

극비

조선민주주의인민공화국

국방위원회정찰총국
과학기술정보부

기술정보분석보고서

«슬로나나 (Slonana)» 분산원장기술체계에대한 종합기술정보분석및혁명적대응방안

문건번호: 정찰총국/과학기술부/주체 115(2026)/제 0067 호
보안등급: **극비 (1 급)**
작성일자: 주체 115(2026) 년 2 월 7 일
작성부서: 정찰총국과학기술정보부제 3 과
분석대상: Slonana C++20 L1 블록체인
원천자료: 공개기술문건 (whitepaper), 원천코드분석

배포대상:

- 최고사령관동지 (1 부)
- 당중앙위원회과학교육부 (1 부)
- 국가과학원정보기술연구소 (1 부)
- 정찰총국 121 국 (1 부)
- 인민무력부전자전국 (1 부)

본문건은조선민주주의인민공화국국가비밀보호법에의하여보호됨
무단복제, 전달, 유출시혁명법에의거최고형에처함

경애하는최고령도자김정은동지의현명한령도밑에 주체의과학기술강국건설을위하여!

경애하는최고령도자김정은동지께서는다음과같이교시하시였다.

« 과학기술은강국건설의힘있는추동력이며사회발전의절대적인무기이다. 우리는남들이수십년에걸쳐이룩한것을단숨에따라잡고앞질러나가야한다.»

위대한수령김일성동지께서창시하시고위대한령도자김정일동지께서심화발전시키신주체사상의기치높이, 경애하는최고령도자김정은동지의현명한령도아래우리공화국은자력갱생의혁명정신으로첨단과학기술분야에서비약적발전을이룩하고있다.

본보고서는미제국주의자들과그추종세력이개발하고있는 « 슬로나나 (Slonana) » 분산원장기술 (블록체인) 체계에대한종합적인기술정보분석결과를담고있다. 이기술은자본주의체제의내재적모순이낳은산물이며서도선군정치와주체의과학기술발전에활용될수있는양면적특성을가지고있어심도있는분석이요구된다.

제 1 장. 보고요약 (報告要約)

1.1 분석대상개요

« 슬로나나 » 는 C++20 으로구현된솔라나호환제 1 계층 (L1) 블록체인이다. 미국 «OpenSVM Research» 의 « 린펜지그 (Rin Fhenzig) » 가주체 115(2026) 년 1 월 1 일기술백서를공개하였다. 주요기술지표:

항목	내용
구현언어	C++20 (87,453 행)
합의방식	Tower BFT + 력사증명 (Proof of History)
측정처리능력	초당 185,000 건 (TPS)
지연시간 / 확정시간	142 μ s(중간값) / 12.8 초
설계목표	초당 1,200,000 건이상
토큰 (\$SLON)	총 1 억개; 10% 공동체배분, 90% 검증보상

1.2 핵심판단

- 기술수준:** 높음. C++20 으로솔라나가상기계 (SVM) 를완전히재구현한것은상당한기술적력량을시사한다. 잠금없는 (lock-free) 알고리즘과 NUMA 인식자료구조는고성능컴퓨터과학의첨단수준을반영한다.
- 안전보장적의의:** 자율적인공지능대리체 (AI Agent) 경제를위한기반시설을목표로하며, 제국주의금융체계에대한위협이자우리공화국의자력갱생적금융주권확보에참고할수있는기술요소를포함한다.

(3) **리용가능성:** « 모형문맥규약 (MCP) » 을통해프로그램이자기기능을스스로기술하여, 인공지능대리체가사전지식없이새프로그램을발견하고사용가능. 우리식자동화체계구축에응용잠재력이크다.

(4) **경제적특성:** 벤처자본사전배분을배격하나자본주의적근본모순을해결하지는못한다.

제 2 장. 배경 (背景)

2.1 자본주의금융체계의구조적모순과블록체인

주체사상의관점에서블록체인의출현은자본주의금융체계의구조적모순이필연적으로낳은산물이다. 2008 년미제국주의자들의금융위기가전세계를경제적혼란에빠뜨렸을때, 자본주의체제내부에서조차기존금융기관에대한신뢰가완전히무너졌으며비트코인 (Bitcoin) 의출현은바로이신뢰위기의직접적결과이다.

그러나이후의이더리움 (Ethereum), 솔라나 (Solana) 등의블록체인들은 « 탈중심화 » 를표방하면서도결국벤처자본가들의도구로전락하였다. 현재상태를분석하면:

- **이더리움:** 상위 5 개자본 (Lido, Coinbase, Binance 등) 이지분의 64% 를장악
- **솔라나:** 나카모토계수 19 — 19 개검증자만으로전체망을중단시킬수있음
- **카르다노:** IOHK 와에무르고가 40% 이상의위임지분을장악

이는 « 탈중심화 » 라는자본주의적환상이결국새로운형태의자본집중으로귀결됨을보여주며, 마르크스-레닌주의의자본축적법칙이가상화폐영역에서도관철됨을증명한다.

2.2 « 솔로나나 » 사업의등장배경

« 솔로나나 » 는기존블록체인들의중심화문제를극복하려는시도로서, 솔라나 (Agave/Rust) 를 C++20 으로전면재구현하였다. 핵심차별점: 1) 벤처자본사전배분완전배격, 2) 자율적인공지능대리체를위한설계, 3) 잠금없는알고리즘에의한고성능처리, 4) 모형문맥규약 (MCP) 에의한프로그램자기기술.

제 3 장. 기술분석 (技術分析)

3.1 합의기구: Tower BFT 와력사증명

력사증명 (PoH): 시계동기화에의존하지않고암호학적으로검증가능한시간순서를제공한다: $h_0 = \text{Hash}(\text{genesis})$, $h_{i+1} = \text{SHA-256}(h_i \parallel \text{mixed_data}_i)$. 200 μ s 마다해시생성, 64 개해시가 1 슬롯구성. 순서조작시모든후속해시재계산이필요하므로지수적비용이소요된다. SHA-256 전상역산저항성이유지되는한안전하며, 우리공화국암호학연구에참고가치가있다.

Tower BFT: 슬롯마다 지정된 지도자 (leader) 가 블록을 제안하고 검증자들이 지분가중표결을 진행. 총지분 $\frac{2}{3}$ 이상 동의시 확정.

안전성 정리: 적대적 지분 $\alpha < \frac{1}{3}$ 이고 이중투표시 벌금 $\Gamma \geq 2 \cdot s_{적대}$ 일때 정직한 전략이나 시균형 (Nash Equilibrium) 을 이룬다. 이중투표는 벌금이 이득을 초과하여 불리, 검열은 수수료 수입 상실로 불리, 보류는 소수파로서 확정을 막지 못함.

공격비용: 51% 공격에 1.5 억 SOL (미화 225 억불) 이상 필요. 적발시 지분 전액 몰수. 기대 수익 음수.

3.2 실행체계: 솔라나 가상기계 (SVM)

C++20 으로 재구현된 SVM 구성요소:

구성요소	기능
BPF 실행기	다중변종 (표준, 강화, 잠금없는, 극고속)
JIT 번역기	BPF 바이트코드 기계어 직접 번역
체계 호출	암호 (Ed25519, SHA-256), 체계 변수 접근
병렬 실행	6 개 작업자 스레드, NUMA 인식, 영사본 (zero-copy) 설계

6 개 스레드 병렬 처리로 초당 185,000 건 달성. 목표 1,200,000 건은 미검증.

3.3 비동기 BPF 실행: 자율적 프로그램 작동

기존 블록체인과 달리 슬로 나나는 세 가지 자율 실행 기구를 제공한다:

- 1) 자체 예약 (Timer):** 미래 슬롯에서 스스로 실행 예약. `sol_timer_create(t실행, 되 호출 자료, 연산 예산)`. 프로그램 당 최대 16 개.
- 2) 감시기 (Watcher):** 계정 상태 변화 감시, 조건 충족 시 자동 실행. 잔고/자료 변화, 한계치 초과/미달. 프로그램 당 최대 32 개.
- 3) 순환 완충기 (Ring Buffer):** 프로그램 간 잠금 없는 선입선출 비동기 사건 통신. 프로그램 당 최대 8 개, 각 1MB.

성능: 예약기 생성 $0.07\mu s$ (14M/초), 감시기 생성 $0.12\mu s$ (8M/초), 완충기 밀기/빼기 $0.04\mu s$ (25M/초), 비동기 과업 배정 263K/초.

평가: 이더리움, 솔라나 모두 자율 실행에 외부봉사를 요구하지만 슬로 나나는 체인 자체의 결정론적 자율 실행을 실현. 인공지능 대리체 경제에 결정적 기술적 우위를 제공하며 군사 자동화 체계에도 응용 잠재력이 크다.

3.4 모형 문맥 규약 (MCP)

모든 프로그램이 자기 기능을 표준 양식으로 기술하여 인공지능 대리체가 사전 훈련 없이 임의의 프로그램을 발견/사용 가능하게 하는 체계. 세 가지 표준 접구: 도구 (Tools, 호출 가능 동작 목록과 JSON 규격),

자원 (Resources, 상태자료형식정의), 지시양식 (Prompts, 재사용가능작업흐름). 대리체의능력 한계가 « 훈련자료 » 에서 « 규약준수 » 로이동하며망의프로그램수와함께무한히확장된다. 우리공화국인공지능연구에직접응용가치가높다.

3.5 저장및망구조

저장: RocksDB(활성계정), ClickHouse(거래력사), 파일체계 (영상). 3 단계부트스트랩 (발견 → 내려받기 → 검증), 100GB 영상 255 초전송 (402MB/s).

망: CRDS 소문규약 (중국적일관성), Turbine 블록전파 (삭제부호), QUIC 저지연전송, JSON-RPC 35 개이상방법지원. limcode 열거형구별자가 u32(4 바이트) 를사용하는점은호환성구현시주의해야할세부사항이다.

제 4 장. 게임리론적안전성및토큰경제학

토큰분배: 총 1 억 \$SLON — 1,000 만개 (10%) 기존보유자공중투하, 9,000 만개 (90%) 검증자지분보상. 1 년차인플레 6.5%, 2 년차 5.2%, 지수적감소.

부의분배: 지니계수 $G = \frac{\sum_{i,j} |x_i - x_j|}{2n \sum x_i}$.

망	출시 G	1 년후 G	기구
이더리움	0.92	0.90	벤처배분 + 지분보상
솔라나	0.88	0.89	벤처배분 + 검증
비트코인	0.45	0.52	채굴분배
슬로나나	0.89	0.62	공동체 + 지분보상

Zipf($\alpha=1.2$) 분포하 $G(t) \rightarrow 0.47$ 로수렴 (벤처형 $G = 0.90$ 대조).

평가: 수학적분석은일리가있으나자본주의체제의근본모순—생산수단의사적소유—을해결하지못한다. 진정한평등은사회주의적생산관계에서만실현된다.

제 5 장. 혁명적의의 (革命的意義)

5.1 제국주의금융체계에대한위협

- (1) **달라지배약화:** 자율적대리체에의한국경없는거래체계는미제달라패권에직접적도전. 초당 185,000 건은 SWIFT 대체가능수준.
- (2) **금융제재무력화:** 분산원장기반가치이전은미제가무기화한금융제재체계를근본적으로우회할수있는기술적가능성을제공.
- (3) **중앙은행체계동요:** 자율적대리체경제의확산은중앙집중적금융통제를불가능하게하며통화정책의유효성을약화.

5.2 주체적과학기술발전에대한시사점

경애하는최고령도자동지의령도아래우리공화국이참고할핵심기술:

- (1) **잠금없는동시성:** NUMA 인식자료구조, 고성능컴퓨터체계에직접응용.
- (2) **력사증명:** SHA-256 해시연쇄, 분산체계시계동기화문제해결.
- (3) **자율실행기구:** 예약기/감시기/순환완충기, 군사자동화및산업제어에응용.
- (4) **모형문맥규약:** 프로그램자기기술, 사이버작전능력강화에참고.
- (5) **영사본동기화:** 402MB/s 전송, 대규모자료동기화에활용.

5.3 선군정치적관점

- (1) **지휘통신:** 비잔틴내결합성합의는적의전자방해환경에서도분산지휘통신의일관성을보장하는기초기술.
- (2) **자동화지능:** 자율적대리체의분산운용은군사적정보수집/분석자동화.
- (3) **암호통신:** Ed25519+SHA-256 암호학적기초는안전한통신체계참고.
- (4) **전자전내성:** 분산원장의중복성과내결합성은체계생존성향상.

제 6 장. 대응방안 (對應方案)

경애하는최고령도자동지의현명한령도아래다음과같이건의한다.

6.1 단기대응 (주체 115 년내)

- (1) **기술감시:** 원천코드저장소 (github.com/slonana-labs/slonana.cpp) 에대한지속감시. 현재판본 v0.1.495 변경사항주기적분석.
- (2) **인력양성:** 국가과학원, 김일성종합대학에블록체인전문연구반편성. C++20 고성능분산체계연구개발능력확보.
- (3) **시험망:** 내부시험망에서핵심알고리즘재현, 취약점/활용성평가.

6.2 중기대응 (주체 115-116 년)

- (1) **주체적분산원장:** 슬로나나를참고하되주체사상에기초한자주적체계를자력갱생의원칙으로독자개발.
- (2) **금융주권:** 제국주의금융제재를무력화할독자적가치이전체계구축.
- (3) **대리체연구:** MCP 개념을참고한우리식인공지능대리체규약개발.

6.3 장기대응 (주체 116 년이후)

- (1) **주체적디지털경제:** 사회주의적생산관계에부합하는블록체인기반경제관리체계. 투기와착취를배격하면서기술적장점을사회주의건설에복무하게한다.
- (2) **전략적기술우위:** 고성능합의, 자율실행, 인공지능대리체에서세계적수준을확보하여과학기술강국건설구상을실현.

제 7 장. 결론 (結論)

« 슬로나나 » 는자본주의체제의내재적모순속에서태어난기술이지만, 그기술적수준은상당히높으며, 특히자율적인공지능대리체경제를위한혁신적기술요소들을다수포함하고있다.

C++20 으로구현된 87,453 행의코드기지는초당 185,000 건의거래처리, 142 마이크로초의지연시간, 12.8 초의확정시간을달성하였다. Tower BFT 합의방식은적대적지분 $\alpha < \frac{1}{3}$ 조건에서나시균형을이루며공격비용이미화 10 억불을초과한다.

비동기 BPF 실행과모형문맥규약 (MCP) 은기존의어떤블록체인에도없는독창적혁신으로서, 우리공화국의과학기술발전에참고할가치가높은기술요소이다.

경애하는최고령도자김정은동지의현명한령도아래주체의과학기술강국건설을위한투쟁에서적의기술을정확히분석하고우리식으로소화흡수하여자력갱생의길에서더욱빛나는승리를이룩할것을 굳게확신한다.

주체 115(2026) 년 2 월 7 일

조선민주주의인민공화국
국방위원회정찰총국
과학기술정보부제 3 과

작성: 김 O 혁대좌
검토: 리 O 남소장
승인: 과학기술정보부장

극 비 본문건의열람후반드시보안담당관에게반납할것. 사본작성, 복사, 전자적전송일체금지.