



The Nexa Blockchain

None of the information provided in this lecture is financial advice.

MARCH 2025 | JORGEN NOTLAND

About Me

- **Bsc. informatics**
- Blockchain enabled Trust & Transparency in supply chains (26+ citations)
- **Msc. Blockchain and supply chain**
- The Minimum Hybrid Contract (MHC) Combining Legal and Blockchain Smart Contracts
- **Various mobile-based projects/startups**
- Asking nearby people for help, uploading pictures that are deleted after 24h
- Trondheim Open Blockchain Meetup
- Founded in 2017, meetups 1-2 a year since
- Public speaker on Blockchain at various venues and audiences
- On-chain voting

Worked on on-chain voting with Bitcoin Unlimited before I moved over to Nexa

- Wally Wallet: Open source mobile wallet
- Nexa wallet for NEX, tokens and NFTs



Why am I here?

- Ambassador from Nexa to increase institutional awareness especially within computer science and finance, and explore blockchain technology with you all
- The University of Exeter is a great platform for developing learning material and gathering feedback from the next generation of developers (i. e. Msc Computer Science) and power-users (i. e. Msc. Finance) students.
- Motivate students to consider building on Nexa, as we are committed to enabling the next generation of developers and builders to work on a future-proof network designed for the digital economy of the future

Disclaimer before I begin

None of the information I share in these lecture or computer lab is intended as financial advice. I am not here to shill or sell the Nexa coin.

I am not giving financial advice, but educating people on how to evaluate the pros and cons of different blockchains, which is what the market must do for price discovery. The volatility in crypto prices is partly because most of their market-cap is future-value, not present utility value, but also because the market has a hard time evaluating the different coins when they can appear so similar to the casual external observer. Only "under the hood" are the differences much more apparent

Disclaimer before I begin

Be prepared to share 1 key learning with the class at the end of this lecture

1st, 2nd and 3rd generation blockchains explained

What is Nexa?

To expand a little on why we are talking about Nexa is it is an example of the advancement in blockchain technology since Bitcoin was launched 16 years ago.

We could call it "3rd gen" without being inaccurate as it collates so many things learned from 1st and 2nd gen blockchains. The native tokens, flexible RPN scripting with non-turing complete looping, UTXO model suitable for parallelization and therefore, hardware acceleration.

blockchains a second generation, also it will have fast blocks, token support, smart contract capability.

But, I regard the UTXO design as superior. Hence a UTXO design, with fast blocks, scalable, native tokens, advanced scripting, NFT support etc, a 3rd gen blockchain

Before Nexa, there was Bitcoin Unlimited

- Bitcoin Unlimited is the organization behind the Nexa cryptocurrency
- Started on 2015
- ‘The Block Wars’ - what motivated Bitcoin Unlimited to begin?

BLOCK SIZE LIMIT DEBATE WORKING PAPER

A Transaction Fee Market Exists Without a Block Size Limit

Peter R. Rizun[†]
August 4, 2015

Abstract. This paper shows how a rational Bitcoin miner should select transactions from his node's mempool, when creating a new block, in order to maximize his profit in the absence of a block size limit. To show this, the paper introduces the *block space supply curve* and the *mempool demand curve*. The former describes the cost for a miner to supply block space by accounting for orphaning risk. The latter represents the fees offered by the transactions in mempool, and is expressed versus the minimum block size required to claim a given portion of the fees. The paper explains how the supply and demand curves from classical economics are related to the derivatives of these two curves, and proves that producing the quantity of block space indicated by their intersection point maximizes the miner's profit. The paper then shows that an unhealthy fee market, where miners are

“Satoshi definitely envisaged fees gradually replacing the reward as the long-term funding mechanism for BTC blockchain security.

My view is there is a very real risk, at the next halving of a post-peak long-term decline in BTC price and a trend to dis-investment:

a) because it is much more primitive and limited than coins launched in the last decade, including Nexa which has advanced token and scripting functionality

b) the failing security model as discussed above.”

- **Solex, B.U President**

Introducing Nexa

"Sound money cryptocurrency for everyone every day" - Andrew Stone (Nexa Lead Developer)

The Blockchain Trilemma

We reject the “blockchain trilemma” as an artifact of design choices made by the Ethereum architecture.



What is Nexa?



NEXA is a robust UTXO Layer-1 blockchain, offering native token services and smart contracting capabilities. While modeled after Bitcoin's tokenomics, our network offers a unique and more scalable solution.

NEXA is one the most mineable cryptocurrency coins, and is composed of identical tokenomics to Bitcoin, including halving events which occur every 1,050,000 blocks. NEXA's PoW (Proof-of-Work) algorithm is currently engineered for a 2-minute block time. With a unique PoW (Proof-of-Work) algorithm, NEXA will scale to over 10 billion transactions per day.



Key Features defined:

Satoshi UTXO architecture + Proof-of-Work

Supply: Maximum of 21,000,000,000,000 NEX units

Tokenomics: Nexa's issuance model follows the Bitcoin protocol, with a 4-year halving cycle, built for long-term financial stability

Fair Launch: Announced before genesis block, Nexa does not have any development team carve out or pre-mine.

Advanced token and Scripting: tokens are native to the base-layer and miner-validated, allowing very robust business use-cases. It has advanced OP codes for powerful scripting, including looping, which replicates most capabilities of smart-contracts without a Virtual Machine environment, without requiring gas.

Instant Transactions: Double-spend proofs enables users to transact without requiring long waits for confirmation counts.

Scalability: Throughput targets of up to 4 billion transactions per day are achievable.

What is NexScript?

Smart contracts for Nexa

Efficient and Reliable Verification

Smart contracts on Nexa are stateless and UTXO-based. This model allows transactions to be verified independently and efficiently. Because there is no global state that can impact the execution of these smart contracts, the results are deterministic and predictable.

Private and Isolated Contracts

Because of Nexa's UTXO-based model, each contract is fully independent and isolated from each other. This limits systemic risk and makes contract upgrades much simpler.

Strong Abstraction

Nexa transactions run on a virtual machine called raw Nexa Script. Writing bytecode for this virtual machine is difficult and error-prone. NexScript offers a strong abstraction for writing Nexa smart contracts, improving developer experience and reliability of contracts.

DeFi on Nexa

Most DeFi applications are currently built on top of the EVM. Nexa contracts use a different paradigm than EVM chains due to its UTXO architecture. But with Script Templates, transaction introspection and local state, DeFi is very much possible on Nexa.

A Comparison

UTXO blockchains like Nexa, versus the rest

Ethereum/Solana (EVM) vs Nexa smart contracts

- Ethereum is Turing complete (means contract can make any change it is authorized to make).
- Nexa is NOT Turing complete WRT ledger changes (ALL changes specified up front).
- Blind signing problem
- Massive parallelism



Feature	NexScript (Nexa)	Solidity (Ethereum)
Model	UTXO L1	Account-based, L2
Model	Native tokens	Smart-contract based tokens
Execution	Script validation in tx	EVM bytecode execution
Interaction	Construct tx's to interact	Calls contract functions
Gas Fees	Tx fees only based on script execution	Gas fees per computation step
Turing Completeness	Non-turing complete	Turing complete

Nexa decentralized exchange vs Ethereum decentralized exchange

Is Solana an attempt to circumvent the trilemma?

Nexa vs Uniswap L2 (CPMM)

- Trading two tokens such as Tether and Shiba inu on Ethereum or Solana requires a third token called a LP token.
- The LP token is essentially an on-chain Constant Product Market Maker which is cool in itself. This basically all on-chain trading on EVM
- No need for this in Nexa

Nexa vs EVM (Ethereum, Solana, etc) Summarised

- Useability / Security
- No “bad” MEV (maximal extractable value)
- No “blind signing” problem
- Intrinsic token enforcement
- No GAS



Q&A Break



Exploring Script Templates

What is a Script Template?

A script template is a generalization of the P2SH (pay-to-script-hash) format, that allows for the implementation of covenants. It is perhaps conceptually difficult to understand at first, but is both easy to implement over the existing Bitcoin scripting system and is powerful.

A script template factors all data in a traditional script out into arguments that are furnished by the owner and spender.

What is a Script Template?

For example, a traditional pay-to-pubkey-hash script looks like this:

```
DUP HASH160 PUSH pubkeyhash EQUALVERIFY CHECKSIG
```

Since the pubkeyhash changes for each address, a slightly different script is created for each address. A script template factors this data out of the script, expecting it as arguments (i.e. on the stack) before the script is executed. This means that every pay-to-pubkey-hash script is the exact same bytes.

Why do you need to know this?

Our computer lab session tomorrow will involve an exercise with NexScript, and our Playground: <https://playground.nexscript.org/>

- Learn how to utilise Script Templates, and what goes into blockchain development
- Learn how to compile a smart contract using the Playground
- Evaluate the key differences between NexScript and Solidity (Ethereum)

The Possibilities, with blockchain

Explore some of the use cases and innovations we are working on at Nexa.

Tailstorm

Wally Wallet

Falcon

DEX

Custom Hardware for Scaling

Share Key Learning + Q&A