PALISADE

HOMOMORPHIC ENCRYPTION FOR PALISADE USERS:

BLOCKCHAIN AND WEB APPLICATIONS

June 11, 2021

AGENDA

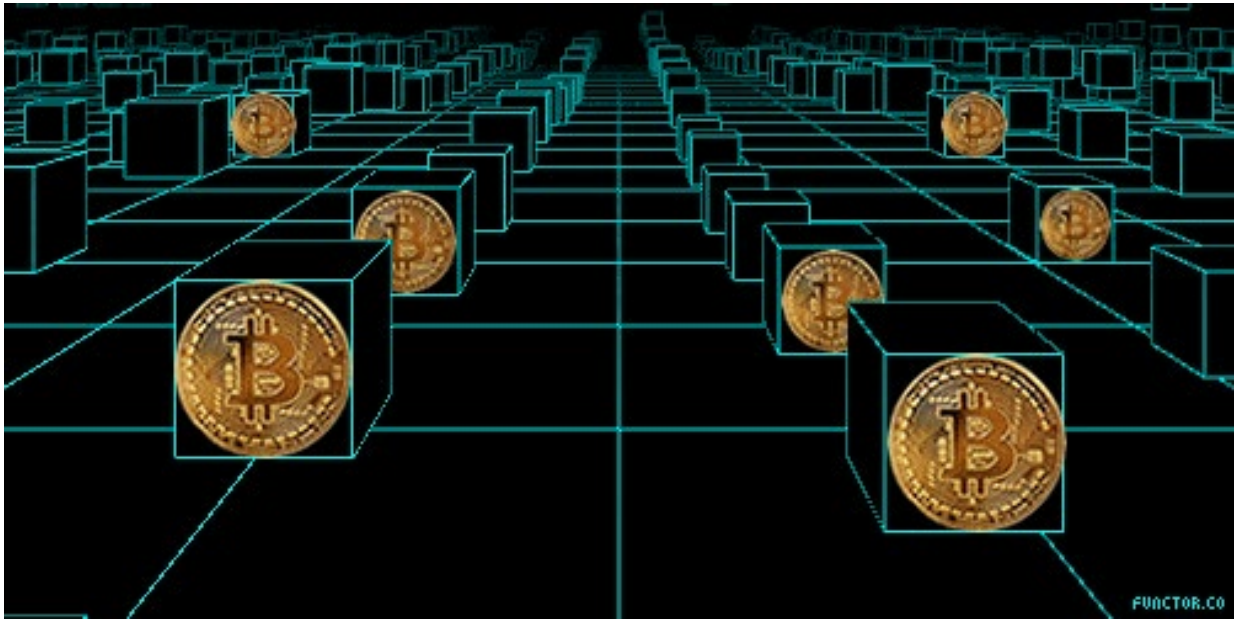
- Blockchain Background:
- Blockchain Projects and FHE:
  - DERO
  - NuCypher

Blockchain Applications

The intersection of fully homomorphic encryption and blockchains

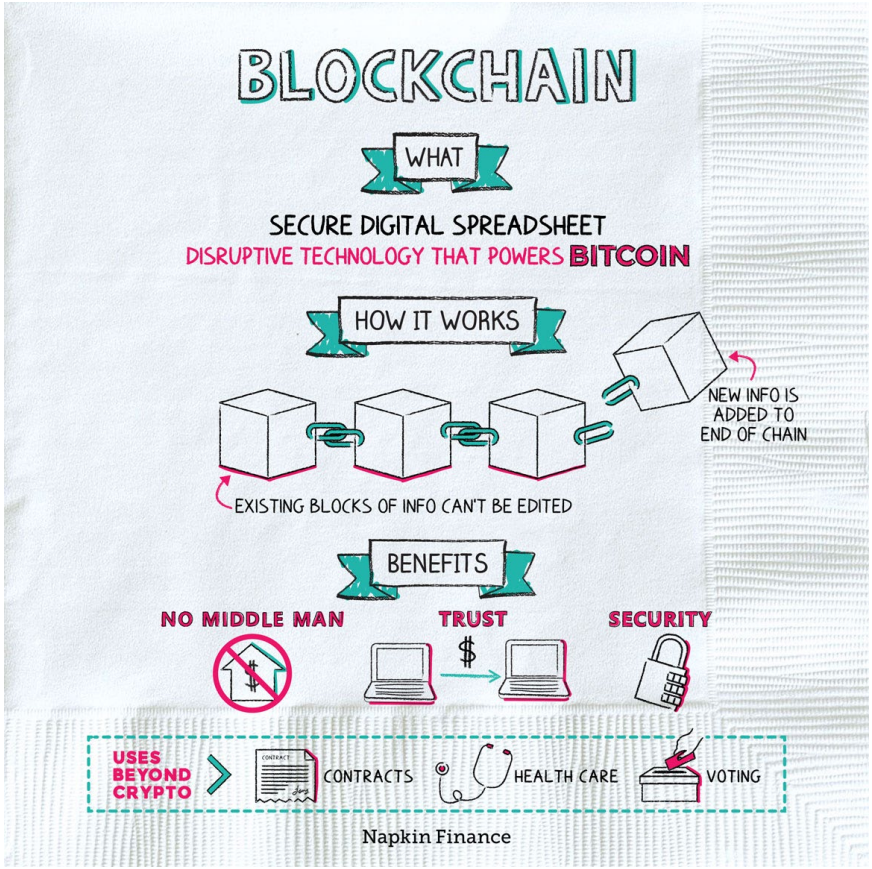
BLOCKCHAIN BACKGROUND:

It’s NOT (just) this:



PALISADE

BLOCKCHAIN BACKGROUND:

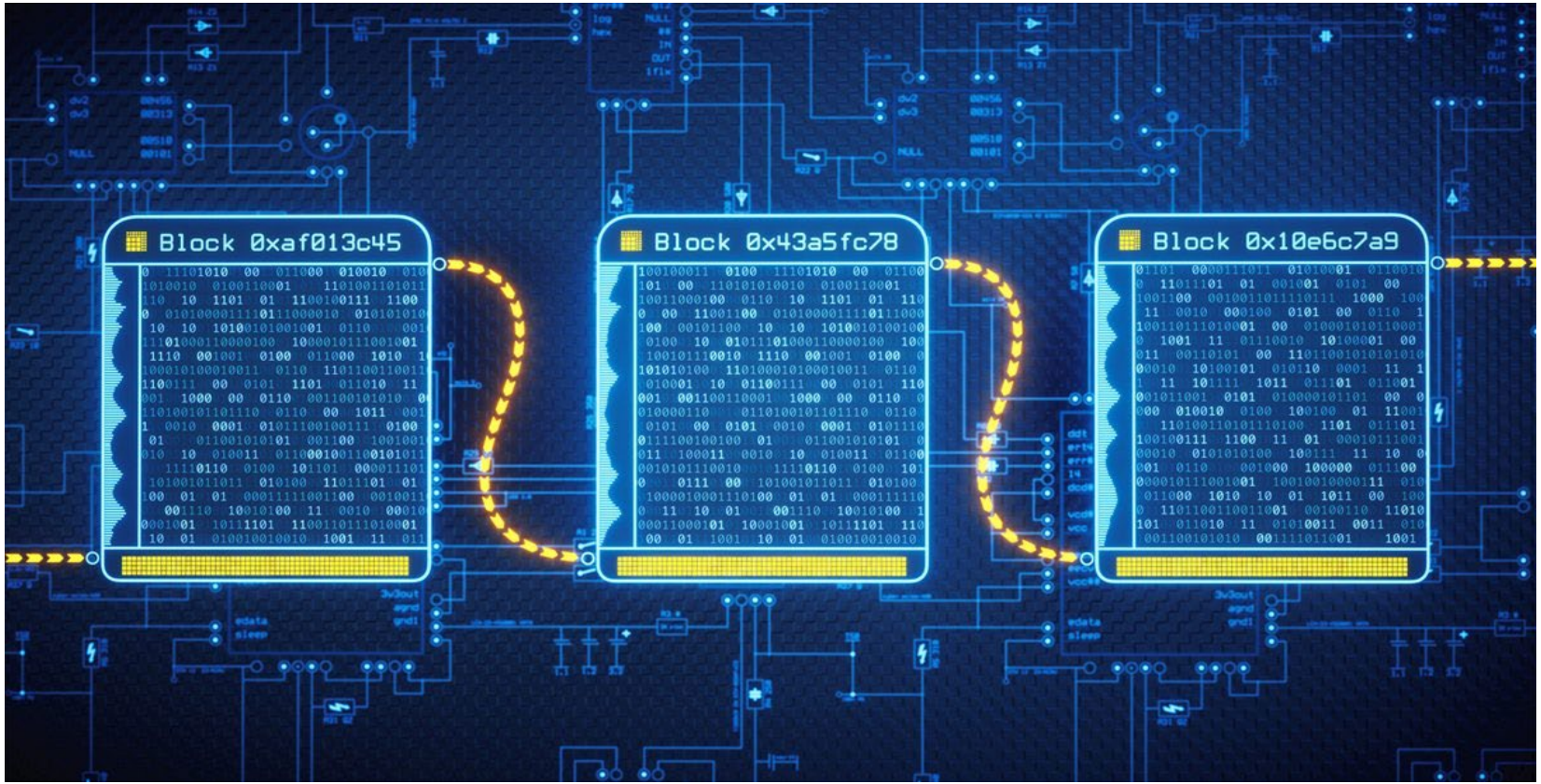


PALISADE

BLOCKCHAIN BACKGROUND:

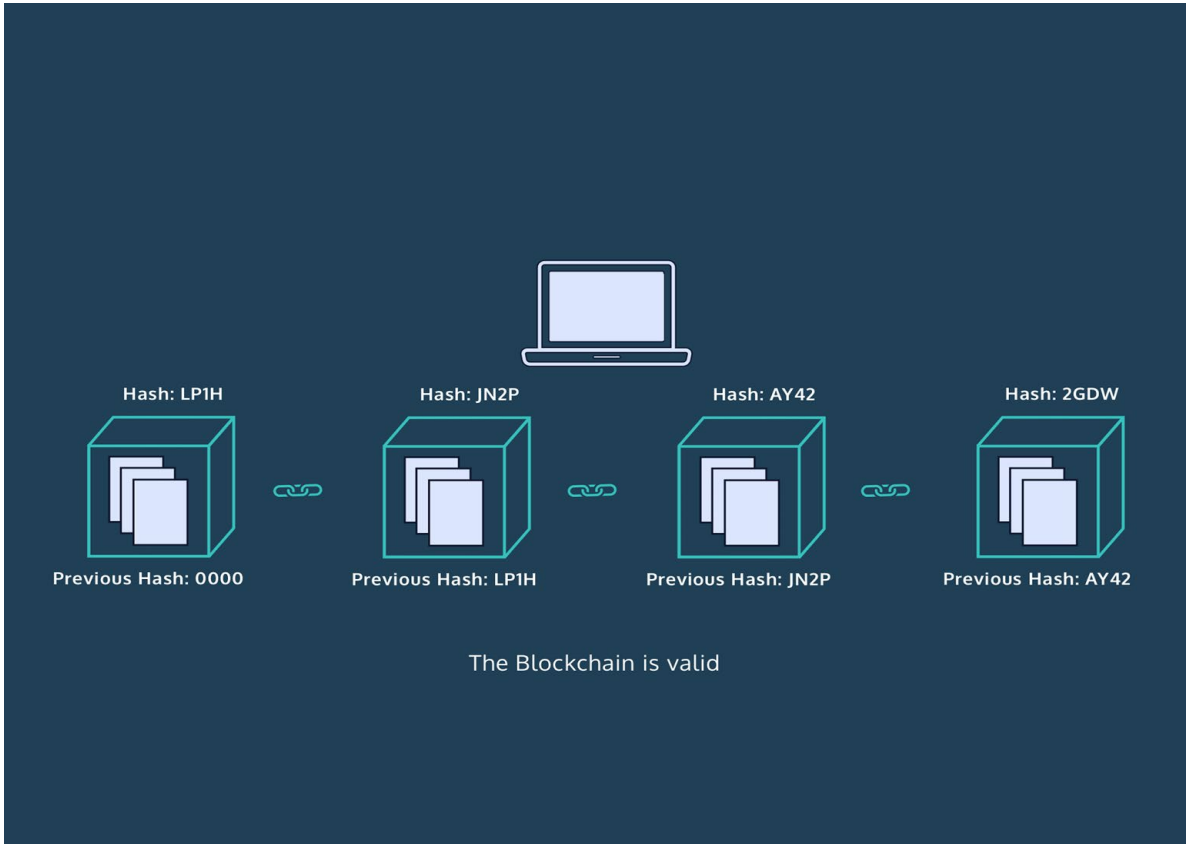
- Stuart Haber and W. Scott Stornetta described what is currently known as blockchain, in 1991. (Haber, S.; Stornetta, W. S., 1991).
- Their first work involved working on a cryptographically secured chain of blocks whereby no one could tamper with timestamps of documents.
- They then built on an earlier thesis concept of David Chaum's blockchain-like system for maintaining computer systems in a mutually suspicious group (Chaum, D. 1982).
- Chaum would go on to describe the first digital currency a year later after his thesis (Chaum, D. 1983), though it is important to note this was not the first conceptualization of "electronic cash".

BLOCKCHAIN BACKGROUND:



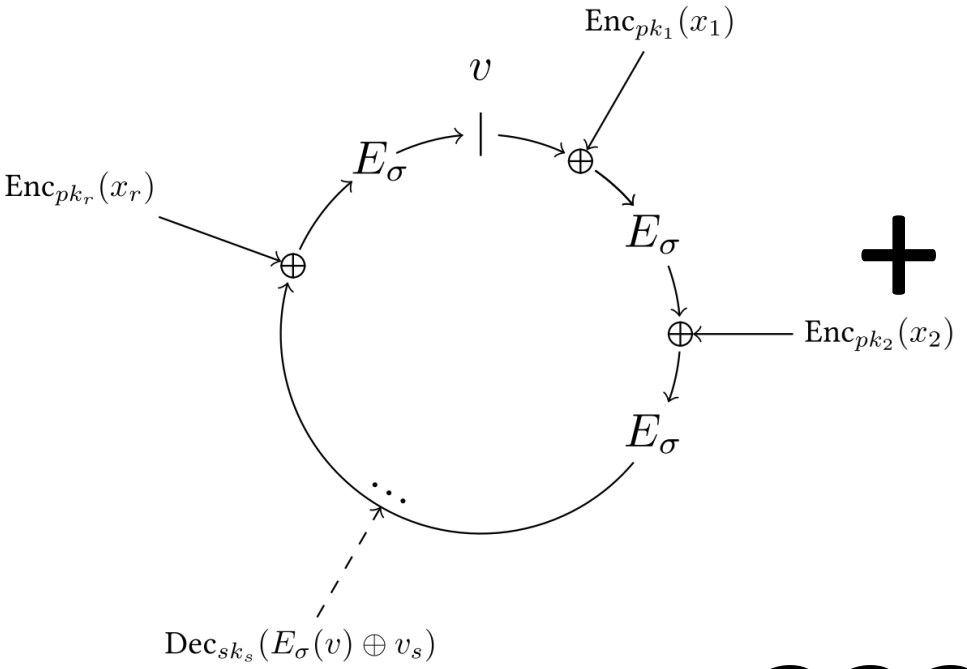
PALISADE

BLOCKCHAIN BACKGROUND:

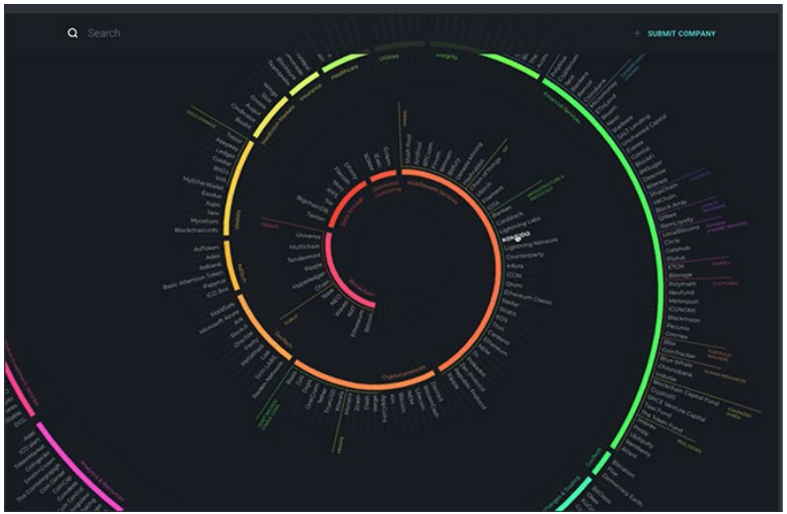


PALISADE

BLOCKCHAIN BACKGROUND:



+



= ???

PALISADE

Blockchain Projects and FHE

State of the art in Blockchain/FHE - DERO

BLOCKCHAIN PROJECTS AND FHE: DERO

- “DERO is the first crypto project to combine a Proof of Work blockchain with a DAG (Directed Acyclic Graph) block structure and fully anonymous transactions based on Homomorphic Encryption.”
- The distributed ledger has a 60 second average block time (time to process transactions) and “is secure against majority hashrate attacks”.
- DERO uses Homomorphic Encryption and has smart contracts on its native chain without any extra layers or secondary blockchains.
- At present DERO has Smart Contracts on the first version of the CryptoNote protocol testnet.

BLOCKCHAIN PROJECTS AND FHE: DERO

	Latency	Height/Topo	Block Propagation	Peers INC	Peers OUT	Version	Last 10 blocks propagation	Avg	Last upda
NL4	108 ms	96573 / 96687	466 ms	0	0	2.0.0-1.alpha.atlantis+27062018		146 ms	5s ago
Europools.tech	109 ms	96573 / 96687	318 ms	0	0	2.0.0-1.alpha.atlantis+27062018		803 ms	5s ago
bailout2k18	110 ms	96573 / 96687	197 ms	0	0	2.0.0-1.alpha.atlantis+27062018		505 ms	5s ago
Dank Node	82 ms	96573 / 96687	0 ms	0	0	2.0.0-1.alpha.atlantis+27062018		454 ms	5s ago
sg.dero.miner.rocks - 1	264 ms	96573 / 96687	1944 ms	0	0	2.0.0-1.alpha.atlantis+27062018		1529 ms	3s ago

PALISADE

BLOCKCHAIN PROJECTS AND FHE: DERO

PALISADE

BLOCKCHAIN PROJECTS AND FHE: DERO

- Specifically, DERO uses Homomorphic Encryption to do arithmetic operations and “settle balances with data being always encrypted”. They claim that “balances are never decrypted before/during/after operations in any form”.

- They utilize “Homomorphic Rings” for confidential transactions: This provides “**untraceability, privacy, and fungibility”** while making sure that the system is stable and secure.

OTHER DERO (FHE BASED) FEATURES:

- **Homomorphic account based model** (Transaction Execution, lines 82-95).
- Instant account balances[Need to get 66 bytes of data only from the blockchain].
- No more chain scanning or wallet scanning to detect funds, no key images etc.
- Fixed per account cost of 66 bytes in blockchain[Immense scalability].
- **Perfectly anonymous transactions with many-out-of-many proofs** [bulletproofs and sigma protocol]
- Deniability

OTHER DERO (FHE BASED) FEATURES:

- **Fixed transaction size say ~2.5KB (ring size 8) or ~3.4 KB (ring size 16) etc based on chosen anonymity group size[logarithmic growth]**
- Anonymity group can be chosen in powers of 2.
- **Allows homomorphic assets (programmable SCs with fixed overhead per asset), with open Smart Contract but encrypted data.**

PALISADE

OTHER DERO (FHE BASED) FEATURES:

- Allows chain pruning on daemons to control growth of data on daemons.
- Transaction generation takes less than 25 ms.
- Transaction verification takes even less than 25ms time.
- No trusted setup, no hidden parameters.
- Pruning chain/history for immense scalability[while still secured using merkle proofs].
- Example disk requirements of 1 billion accounts (assuming it does not want to keep history of transactions, but keeps proofs to prove that the node is in sync with all other nodes)

DERO SIZES:

Ring Size	DEROHE TX Size
2	1553 bytes
4	2013 bytes
8	2605 bytes
16	3461 bytes
32	4825 bytes
64	7285 bytes
128	11839 bytes
512	~35000 bytes

Blockchain Projects and FHE

State of the art in Blockchain/FHE - NuCypher

BLOCKCHAIN PROJECTS AND FHE: NuCypher

A GPU implementation of fully homomorphic encryption on torus

This library implements the fully homomorphic encryption algorithm from `TFHE` using CUDA and OpenCL. Unlike `TFHE`, where FFT is used internally to speed up polynomial multiplication, `nufhe` can use either FFT or purely integer NTT (DFT-like transform on a finite field). The latter is based on the arithmetic operations and NTT scheme from `cuFHE`. Refer to the project documentation for more details.

Usage example

```
import random
import nufhe

size = 32
bits1 = [random.choice([False, True]) for i in range(size)]
bits2 = [random.choice([False, True]) for i in range(size)]
reference = [not (b1 and b2) for b1, b2 in zip(bits1, bits2)]

ctx = nufhe.Context()
secret_key, cloud_key = ctx.make_key_pair()

ciphertext1 = ctx.encrypt(secret_key, bits1)
ciphertext2 = ctx.encrypt(secret_key, bits2)

vm = ctx.make_virtual_machine(cloud_key)
result = vm.gate_nand(ciphertext1, ciphertext2)
result_bits = ctx.decrypt(secret_key, result)

assert all(result_bits == reference)
```


PALISADE

BLOCKCHAIN PROJECTS AND FHE: NuCypher

- Created GPU Optimized version of TFHE (GSW based), called called nuFHE. It is optimized for CUDA and OpenCL.

- There is an optimization on the FHE operations using FFT and non-integer NTT (number theoretic transform) . The latter functionality is available in cuFHE, the CUDA port of TFHE, and both are also available in PALISADE (DFT's using FFT , but CRT is an integer-only NTT in EVALUATION mode).

BLOCKCHAIN PROJECTS AND FHE: NuCypher

- Miners can then compute directly on any subset of the users' encrypted inputs. **No off-chain coordination needed. No interaction necessary for the computation. No need for the users to even be online."**

THANK YOU!

https://palisade-crypto.org

PALISADE