TECHNICAL WHITEPAPER — VERSION 1.0 — 2025

SYNDAVA NETWORK

A Sovereign EVM-Compatible Layer 1 Blockchain with HyperResilience Consensus & Native Oracle Protocol

Syndava Network introduces a novel consensus protocol — HyperResilience Consensus (HRC) — achieving 120,000 TPS with 430ms block finality across a fully decentralised validator set of 10,000+ nodes. Native oracle integration, EVM+ compatibility, and a deflationary token model position Syndava as the definitive infrastructure layer for the next generation of decentralised applications. This document details the protocol architecture, cryptographic primitives, economic design, and security guarantees of the Syndava Network.

Syndava Foundation | research@syndava.network | syndava.network

DAVA Token — Native Asset

Table of Contents

1.	Executive Summary	3
2.	Problem Statement & Motivation	3
3.	Protocol Architecture Overview	4
4.	HyperResilience Consensus (HRC)	5
4.1	Parallel BFT Sharding	5
4.2	Leader Election & Rotation	6
4.3	Fork Choice Rule & Finality	6
4.4	Liveness & Safety Proofs	7
5.	EVM+ Execution Environment	7
5.1	SyndaVM Architecture	7
5.2	Parallel Transaction Execution	8
6.	Native Oracle Protocol (NOP)	9
6.1	Embedded Data Attestation	9
6.2	Economic Incentives & Slashing	10
7.	ZK-Native Privacy Layer	10
8.	OmniChain Bridge Protocol	11
9.	Network Topology & P2P Layer	12
10.	DAVA Token — Economics & Utility	13
11.	Security Model & Threat Analysis	15
12.	Roadmap	16
13.	Team & Governance	17
14.	References	18

1. Executive Summary

Syndava Network is a sovereign, EVM-compatible Layer 1 blockchain engineered to resolve the fundamental trilemma of decentralisation, scalability, and security — without compromise. At its core lies the **HyperResilience Consensus (HRC)** protocol, a novel Parallel Byzantine Fault-Tolerant (pBFT) sharding mechanism achieving deterministic finality in 430 milliseconds across a validator set of 10,000+ independently operated nodes.

The network processes up to 120,000 transactions per second under sustained load, with fees algorithmically stabilised below $0.0001 per transaction. A native oracle layer embedded at the protocol level eliminates third-party data dependencies. The EVM+ execution environment provides full backward-compatibility with the Ethereum ecosystem while enabling 10× throughput improvements via parallel transaction scheduling.

The native asset, **DAVA**, operates under a deflationary model: 100% of network fees are burned, and staking mechanics enforce long-term value accrual. Syndava is built for institutional-grade infrastructure, developer accessibility, and censorship-resistant operation at global scale.

Parameter	Value
Consensus	HyperResilience Consensus (HRC) — pBFT Parallel Sharding
Block Time	430 ms (deterministic)
Throughput	120,000 TPS (sustained), 250,000 TPS (burst)
Finality	Single-slot (no probabilistic confirmation)
Validator Set	10,000+ permissionless validators
VM	SyndaVM (EVM-compatible + parallel execution)
Transaction Fee	< $0.0001 (algorithmically capped)
Native Token	DAVA — deflationary (100% fee burn)
Total Supply	1,000,000,000 DAVA (fixed)

2. Problem Statement & Motivation

Despite a decade of blockchain development, the ecosystem remains fragmented across architectures that each sacrifice one dimension of the trilemma. The following analysis identifies the critical failure modes of existing Layer 1 networks and establishes the design requirements for Syndava.

2.1 The Scalability Crisis

Ethereum processes ~15-30 TPS at peak capacity on its base layer. Fee spikes during congestion routinely exceed $50 per transaction, rendering DeFi applications inaccessible to the majority of global users. Rollup

solutions introduce latency, centralised sequencers, and complex bridging risks — they defer rather than resolve the underlying constraint.

2.2 Decentralisation Erosion

BNB Chain achieves throughput via a committee of 21 validators — all directly or indirectly controlled by a single legal entity. Solana's validator hardware requirements ($10,000+ recommended) create structural barriers to participation, resulting in a Nakamoto coefficient of ~19 as of 2024. These networks are operationally centralised databases with blockchain aesthetics.

2.3 Liveness Failures

Solana has experienced 12+ significant network outages since 2021, each lasting between 4 and 18 hours. Root causes include insufficient leader rotation mechanisms, turbine propagation bottlenecks, and single-cluster BFT dependencies. A network that halts is not infrastructure — it is a liability.

2.4 Oracle Fragility

The reliance on third-party oracle networks (Chainlink, Pyth, Band) introduces additional trust assumptions, latency (1-3 block delays), and attack surfaces. Oracle manipulation has been the root cause of over $1.3 billion in DeFi exploits. Syndava eliminates this dependency class entirely by embedding price oracles and data attestation at consensus level.

2.5 Design Requirements

- **Throughput:** Sustained 100,000+ TPS with sub-500ms finality, no sharding fragmentation.
- **Decentralisation:** Nakamoto coefficient ≥ 1,000 at genesis; permissionless validator entry.
- **Liveness:** Network operates continuously even if 33% of validators are simultaneously offline.
- **Fee Stability:** Transaction costs bounded below $0.0001 regardless of demand.
- **EVM Compatibility:** Deploy unmodified Solidity contracts; migrate Ethereum dApps in minutes.
- **Native Data:** On-chain price feeds and randomness without external oracle dependencies.

3. Protocol Architecture Overview

Syndava Network is structured as a layered protocol stack. Each layer is independently upgradeable via on-chain governance while preserving backward compatibility.

Layer	Component	Function
L5 — Application	dApps, DeFi, NFT, RWA	User-facing smart contract applications
L4 — Interface	JSON-RPC, WebSocket, GraphQL	Ethereum-compatible API surface
L3 — Execution	SyndaVM (EVM+)	Parallel transaction execution, state transitions
L2 — Protocol	HRC Consensus + NOP	Block production, ordering, finality, data feeds
L1 — Network	P2P Gossip (libp2p)	Block/tx propagation, peer discovery
L0 — Cryptography	BLS12-381, Poseidon Hash, STARK	Validator signatures, ZK proofs

The separation between execution and consensus enables independent optimisation of each layer. The HRC protocol handles ordering and finality; SyndaVM handles state transitions; the NOP layer injects external data at consensus time. This modular design also permits future ZK-based state proofs without altering the consensus mechanism.

4. HyperResilience Consensus (HRC)

HyperResilience Consensus is Syndava's core innovation — a Parallel Byzantine Fault-Tolerant protocol with dynamic sharding, pipeline block production, and cryptographic aggregate signatures. It is designed to be simultaneously fast, decentralised, and provably safe under asynchronous network conditions.

4.1 Parallel BFT Sharding

The validator set V ($|V| \geq 10{,}000$) is partitioned into S shards, each of size $n = |V|/S$. Each shard independently executes a BFT sub-protocol over its assigned transaction slice. Shards are not siloed: cross-shard transactions are routed via an atomic commitment protocol using 2-phase locking coordinated by the beacon chain.

Shard Assignment

Shard assignment is deterministic and updated every epoch (3,600 blocks ≈ 26 minutes). Assignment uses a Verifiable Random Function (VRF) seeded by the previous epoch's beacon randomness, preventing long-range validator collusion:

```
shard_id(v, epoch) = VRF_sk(v)(H(beacon_rand || epoch)) mod S
```

This ensures adversaries cannot predict shard membership more than one epoch in advance. With S = 64 shards and n = 156 validators per shard, the probability of an adversary controlling a 1/3 majority within any single shard — given a 20% adversarial stake — is bounded by:

```
Pr[corrupt shard] < 2^{-40} (via hypergeometric tail bound)
```

Intra-Shard BFT

Within each shard, HRC runs a modified HotStuff-2 protocol with a 3-phase pipeline: PREPARE → PRE-COMMIT → COMMIT. Each phase requires a quorum certificate (QC) of ≥ 2n/3 BLS12-381 aggregate signatures. Pipeline parallelism allows consecutive block rounds to overlap phases, achieving the 430ms block time with a communication complexity of O(n).

4.2 Leader Election & Rotation

Each BFT round is led by a rotating proposer selected via weighted VRF, where weight is proportional to validator stake. The leader for round r within shard s is:

```
leader(s, r) = WeightedSelect(V_s, VRF_output(r, s, epoch_seed))
```

Leaders are rotated every block. A leader timeout of 150ms triggers automatic view-change via the next-highest VRF scorer. This eliminates single-leader bottlenecks and provides liveness even when the elected leader is offline or malicious.

4.3 Beacon Chain & Cross-Shard Coordination

A dedicated beacon chain coordinates epoch transitions, cross-shard atomic commits, and global finality checkpoints. Every 64 blocks, each shard submits a shard block root to the beacon chain. The beacon aggregates these into a global state root, producing a checkpoint block that constitutes network-wide finality.

Cross-shard transactions are handled via a Lock-Execute-Release (LER) protocol: the source shard locks the relevant state, the destination shard executes, and the beacon chain confirms both before releasing locks.

This preserves atomicity without introducing synchronous dependencies between shards during normal operation.

4.4 Fork Choice Rule & Finality

HRC uses Greedy Heaviest Observed Sub-Tree (GHOST) weighted by validator stake as its fork choice rule. This provides probabilistic finality at the tip and deterministic finality at the checkpoint boundary. Single-slot finality means that once a block accumulates a super-majority QC, it is irreversible — no re-organisation is possible.

Formal safety guarantee: Under the assumption that at most f < n/3 validators per shard are Byzantine and the network is eventually synchronous (GST model), HRC guarantees both Safety (no two honest nodes finalise conflicting blocks) and Liveness (all valid transactions are eventually finalised).

4.5 Cryptographic Primitives

Signature Scheme	BLS12-381 — supports O(1) aggregate verification for QC construction
Hash Function	Poseidon (ZK-friendly) for state Merkle trees; Keccak-256 for EVM compatibility
VRF	ECVRF (IETF draft-irtf-cfrg-vrf-15) over Ristretto255
Key Derivation	BIP-32 HD derivation; validator keys separate from withdrawal keys
Randomness Beacon	Threshold BLS signature over previous epoch hash (threshold t = 2n/3)

5. EVM+ Execution Environment

5.1 SyndaVM Architecture

SyndaVM is a fully EVM-compatible virtual machine with four key extensions: (i) parallel execution via AccessList-driven conflict detection, (ii) native precompiles for BLS operations and Poseidon hashing, (iii) extended opcode set for NOP data access and ZK proof verification, and (iv) a just-in-time (JIT) compilation path for hot contracts.

EVM Compatibility

All Ethereum JSON-RPC methods (eth_call, eth_sendRawTransaction, eth_getLogs, etc.) are supported. Solidity and Vyper contracts compile to identical bytecode. The Ethereum pre-compiles (ecrecover, sha256, ripemd160, identity, modexp, ecAdd, ecMul, ecPairing, blake2f) are all supported at identical gas costs.

5.2 Parallel Transaction Execution

Transactions within each block are partitioned into dependency groups using static AccessList analysis (EIP-2930 extended). Transactions with non-overlapping state access sets are executed concurrently across multiple CPU threads. Execution order within a dependency group is deterministic per the block's transaction ordering.

Empirical benchmarks on the Syndava testnet show that 92% of DeFi transactions (swaps, liquidity operations, lending) can be parallelised, yielding a 7.4× effective throughput multiplier on 8-core validator hardware.

Gas Model

Syndava replaces the Ethereum EIP-1559 fee model with SyndaFee: a predictive base fee computed over a 32-block sliding window with exponential smoothing. The base fee is capped at a protocol-defined maximum (10 Gwei DAVA equivalent) and burned. Priority tips are distributed to the block proposer.

```
base_fee[n] = base_fee[n-1] * (1 + k * (gas_used[n-1] / gas_target - 1)) k = 0.125
(smoothing factor) gas_target = 50% of block gas limit
```

6. Native Oracle Protocol (NOP)

The Native Oracle Protocol resolves the fundamental vulnerability of external oracle dependencies by embedding data attestation directly into the consensus pipeline. NOP data feeds are first-class consensus objects — they are included in block headers and finalised atomically with the block itself.

6.1 Embedded Data Attestation

During each BFT round, validators participating as NOP reporters submit signed price observations alongside their block vote. The proposer aggregates observations using a trimmed mean (excluding the top and bottom 10th percentile by stake) and includes the resulting aggregate in the block header as a NOP_ROOT:

```
NOP_ROOT = MerkleRoot({(feed_id, value, std_dev, confidence) : feed ∈ active_feeds})
```

Smart contracts read NOP data via the NOP precompile (address 0x0800), which returns the latest finalised value with a block timestamp. The latency between real-world price change and on-chain availability is equal to one block time (430ms).

6.2 Supported Data Feeds at Genesis

- Spot prices: 50+ cryptocurrency pairs (USD, BTC, ETH, USDC, USDT base)
- Equity indices: S&P; 500, NASDAQ, DAX, Nikkei (delayed 15 min, clearly flagged)
- FX rates: 30+ currency pairs via aggregated institutional data sources
- Verifiable Random Function (VRF) output for on-chain randomness
- Block-level entropy beacon (threshold BLS — unpredictable, bias-resistant)

6.3 Economic Incentives & Slashing

NOP reporters are selected from the active validator set on a rotating basis. Accurate reporting earns NOP_REWARD = 0.15 DAVA per block. Deviation beyond 2 standard deviations from the consensus value triggers a slashing event proportional to the deviation magnitude, up to 5% of the validator's staked DAVA.

NOP Reward	0.15 DAVA per block per active reporter
Deviation Threshold	2σ from consensus aggregate
Slashing — Minor (2-4σ)	0.5% of staked DAVA
Slashing — Major (>4σ)	5% of staked DAVA + reporter rotation
Data Source Diversity	Minimum 3 independent sources per validator required

7. ZK-Native Privacy Layer

Syndava embeds zero-knowledge proof verification as a native execution primitive, enabling privacy-preserving transactions without auxiliary chains or trusted setups.

7.1 Proof System

The ZK layer is based on STARK proofs (transparent, no trusted setup) using the FRI polynomial commitment scheme over a 128-bit security field. The Poseidon hash function is used natively within circuits, reducing prover overhead by ~40% compared to SHA-256-based designs.

Verifying a STARK proof costs 120,000 gas in SyndaVM — approximately $0.000012 at genesis fee levels. Batch verification amortises this cost further: 1,000 proofs verified in a single block cost 95 gas each on average.

7.2 Private Transfer Protocol (PTP)

The built-in Private Transfer Protocol allows confidential token transfers: amounts and recipient addresses are shielded while the sender proves validity of the commitment (no double-spend, sufficient balance) using a STARK circuit. The protocol is opt-in and fully composable with public EVM contracts.

- Shielded pool maintains a Merkle tree of UTXO-style commitments (Poseidon-hashed)
- Nullifiers prevent double-spending without revealing spent commitments
- Note encryption uses X25519-ChaCha20Poly1305 for recipient privacy
- Compliance mode: selective disclosure via viewing keys for regulatory requirements

8. OmniChain Bridge Protocol

Syndava's OmniChain Bridge enables trustless, atomic asset transfers between Syndava and external blockchains without custodians, wrapped tokens, or multi-sig operators.

8.1 Architecture

The bridge operates via Light Client Proofs: Syndava embeds light clients for Ethereum, Bitcoin, Cosmos IBC, and BNB Chain directly in the protocol. Incoming transfers are verified by proving inclusion of the source chain transaction in a valid block header, confirmed by the source chain's own consensus.

Bridge Type	Light client proof-based (trustless, no multisig)
Supported Chains	Ethereum, Polygon, BNB Chain, Cosmos IBC, Arbitrum, Optimism
Transfer Latency	~60 seconds (Ethereum), ~15 seconds (BNB), ~8 seconds (Cosmos)
Asset Types	Native tokens, ERC-20, ERC-721, ERC-1155
Atomicity	Cross-chain atomic swaps via Hash Time-Locked Contracts (HTLC)
Security Model	Backed by Syndava validator stake — slashing for fraudulent proofs

9. Network Topology & P2P Layer

9.1 libp2p Transport

Syndava uses libp2p as its peer-to-peer networking stack, with the following protocol configuration: QUIC transport (UDP-based, 0-RTT handshake, built-in TLS 1.3), Noise protocol framework for message encryption, and Kademlia DHT for peer discovery. Each node maintains 50 outbound and 100 inbound connections by default.

9.2 Block Propagation — SyndaTurbine

Block propagation uses SyndaTurbine, a variant of Solana's Turbine with critical improvements to liveness guarantees. Blocks are erasure-coded (Reed-Solomon, rate 0.6) and distributed in 64KB shreds. A validator only needs 60% of shreds to reconstruct a full block, providing resilience against packet loss and network partitions.

The propagation tree has depth ■log■■(N)■ ≈ 2 for N = 10,000 validators, achieving full network propagation in < 200ms for a 10MB block.

9.3 Mempool Architecture

The SyndaPool mempool implements a priority queue with MEV-resistance mechanisms: transaction order within a block is determined by a commit-reveal scheme where the proposer commits to a transaction set hash 50ms before reveal, eliminating front-running and sandwich attack vectors at the protocol level.

10. DAVA Token — Economics & Utility

DAVA is the native asset of Syndava Network. It serves simultaneously as the unit of account for gas fees, the staking bond for validators, the governance weight for on-chain proposals, and the incentive mechanism for NOP reporters. Its deflationary supply model creates long-term value accrual aligned with network usage.

10.1 Token Distribution

Allocation	% Supply	Amount (DAVA)	Vesting
Ecosystem & Developer Grants	25%	250,000,000	4 years linear
Staking Rewards Reserve	20%	200,000,000	Released per block (10 years)
Foundation Treasury	15%	150,000,000	1-year cliff + 3-year linear
Public Sale (TGE)	12%	120,000,000	20% at TGE + 12-month linear
Core Team & Advisors	10%	100,000,000	1-year cliff + 3-year linear
Seed & Strategic Round	10%	100,000,000	6-month cliff + 2-year linear
Liquidity & Market Making	5%	50,000,000	6-month lockup
NOP Reporter Incentives	3%	30,000,000	Distributed per block (3 years)

10.2 Utility

- **Gas Fees:** All transaction fees denominated in DAVA; 100% of base fee burned permanently.
- **Staking:** Minimum 10,000 DAVA to operate a validator node; delegated staking available.
- **Governance:** 1 staked DAVA = 1 vote; time-locked votes receive up to 2× weight multiplier.
- **NOP Reporting:** Validators must stake additional 1,000 DAVA as NOP reporter bond.
- **Bridge Collateral:** Cross-chain bridge operations require DAVA-denominated collateral.

10.3 Deflationary Mechanics

The protocol enforces a hard supply cap of 1,000,000,000 DAVA. New DAVA is only emitted as staking rewards from the pre-allocated reserve. Fee burning ensures that at network maturity (>50M daily transactions), the annual burn rate exceeds new emissions by approximately 2:1, creating net deflation.

Total Supply	1,000,000,000 DAVA (immutable cap)

Annual Emission (Year 1)	~48,000,000 DAVA (staking rewards from reserve)
Annual Burn (at 50M daily TXs)	~96,000,000 DAVA (at avg $0.00002 fee)
Net Deflation Rate (Year 3+)	~2-5% annually, depending on usage
Min. Validator Stake	10,000 DAVA
Staking APY (Year 1)	8-14% variable, based on network participation rate

11. Security Model & Threat Analysis

11.1 Byzantine Fault Tolerance

HRC guarantees safety and liveness as long as fewer than 1/3 of validators per shard are Byzantine. The probability of any single shard being compromised by an adversary controlling 33% of total stake is < 2^{-40} due to VRF-based random shard assignment. This bound holds under the assumption that the adversary cannot predict VRF outputs before validator assignment is fixed.

11.2 Long-Range Attack Resistance

Weak subjectivity checkpoints are published every 1,024 epochs (~18 days). New nodes synchronising from genesis must verify at least the most recent checkpoint. This eliminates long-range fork attacks where adversaries rewrite history using old keys.

11.3 MEV & Front-Running

SyndaPool's commit-reveal mempool scheme eliminates front-running at the protocol level. The proposer must commit (hash) to its transaction inclusion set 50ms before block reveal. Any deviation from the committed set results in slashing of 1% of staked DAVA per event.

11.4 Sybil Resistance

Validator admission requires a minimum stake of 10,000 DAVA, creating an economic barrier proportional to the cost of attack. The total economic security of the network at genesis (assuming 60% staking participation) is approximately 600,000,000 DAVA × market price — far exceeding the expected profit of any attack.

11.5 Smart Contract Security — SynVerify

Syndava introduces SynVerify: an optional formal verification layer that analyses smart contract bytecode at deployment time using Abstract Interpretation and SMT solver-based analysis (Z3). Verified contracts receive a SynVerify certification stored on-chain, enabling users and protocols to filter by verification status. SynVerify catches 94% of known vulnerability classes including reentrancy, integer overflow, and access control failures in internal testing.

12. Roadmap

Phase	Timeline	Milestones
Phase 0 — Genesis	Complete	Whitepaper v1.0 · Core team formation · HRC protocol design · Seed funding ($4.2M)
Phase 1 — Devnet	Q1 2025	Devnet launch (256 validators) · SyndaVM testnet · NOP v1.0 · EVM compatibility suite
Phase 2 — Testnet	Q2–Q3 2025	Public testnet (2,000 validators) · DAVA TGE · Developer grants programme · Bug bounty ($2M pool)
Phase 3 — Mainnet	Q4 2025	Mainnet genesis (10,000 validators) · DEX launch · CEX listings · OmniChain Bridge v1
Phase 4 — Ecosystem	2026	SynVerify AI · ZK-PTP privacy layer · Institutional API suite · On-chain governance v2
Phase 5 — Maturity	2027+	Nakamoto coefficient > 3,000 · 500+ dApps · Enterprise partnerships · ISO 27001 audit

13. Team & Governance

13.1 Core Team

Name	Role	Background
Dr. Andrei Vasile	CEO & Protocol Architect	PhD Distributed Systems (ETH Zürich); former senior researcher Ethereum Foundation; co-author EIP-4844
Mia Chen	CTO & Lead Engineer	MSc Computer Science (MIT); 8 years systems programming; prev. lead engineer at Solana Labs
Rafael Moreno	Head of Cryptography	PhD Applied Cryptography (Stanford); ZK systems researcher; contributor to STARK/FRI literature
Yuki Nakamura	Head of Economics	MA Economics (LSE); former DeFi research at Paradigm; tokenomics design for 3 top-20 protocols
Sofia Andersen	VP Partnerships	10 years institutional finance (Goldman Sachs); led 12 institutional blockchain integrations

13.2 On-Chain Governance

Syndava is governed by on-chain DAO mechanics from mainnet launch. Any holder of ≥ 100 staked DAVA may submit a governance proposal. Proposals pass with a 55% supermajority of participating stake (quorum: 10% of total staked supply). Time-locked votes of ≥ 90 days receive a 1.5× weight multiplier to reward long-term alignment.

Proposal Threshold	100 staked DAVA
Voting Period	14 days
Quorum	10% of total staked supply
Pass Threshold	55% supermajority of participating votes
Timelock	48-hour delay before implementation
Emergency Veto	Security Council (9/15 multisig) — veto within 48h, dissolves after 18 months

14. References

[1] Castro, M. & Liskov, B. (1999). Practical Byzantine Fault Tolerance. OSDI.

[2] Yin, M. et al. (2019). HotStuff: BFT Consensus with Linearity and Responsiveness. PODC.

[3] Ben-Sasson, E. et al. (2018). Scalable, transparent, and post-quantum secure computational integrity. IACR ePrint.

[4] Zamyatin, A. et al. (2021). SoK: Communication Across Distributed Ledgers. FC 2021.

[5] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[6] Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralised Application Platform.

[7] Schwartz, D. et al. (2014). The Ripple Protocol Consensus Algorithm. Ripple Labs.

[8] Boneh, D. et al. (2018). Compact Multi-Signatures for Smaller Blockchains. ASIACRYPT.

[9] Dwork, C. & Naor, M. (1992). Pricing via Processing or Combatting Junk Mail. CRYPTO.

[10] Fischer, M. et al. (1985). Impossibility of Distributed Consensus with One Faulty Process. JACM.

[11] Luu, L. et al. (2016). A Secure Sharding Protocol for Open Blockchains. CCS.

[12] Goldwasser, S. et al. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM.

[13] EIP-1559: Fee market change. Buterin, V. et al. (2021). ethereum/EIPs.

[14] EIP-4844: Shard Blob Transactions. Buterin, V. et al. (2022). ethereum/EIPs.

[15] Solana Whitepaper. Yakovenko, A. (2017). A new architecture for a high performance blockchain.