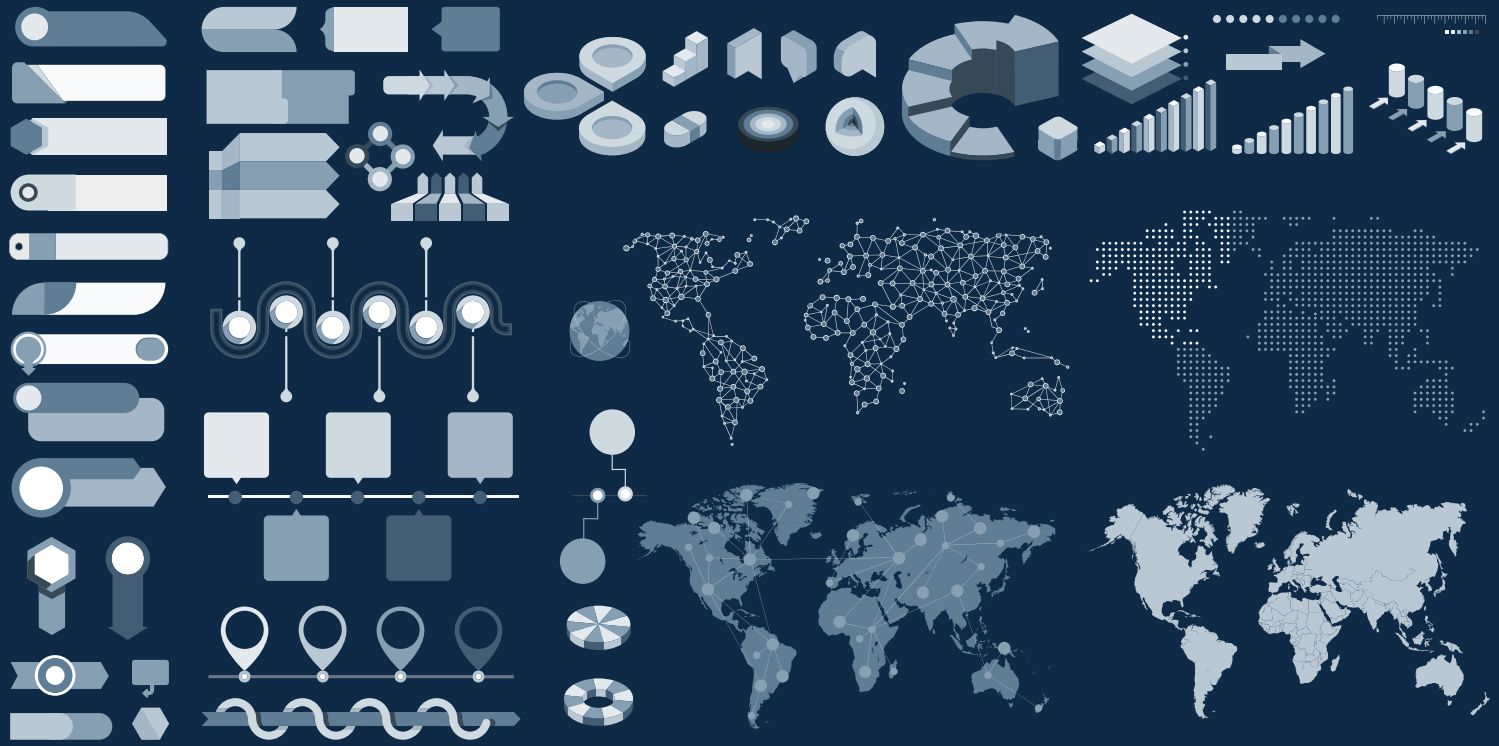
Ledger, Ledger Nano S, Ledger Vault are registered trademarks of Ledger SAS.

(c) Ledger SAS 2020 - All rights reserved

Use our editable graphic resources...

You can easily resize these resources, keeping the quality. To change the color, just ungroup the resource and click on the object you want to change. Then, click on the paint bucket and select the color you want. Don’t forget to group the resource again when you’re done.





...and our set of editable icons

You can resize these icons, keeping the quality.
You can change the stroke and fill color; just select the icon and click on the paint bucket/pen.
In Google Slides, you can also use Flaticon's extension, allowing you to customize and add even more icons.

Business Icons

Avatar Icons

Creative Process Icons

Educational Process Icons

Help & Support Icons

Medical Icons

Nature Icons

Performing Arts Icons

SEO & Marketing Icons

Teamwork Icons