Crossing the Chasm: Blockchain Scalability

블록체인 확장성 솔루션에 대하여

한겨레

kr8534@gmail.com

Scalability 팀 (김호기, 손현석, 안상화, 이종복, 전정호, 한겨레)

Make a difference

DE-FERENCE 2018

The 1st Blockchain Conference by Decipher

연사 소개

한겨레

- ✓ 서울대학교 전기공학부 학사 졸업
- ✓ 서울대학교 Petabyte-scale In-memory Database 연구실 박사과정
- ✓ 서울대학교 블록체인 학회 디사이퍼 공동 조직

진행중인 연구

- ✓ Blockchain Scalability Solutions Survey
- ✓ Lightning Network Simulations

Agenda

1. 연구 목적
2. 배경 지식
3. 확장성 솔루션 비교 분석
   - 비교표
   - 평가지표
   - 상세 설명
4. 결론

Agenda

1. 연구 목적
2. 배경 지식
3. 확장성 솔루션 비교 분석
   - 비교표
   - 평가지표
   - 상세 설명
4. 결론

The Hitchhiker's Guide to the Scalability

- ✓ 다양한 솔루션들
  - 온체인 / 오프체인 솔루션
  - 다른 자료구조 기반 (예, DAG)
  - 인터체인 / 사이드체인
  - 특정 도메인에 특화된 솔루션

The Hitchhiker's Guide to the Scalability

- ✓ 다양한 솔루션들
  - 온체인 / 오프체인 솔루션
  - 다른 자료구조 기반 (예, DAG)
  - 인터체인 / 사이드체인
  - 특정 도메인에 특화된 솔루션

The Hitchhiker's Guide to the Scalability

- ✓ 무엇을 선택해야 하는가?
  - 목적
  - 환경

확장성(Scalability)

컴퓨터 과학에서의 정의

- 시스템, 네트워크 또는 프로세스의 성능 확장성.
  여기서의 성능확장성이란 더 많은 리소스 (예, CPU 코어 등)를 투입함으로써 그에 따라 더 좋은 성능을 내는 것

블록체인에서의 정의?

- 1,000,000 TPS
- Sharding, State Channel, Application-specific Solutions, …

문제의식

- ✓ 현재 시점에서, TPS는 확장성 솔루션 비교를 위한 유일한 지표가 될 수도 없고 되어서도 안됨

- ✓ TPS 외에도 확장성 솔루션을 비교할 수 있는 여러 지표들이 있으며 나름의 기준을 세워 비교해보자!

Agenda

1. 연구 목적
2. 배경 지식
3. 확장성 솔루션 비교 분석
   - 비교표
   - 평가지표
   - 상세 설명
4. 결론

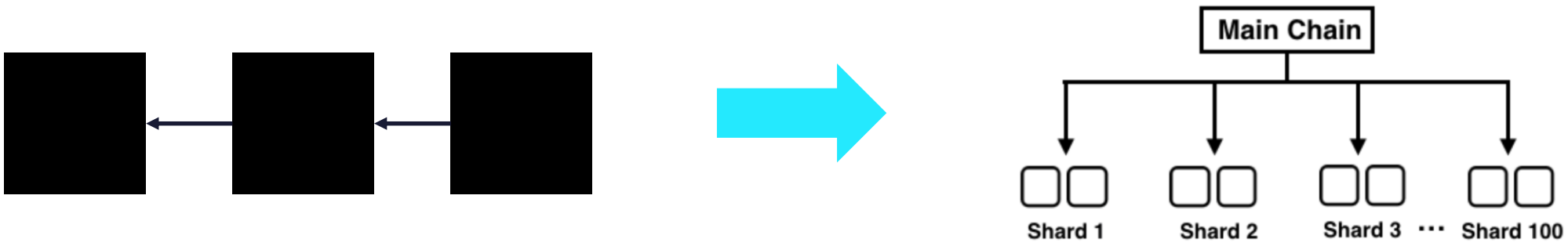
대상 프로토콜 목록

- ✓ 온체인 솔루션 / 다른 자료구조 기반 (예, DAG)
  - Sharding
  - DAG (Directed Acyclic Graph)
- ✓ 오프체인 솔루션
  - State Channel
  - Outsourcing Computation
- ✓ 인터체인 / 사이드체인
  - Two Way Pegging
  - Relayer
  - Atomic Swap

Sharding

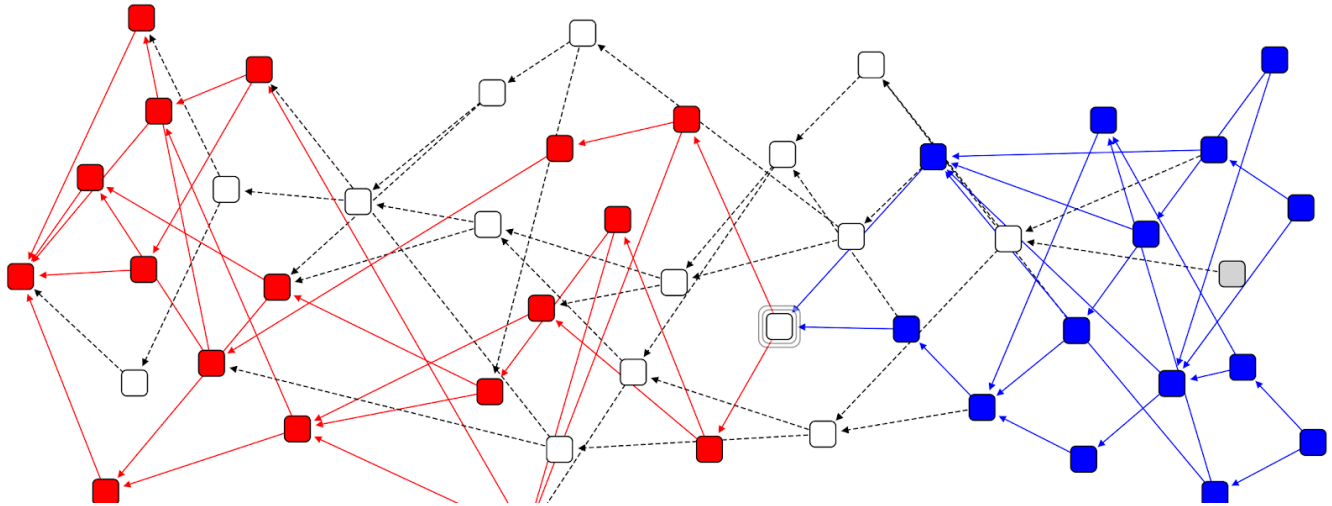
- ✓ 데이터를 여러 개의 체인에 나누어 저장 및 처리
- ✓ 난수 생성 및 샤드 체인간 트랜잭션 처리에 대한 중요성 증가

한 개의 메인 체인에서 여러 개의 샤드 체인으로

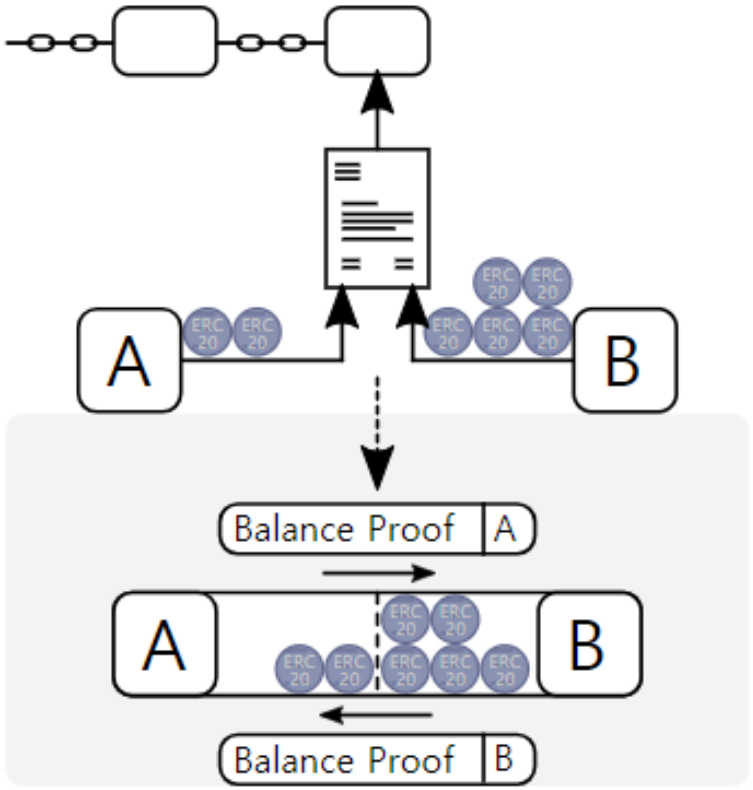


DAG (Directed Acyclic Graph)

- ✓ 블록 대신 거래를 연결
- ✓ 병렬로 그래프를 확장
- ✓ 채굴자 없이 거래 생성자가 검증 분담



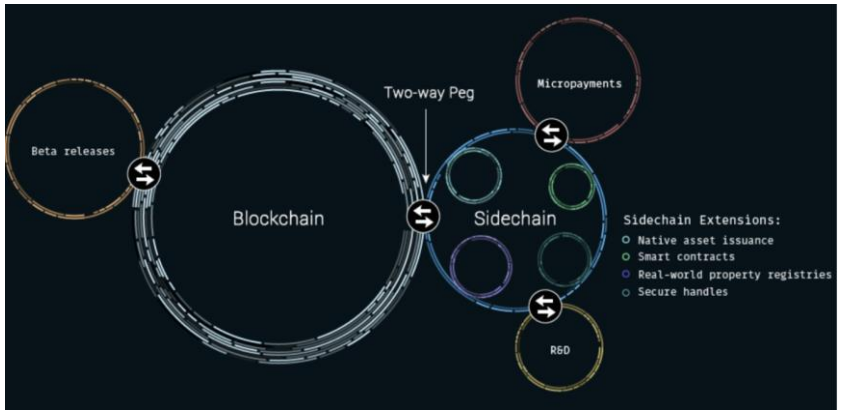
State Channel

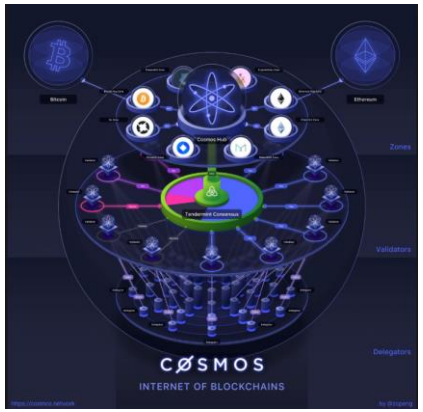


- ✓ 소수 사용자간 양방향 트랜잭션의 빠른 처리 목적
- ✓ 사용자간 트랜잭션의 최종 결과만을 메인 네트워크에 반영

Interchain / Sidechain

- ✓ 서로 다른 블록체인 네트워크간 자산/정보 교환 프로토콜
- ✓ 한 쪽에서 자산이 동결되면 다른 쪽에서 동일한 가치의 자산 생성 (two-way peg)
- ✓ 허브라는 특별한 체인에서 서로 다른 체인의 정보를 중계 (cosmos)





[디사이퍼 미디엄: 블록체인 확장성 솔루션 시리즈]

Agenda

1. 연구 목적
2. 배경 지식
3. **확장성 솔루션 비교 분석**
   - 비교표
   - 평가지표
   - 상세 설명
4. 결론

다양한 프로젝트

ethereum

zilliqa

RAIDEN NETWORK

IOTA

KOMODO

OmniLedger
A Secure, Scale-Out, Decentralized Ledger via Sharding

NANO

The Liquid Protocol

지표 선정

- ✓ Security
  - Adversary Model
  - Collusion Resistance
  - Double Spending
    - Sybil Attack
    - Long Range Attack
    - Block Withholding Attack
  - Fork Resistance
  - Single Point of Failure
- ✓ Decentralization
  - # of Consensus Participant
  - Computing Resource
  - Node Authority
  - Censorship Resistance
- ✓ Performance
  - Finality
  - Finality Time
  - Scalability

비교표: 보안

지표

프로토콜 / 프로젝트

Evaluation Metrics		Security						
Methods	Projects	adversary model	Collusion Resistance	Double Spending			Fork Resistance	Single Point of Failure
				Sybil Attack	Block Witholding Attack	Long Range Attack		
Sharding	Ethereum	39%*	+++*	+++	++	++	+++	+++
	Zilliqa	33%	++	+++	+++	+++	+++	+++
	Omni-ledger	25%	++	+++	+++	+++	+++	+++
DAG	IOTA	50%	+	+++	+++	++	+++	+++
	Hashgraph	33%	+++	+++	+++	++	+++	+++
	Nano	50%	++	+++	+++	++	+	+++
State Channel	Lightning Network	-	-	-	-	+++	-	++
	Raiden Network	-	-	-	-	+++	-	++
	Generalized State Channel	-	-	-	-	+++	-	++
Two Way Pegging	Plasma	+ - ++(*)	++	+	++	++	++	+ - ++(*)
	Plasma Cash	+ - ++(*)	+++	+++	++	++	++	+ - ++(*)
	Pegged Sidechain	50%	++			++	++	++
	Liquid	2k-n*	++			++	++	++
Atomic Swap	Komodo	50%	++			++	++	++
Relayer	BTC-Relay	-	++			++	++	
Outsourcing Computation	Truebit	-	-			-	-	+++
Annotation		N%	+++ Not Possible			+++ Not Possible ++ Possible, but Manageable + Possible, not Manageable	+++ Very Low Possibilty ++ Low Possibility + Possible	+++ One Participant Shutdown ++ Multiple Participants Shutdown + Entire Network Shutdown
		Committee number =						

진행중인 연구이기에
지표 및 수치가 변경될 수 있습니다.

비교표: 탈중앙화 및 성능

지표

Evaluation Metrics		Decentralization				Performance				
Methods	Projects	#Consensus Participant	Computing Resource	Node Authorization	Censorship Resistance	TPS	Finality	Finality Time	Scalability	#permitter?
Sharding	Ethereum	+++	L	P-L	+++*	-	D	++	O(m)	+
	Zilliqa	+++	S	P-L	++	2488 (6 shards)	D	+ (샤드에서 가검증)	O(m)	
	Omni-ledger	++ - +++	S	P-L	++		D	++	O(m)	+
DAG	IOTA	+++	L	P-L	+	500-800	P	++	O(n)	+*
	Hashgraph	+++	L	P	+	250,000	P	+++	O(n)	+*
	Nano	+++	L	P-L	++	10,000	D	++	O(n)	+++
State Channel	Lightning Network	++	S	P-L	++	-	D	-	O(1)	+
	Raiden Network	++	S	P-L	++	-	D	-	O(1)	+
	Generalized State Channel	++	S	P-L	++	-	D		O(1)	+++
Two Way Pegging	Plasma	+	S	P-L	++	-	P	+	O(m)	-
	Plasma Cash	+	S	P-L	++	-	P	+ +	O(m)	-
	Pegged Sidechain	+	S	P-L	++	-	D	+		+
	Liquid	+	S	P-L	++	-	D	+		+
Atomic Swap	Komodo	+++	L	P-L	++	20,000	D			+++
Relayer	BTC-Relay	-	S	P-L	+++	-	D			+
Outsourcing Computation	Truebit	-	L	P-L	-	-	D		-	
Annotation		+++ High ++ Medium (10~30) + Low	L : Light Nodes can participate (Do not require full-state storage) S : Only Super Nodes can join	P : Permissioned P-L : Permissionless	+++ High ++ Medium + Low	Estimated Number	D = Deterministic P = Probabilistic		n : 노드의 수 m : (샤이드) 체인의 수	+++ Only Parties to a transaction ++ Parties + 1 (ex. miner) + Parties + 2 (ex. miner, DB custodian)
										*According to the standard

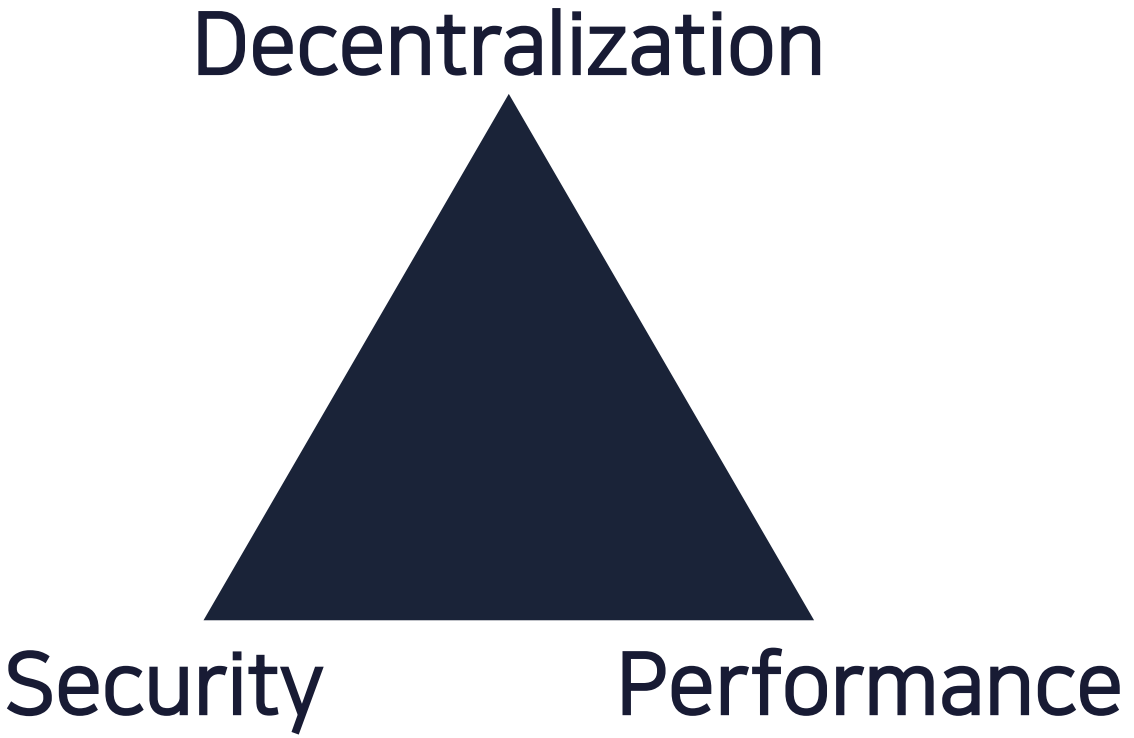
프로토콜 / 프로젝트

진행중인 연구이기에
지표 및 수치가 변경될 수 있습니다.

Agenda

1. 연구 목적
2. 배경 지식
3. **확장성 솔루션 비교 분석**
   - 비교표
   - 평가지표
   - 상세 설명
4. 결론

Scalability Solutions Survey: 평가지표



Scalability Solutions Survey: 평가지표 (1)

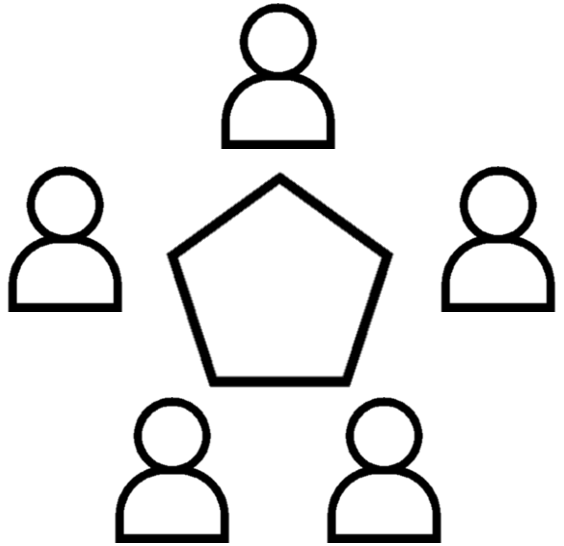
Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

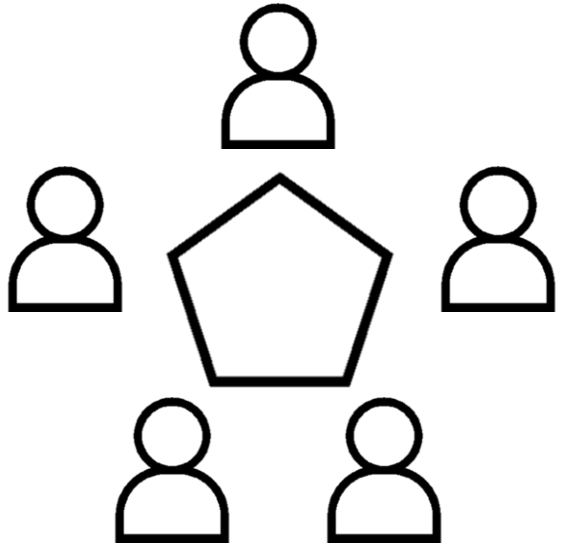


구성원의 몇%까지 비잔틴이어도
네트워크가 안전한가?

Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure



담합이 가능한가?

상(+++) : 담합 시도가 (거의) 불가능
중(++) : 담합은 가능하나, 발견하고 대처할 수 있음
하(+) : 담합이 가능하며, 대처도 할 수 없음

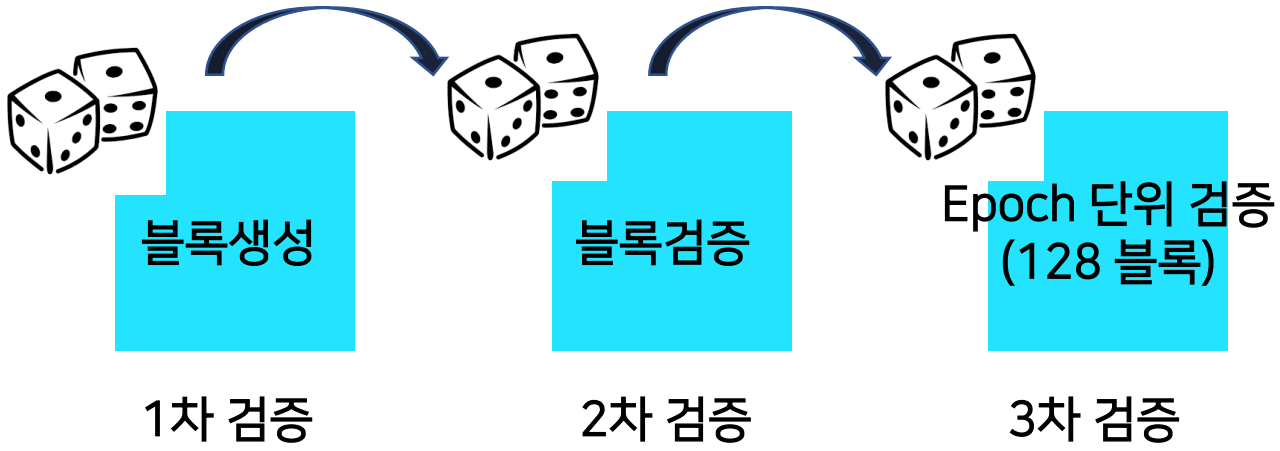
Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

ETH 샤딩: 상 (+++)

- ✓ 기존의 PoW 와 같이 채굴자가 블록을 만들고 바로 전파하는 형태가 아님
- ✓ 블록생성, 블록검증, Epoch 단위 검증의 과정을 거침



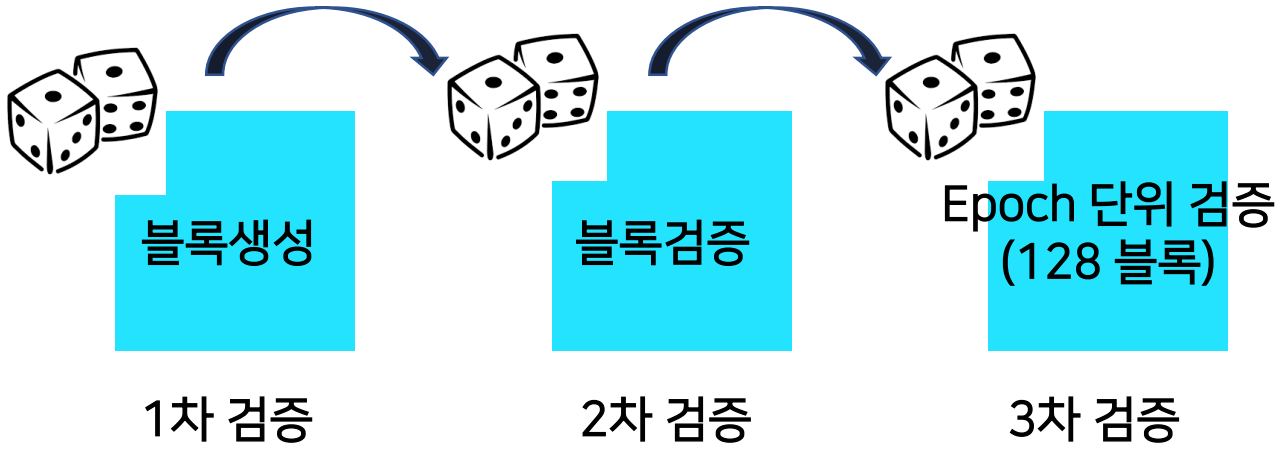
Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

ETH 샤딩: 상 (+++)

- ✓ VDF (Verifiable Delay Function) 기반 RANDAO를 통해 각 과정의 참여자 임의 선정
- ✓ 검증자 집단이 $2^9 \sim 2^{10}$ 규모일 때, 세 단계에 걸친 합의 과정을 통과시킬 가능성은 약 2^{-40}



Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

플라즈마: 중 (++)

- ✓ 부모 체인으로 제출되는 트랜잭션의 내용을 통해 담합 유무를 판단할 수 있음
- ✓ 해당 플라즈마 체인을 나가는 형태로만 대응 가능

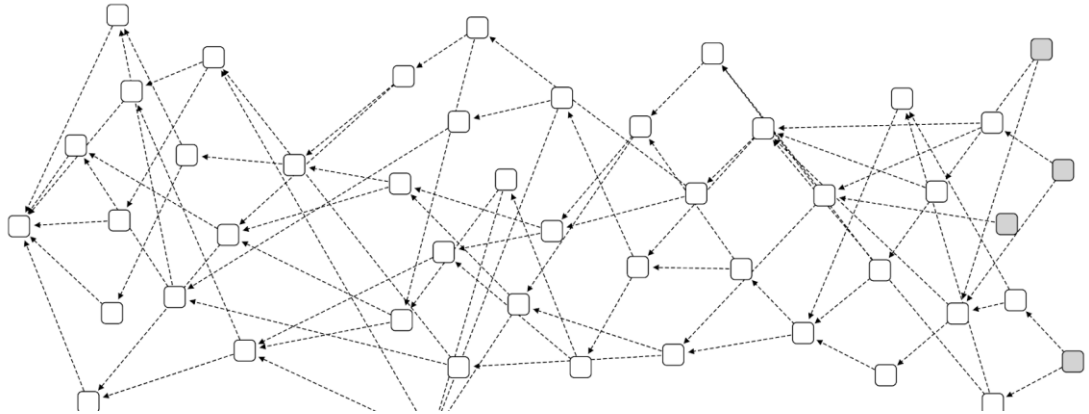
Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

IOTA: 하 (+)

- ✓ 다수가 특정 거래를 의도적으로 피하면, 거래가 인정받지 못하고 취소 확률이 높아짐
- ✓ 거래 뒤에 모순되는 거래를 연결하여 적극적으로 방해할 수도 있음
- ✓ 하지만 전자의 경우, 담합에 의한 결과인지 임의로 거래를 선택해 검증하는 과정에서의 결과인지 판단이 힘듦

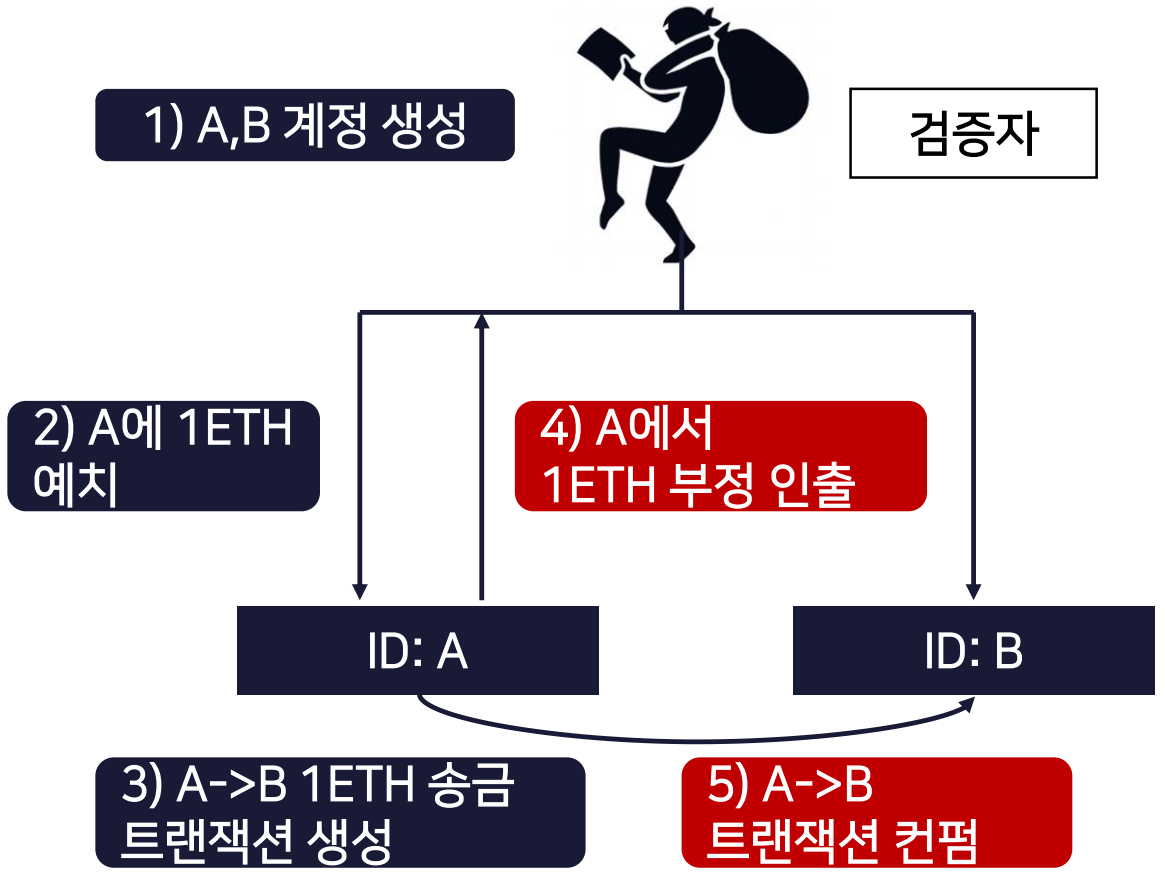


Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

Sybil Attack: 혼자서 마치 여러 명인 것처럼 속이는 공격 형태



Scalability Solutions Survey: 평가지표 (1)

Security

- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

상 (+++) : Sybil Attack이 (거의) 불가능한가 혹은 효과가 없는가
중 (++) : Sybil Attack이 일어날 수도 있지만 대처가능한가
하 (+) : Sybil Attack이 발생해도 대처가 불가능한가

Scalability Solutions Survey: 평가지표 (1)

Security

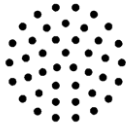
- ✓ Adversary Model
- ✓ Collusion Resistance
- ✓ Double Spending
  - Sybil Attack
  - Long Range Attack
  - Block Withholding Attack
- ✓ Fork Resistance
- ✓ Single Point of Failure

특정 노드가 공격받았을 때 (예, 해킹 / DoS 등)

상 (+++) : 해당 노드만 정상적인 작동을 못할 경우
중 (++) : 몇몇 다른 노드들이 정상적인 작동을 못할 경우
하 (+) : 네트워크 전체가 마비될 경우

Scalability Solutions Survey: 평가지표 (2)

Decentralization

		Evaluation
✓ # of Consensus Participant (합의 과정에 참여하는 노드 수)		+ / ++ / +++
✓ Computing Resource (라이트 노드도 합의 과정에 참여할 수 있는가?)		X / O
✓ Node Authorization (합의 과정에 참여하기 위해 허가가 필요한가?)		O / X
✓ Censorship Resistance (검열이 가능한가?, 검열에 대응 가능한가?)		+ / ++ / +++

Decentralized

Scalability Solutions Survey: 평가지표 (3)

Performance

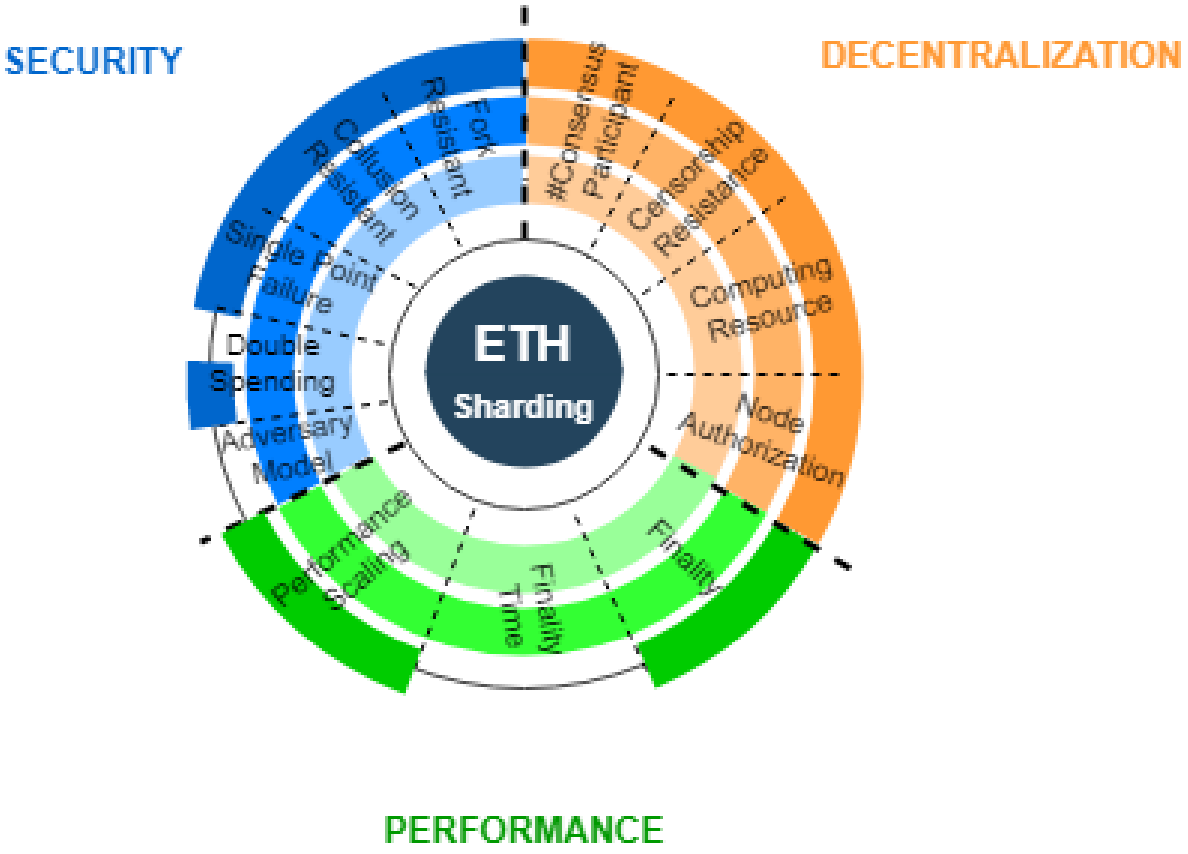
	Evaluation
✓ ~~TPS (Transaction Per Second)~~	Not Evaluated
✓ Finality (Probabilistic vs Deterministic)	X / O
✓ Finality Time (트랜잭션이 확정되는데 얼마나 걸리는지)	+ / ++ / +++
✓ Scalability (더 많은 노드/체인에 비례해 성능이 증가하나)	Bad / Good

Agenda

1. 연구 목적
2. 배경 지식
3. **확장성 솔루션 비교 분석**
   - 비교표
   - 평가지표
   - 상세 설명
4. 결론

이더리움 Sharding

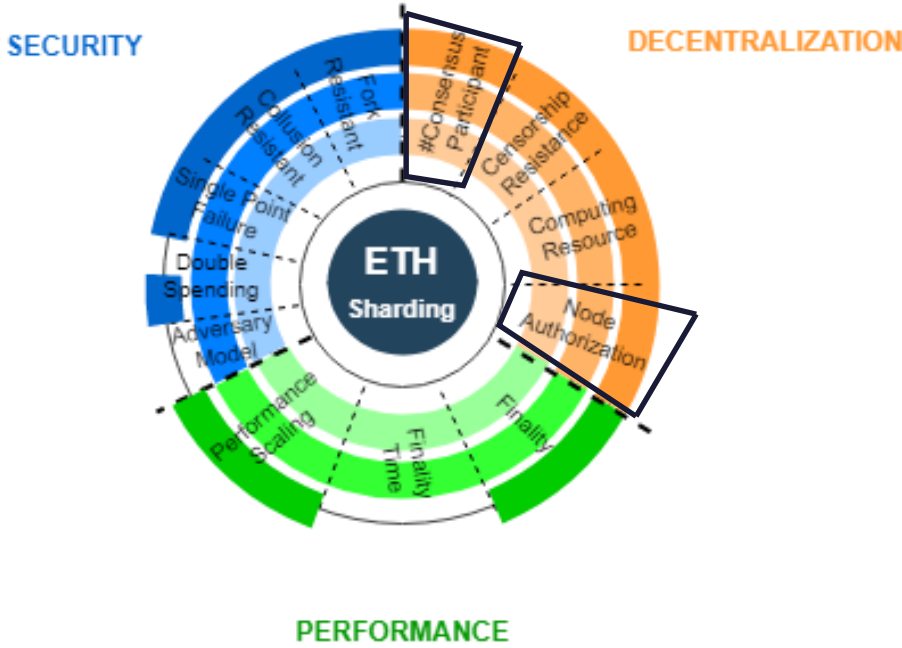
- ✓ 탈중앙화 모든 지표에 있어서
  타 솔루션에 비해 높음
- ✓ 마찬가지로 보안성 항목의
  대부분 공격에 대응 가능
- ✓ 다른 솔루션에 비해
  비약적인 성능 향상은
  없을 것으로 보이나, 알 수 없음
  - 샤드 체인 간 트랜잭션 등
    오픈 이슈가 있으나
    실제로 어느 정도인지 확인 불가



이더리움 Sharding

Decentralization | Security | Performance

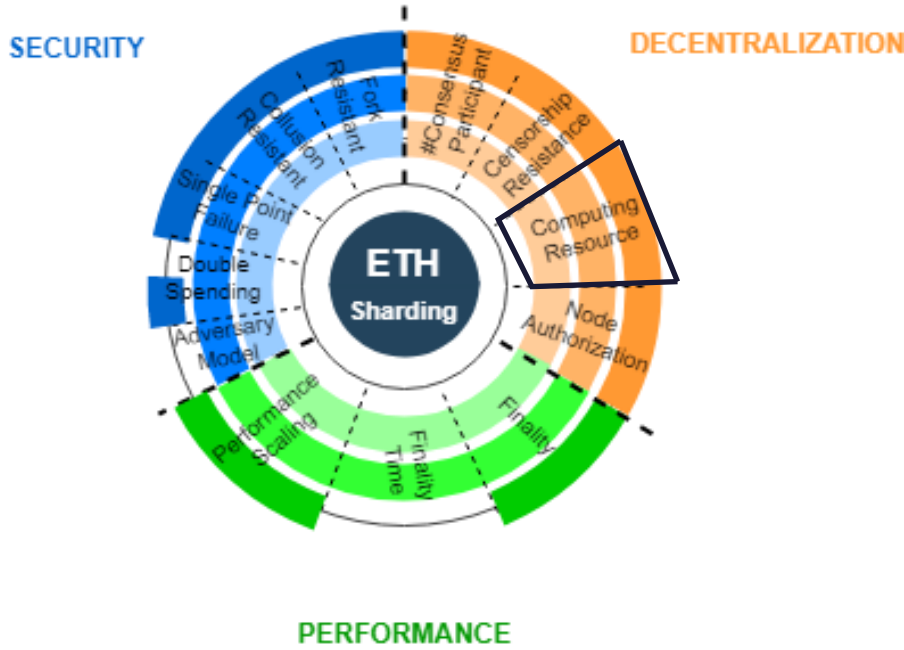
- ✓ # of Consensus Participant
  - 컨센서스 참여자의 숫자 제한이 없음
  - 참여자가 많을수록 랜덤성에 영향을 받는 지표들이 더 안전 (예, 검증자 집단 $2^9 \sim 2^{10}$ ➔ 61% honesty assumption w/ 2^{-40})
- ✓ Node Authorization
  - 32 ETH를 예치하면 누구나 컨센서스 과정에 참여할 수 있음 (Permission-less)



이더리움 Sharding

Decentralization | Security | Performance

- ✓ Computing Resource
  - 슈퍼컴퓨터를 보유하고 있지 않아도 합의 과정에 참여할 수 있도록 하자!
  - Stateless client 및 delayed state execution 의 도입을 통해 누구나 참여할 수 있도록 함



이더리움 Sharding

Decentralization | Security | Performance

✓ Computing Resource

- Stateless client: full state를 들고 있지 않아도 state root 및 트랜잭션 정보만을 이용해서 검증을 수행할 수 있게 함

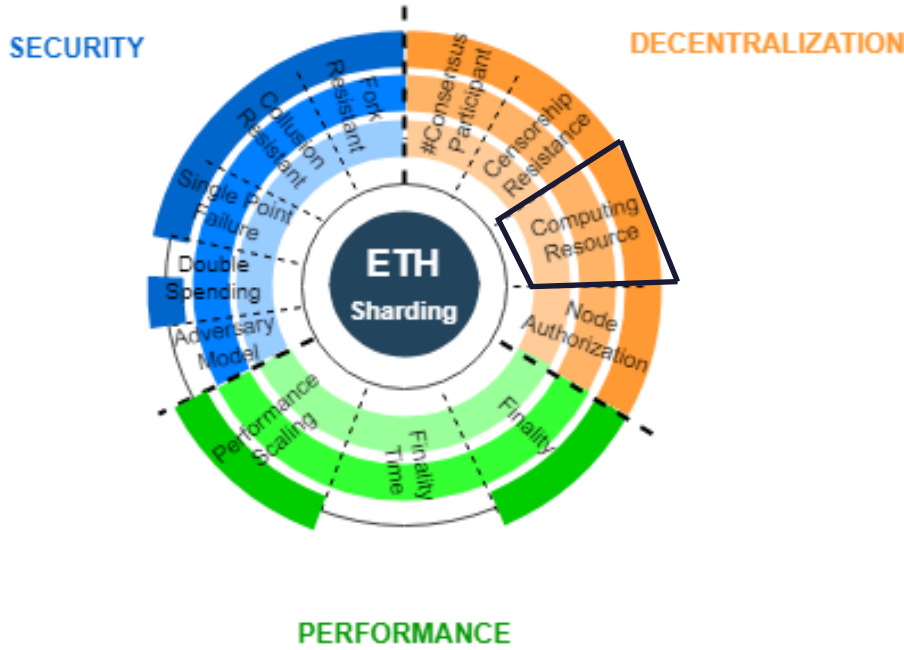
```
TX Body {
  To: ···
  Value: ···
  ···
}
```

AS-IS

```
TX Body {
  To: ···
  Value: ···
  ···
  Witness:
}
```

TO-BE

RLP-encoded List of Merkle Tree Nodes



이더리움 Sharding

Decentralization | Security | Performance

- ✓ Computing Resource
  - Stateless client: full state를 들고 있지 않아도 state root 및 트랜잭션 정보만을 이용해서 검증을 수행할 수 있

트랜잭션을 보낼 때
머클 증명을 누구나 만들 수 있는가?

}

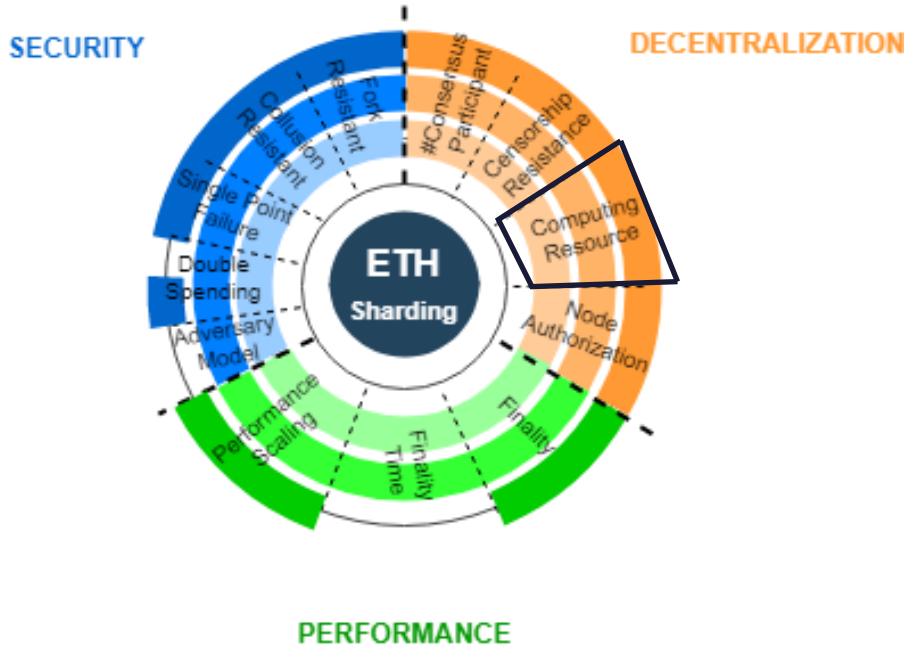
Witness:

}

RLP-encoded List of Merkle Tree Nodes

AS-IS

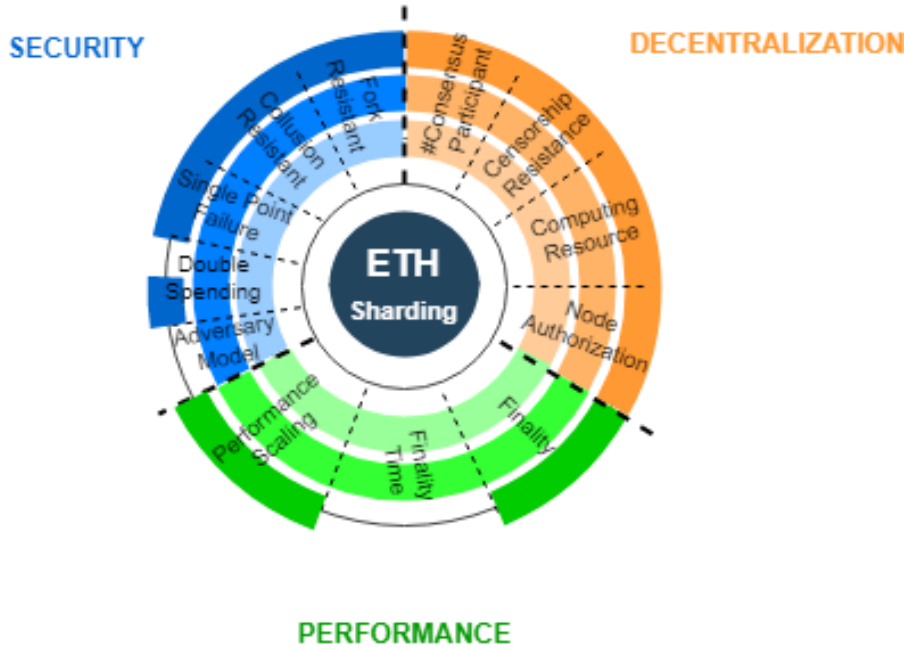
TO-BE



이더리움 Sharding

Decentralization | **Security** | Performance

- ✓ Single Point of Failure
  - 블록 생성을 제대로 하지 않아도
    다음 순번의 생성자에 의해 정상적으로 동작
  - 블록 검증에 참여하지 않거나
    비정상적으로 행동하여도
    나머지 검증자에 의해 $\frac{2}{3}$ 충족 가능
- ✓ Double Spending
- ✓ Fork Resistance
- ✓ Adversary Model



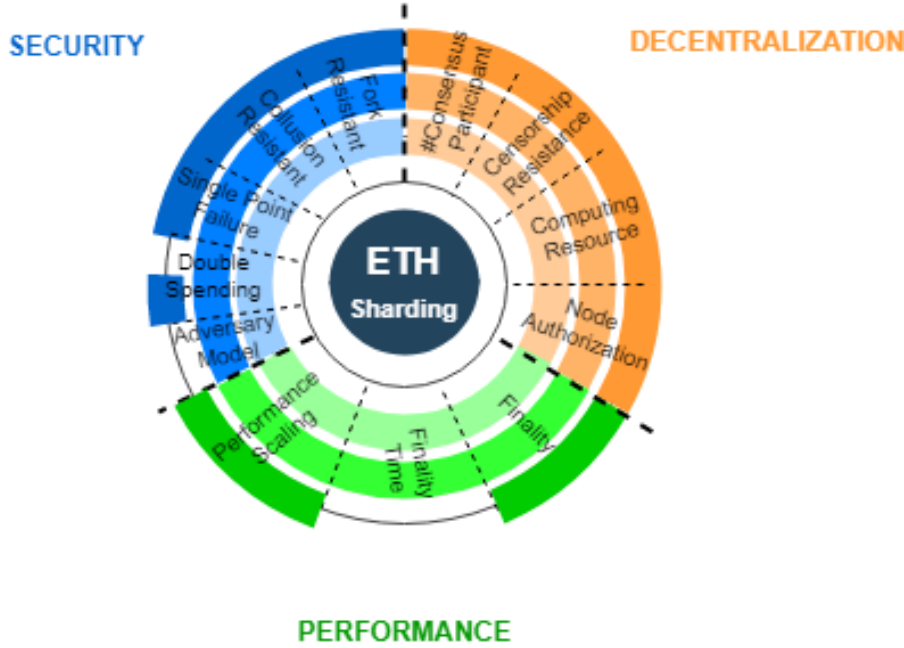
이더리움 Sharding

Decentralization | Security | **Performance**

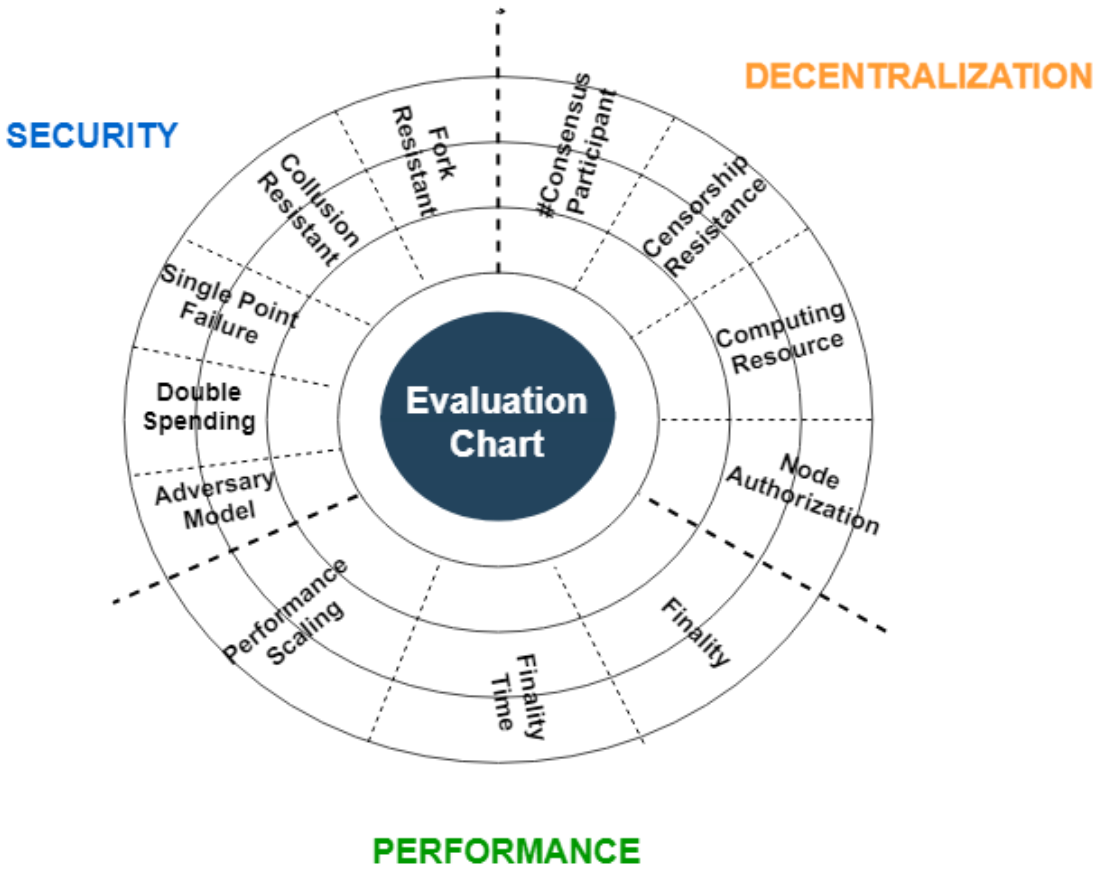
- ✓ Finality: Deterministic

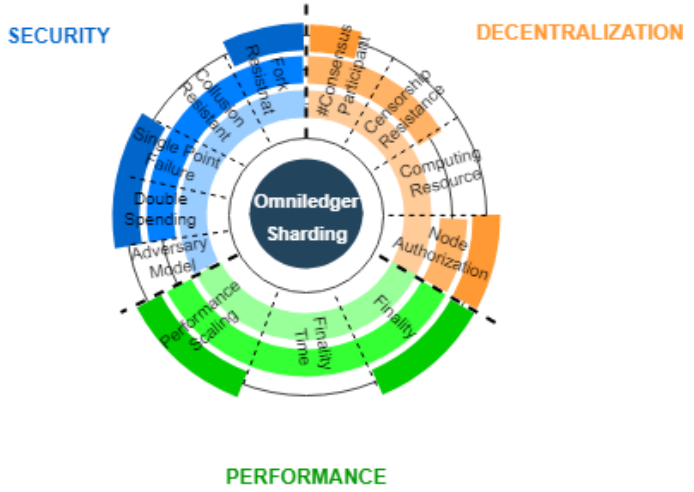
네트워크 구축이 안된 지금 시점에서 성능 비교는 무리

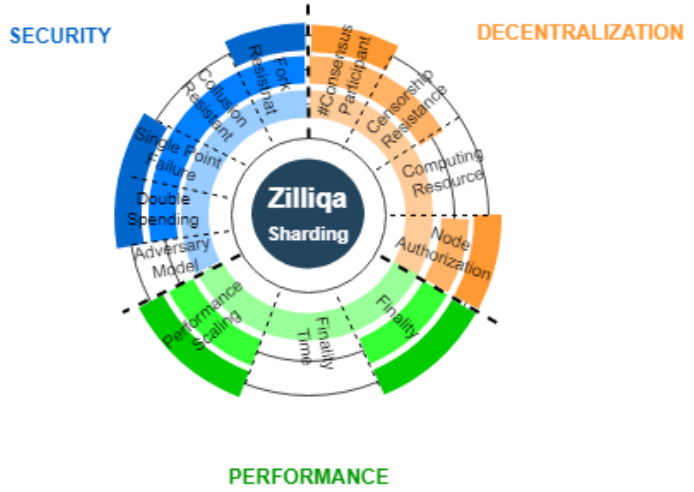
- ✓ ~~TPS~~
- ✓ Finality Time: ++
- ✓ Scalability: O(m)
  - cross-shard communication 에서 얼마나 성능 저하가 있는지 판단이 힘듦
  - 하지만 샤드 체인의 개수가 어카운트에 따라 늘어나는 디자인이 아니라, 개수를 유지하는 형태

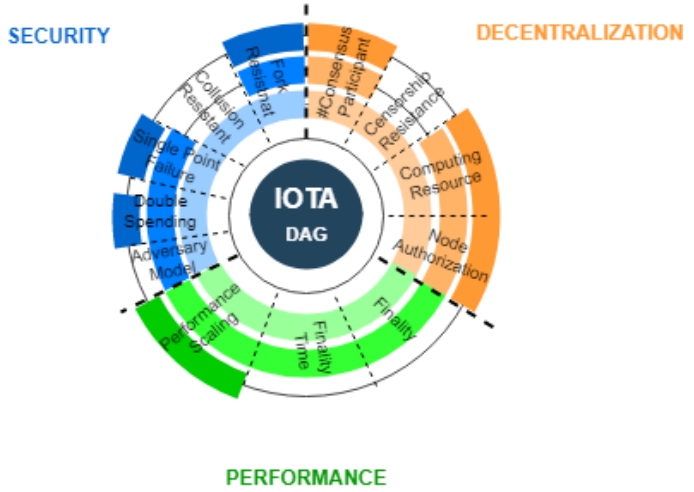


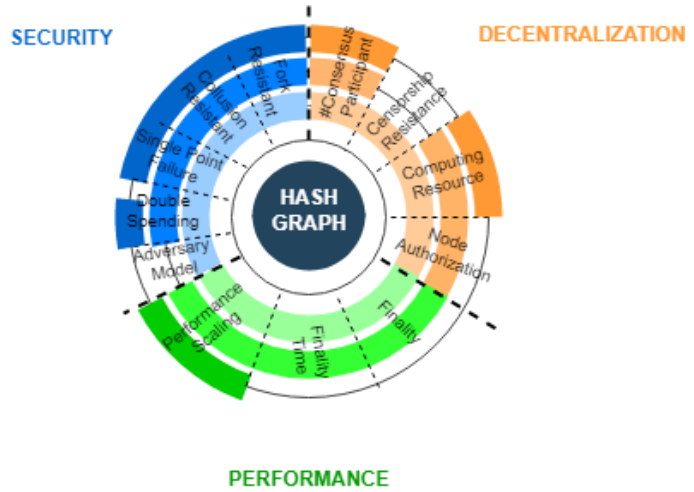
나머지 솔루션들



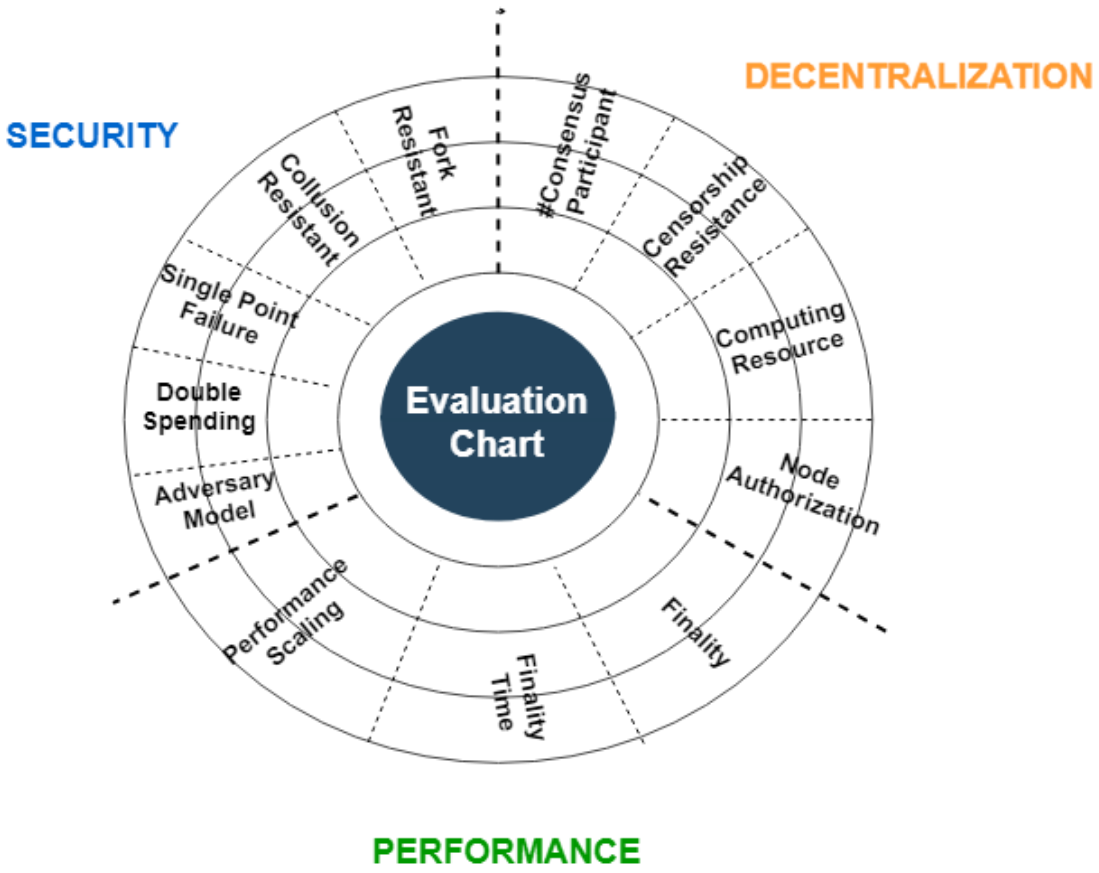


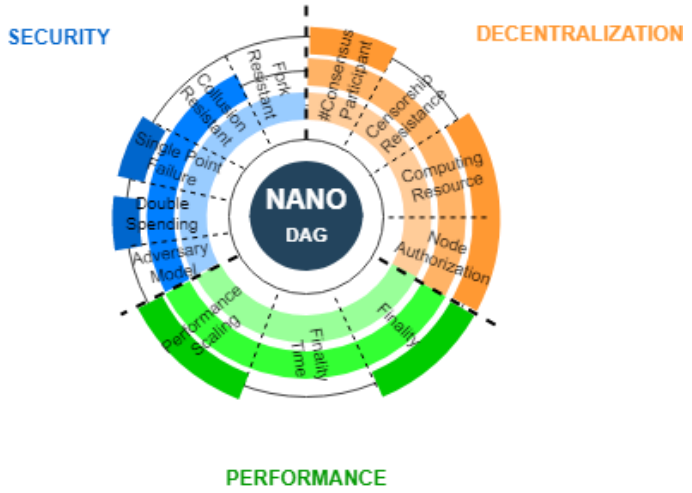


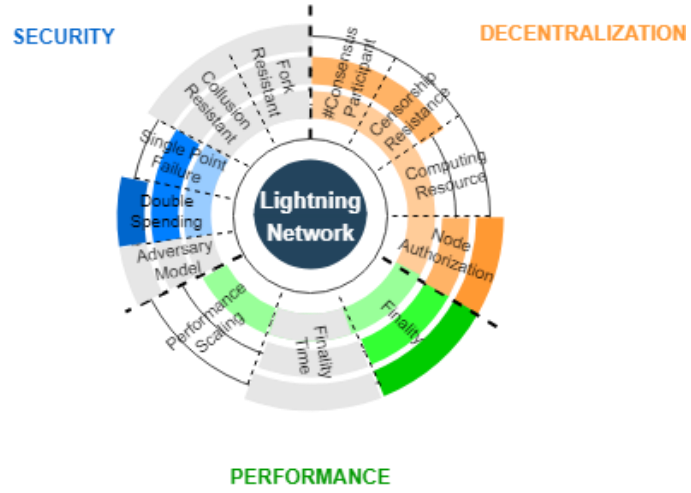


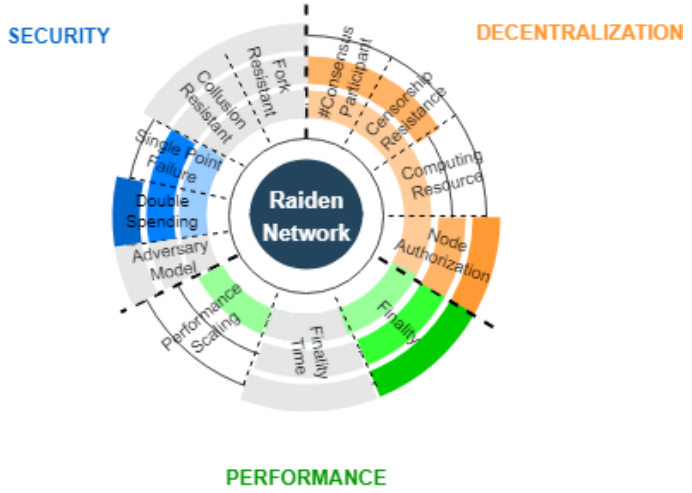


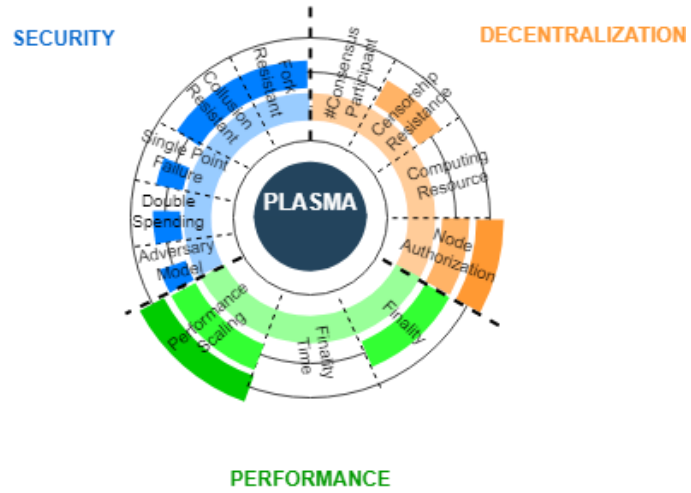
나머지 솔루션들



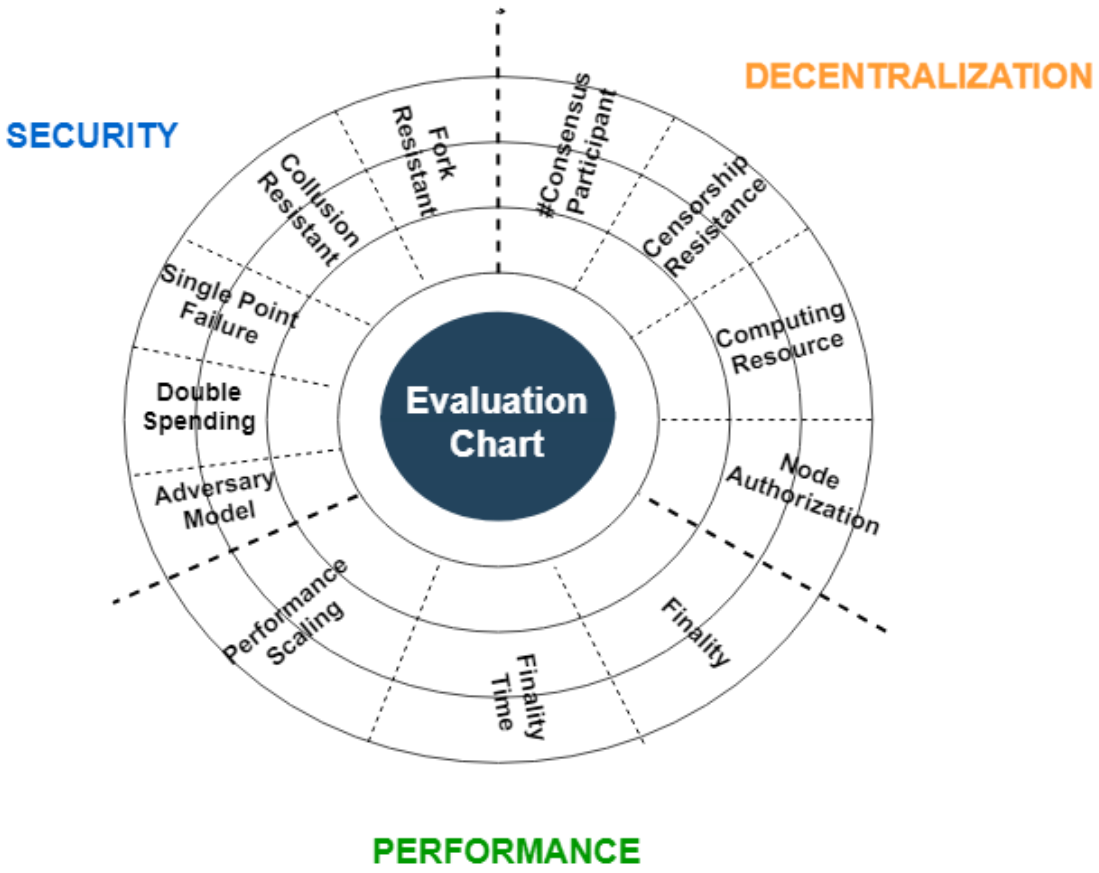


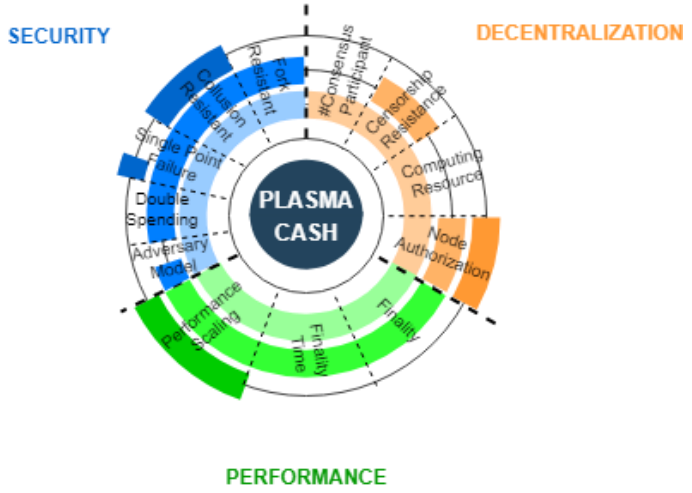


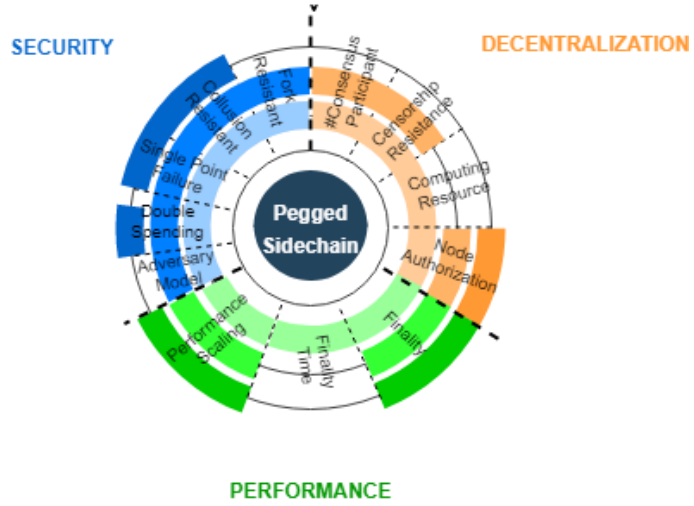


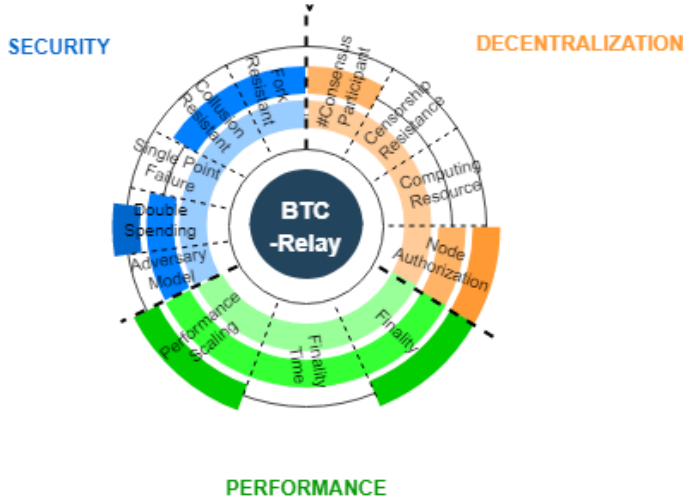


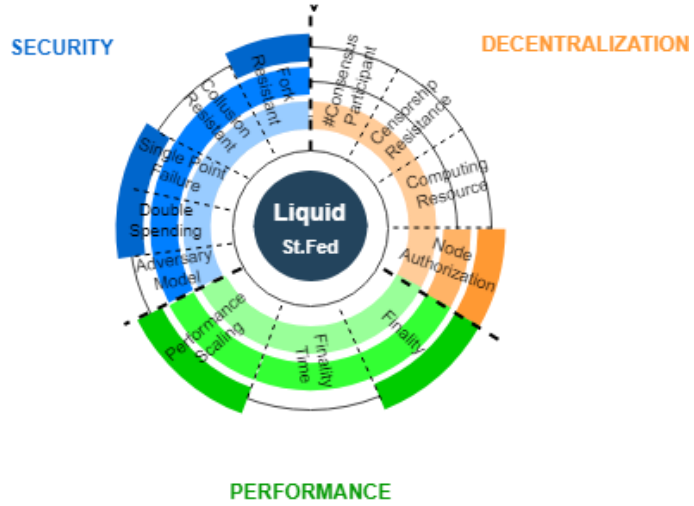
나머지 솔루션들



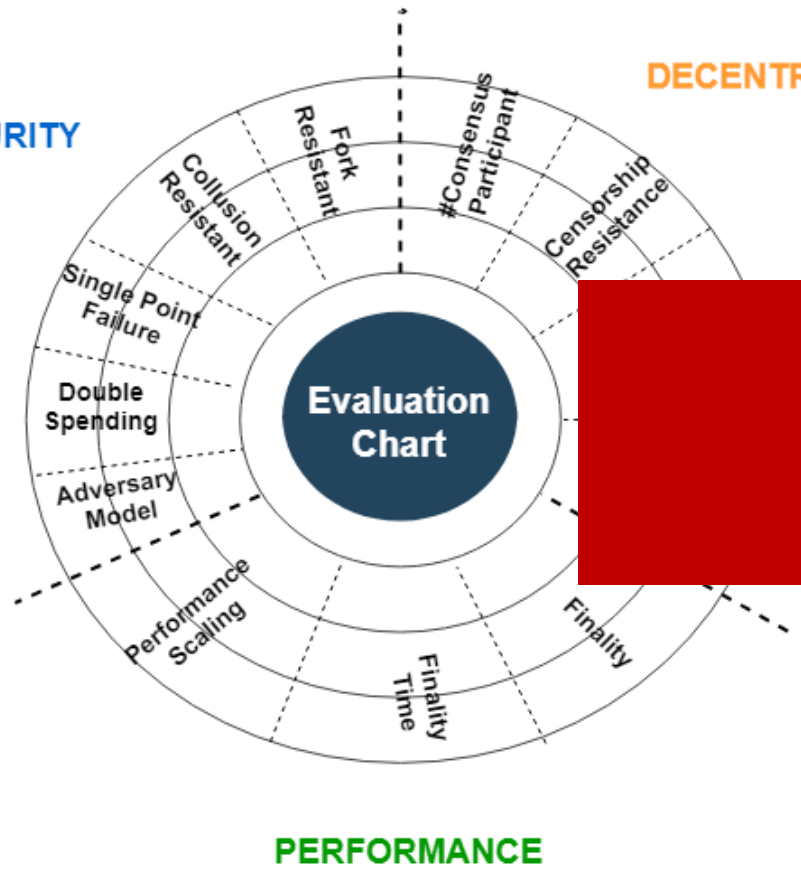


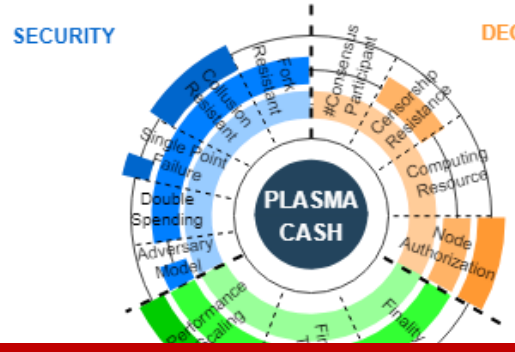




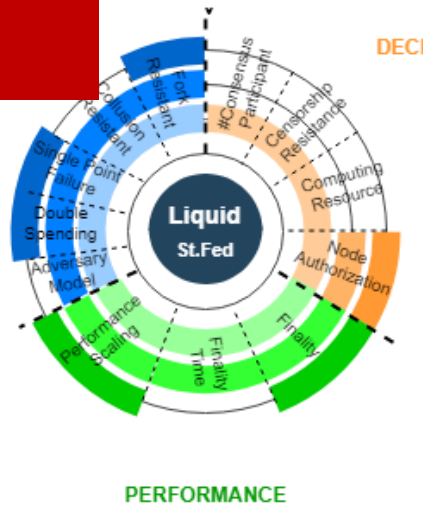


나머지 솔루션들





어딘가 희생하고 있음



Agenda

1. 연구 목적
2. 배경 지식
3. 확장성 솔루션 비교 분석
   - 비교표
   - 평가지표
   - 상세 설명
4. **결론**

Takeaway

- ✓ 대부분의 솔루션이 네트워크가 없는 현재 상황에서
  성능적인 부분, 특히 TPS를 놓고
  뭐가 TPS가 높을지 비교하는 것은 시기상조임.

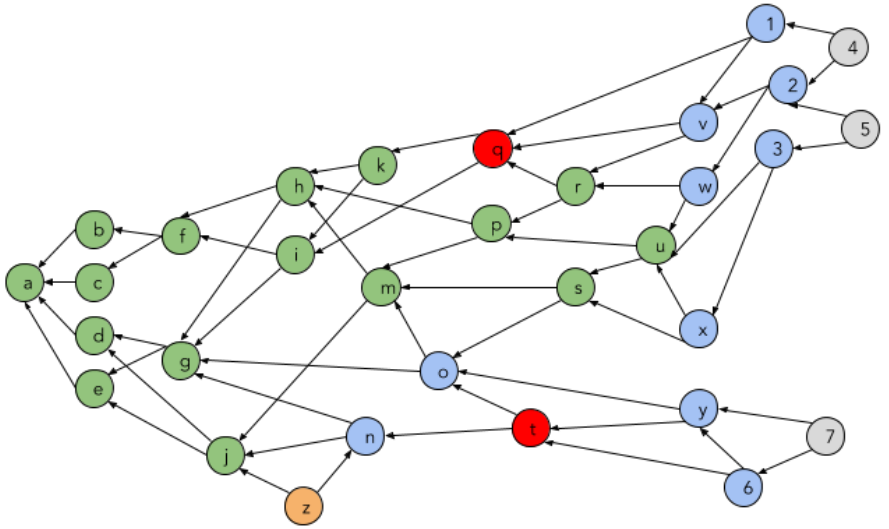
- ✓ 비교를 한다면 얼마나 안전한지,
  얼마나 탈중앙화 기치에 맞는지로 비교해야함.

- ✓ 다양한 프로토콜 및 프로젝트를
  동일선상에서 비교 분석했다는 것에 의의.

- ✓ 단순 survey보다는 시뮬레이션을 통한 보완이 필요.

향후 연구 방향

- ✓ 라이트닝 네트워크, DAG, 샤딩 시뮬레이션
  - ✓ Hub ratio, availability 비율에 따른 라이트닝 네트워크 시뮬레이션
  - ✓ Tip 선택 알고리즘에 따른 DAG 거래 시뮬레이션
  - ✓ 기존 트랜잭션 통계 기반 샤드 체인간 통신 빈도 시뮬레이션



References

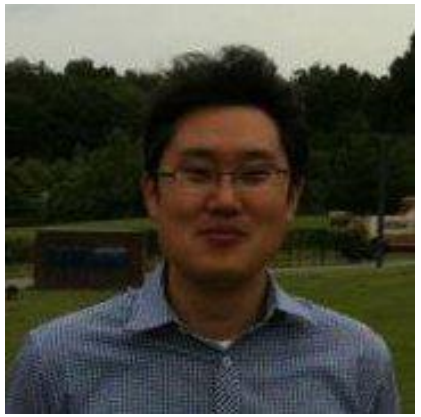
1. Croman, Kyle, et al. "On scaling decentralized blockchains." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016.
2. Eyal, Ittay, et al. "Bitcoin-NG: A Scalable Blockchain Protocol." NSDI. 2016.
3. Goswami, Sneha. "Scalability analysis of blockchains through blockchain simulation." (2017).
4. Li, Wenting, et al. "Towards scalable and private industrial blockchains." Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017.
5. Bano, Shehar, Mustafa. Al-Bassam, and George Danezis. "The road to scalable blockchain designs." USENIX; login: magazine (2017).
6. Bano, Shehar, et al. "Consensus in the age of blockchains." arXiv preprint arXiv:1711.03936 (2017).
7. Luu, Loi, et al. "A secure sharding protocol for open blockchains." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.
8. Gao, Yuefei, and Hajime Nobuhara. "A Proof of Stake Sharding Protocol for Scalable Blockchains." Proceedings of the Asia-Pacific Advanced Network 44 (2017): 13-16.
9. Kokoris-Kogias, Eleftherios, et al. "Omniledger: A secure, scale-out, decentralized ledger via sharding." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.
10. Decker, Christian, Rusty Russell, and Olaoluwa Osuntokun. "eltoo: A Simple Layer2 Protocol for Bitcoin."
11. Miller, Andrew, et al. "Sprites: Payment channels that go faster than lightning." CoRR abs/1702.05812 (2017).
12. Dziembowski, Stefan, Sebastian Faust, and Kristina Hostakova. Foundations of state channel networks. IACR Cryptology ePrint Archive, 2018: 320, 2018.
13. Sompolinsky, Yonatan, and Aviv Zohar. "Secure high-rate transaction processing in bitcoin." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2015.
14. Lewenberg, Yoad, Yonatan Sompolinsky, and Aviv Zohar. "Inclusive block chain protocols." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2015.
15. Sompolinsky, Yonatan, Yoad Lewenberg, and Aviv Zohar. "SPECTRE: A Fast and Scalable Cryptocurrency Protocol." IACR Cryptology ePrint Archive 2016 (2016): 1159.
16. Boyen, Xavier, Christopher Carr, and Thomas Haines. Blockchain-free cryptocurrencies: A framework for truly decentralised fast transactions. Cryptology ePrint Archive, Report 2016/871, 2016.

References

17. Bitcoin scalability problem, https://en.wikipedia.org/wiki/Bitcoin_scalability_problem
18. Segwit2x, https://en.wikipedia.org/wiki/SegWit2x
19. Ethereum Sharding Conpendium, https://notes.ethereum.org/s/BJc_eGVFM
20. Sharding Phase1, https://ethresear.ch/t/sharding-phase-1-spec-retired/1407
21. Zilliqa, https://docs.zilliqa.com/whitepaper.pdf
22. TON, https://www.kriptovaluta.hr/wp-content/uploads/2018/03/TON-Technology.pdf
23. Making Sense of Ethereum's Layer 2 Scaling Solutions, https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4
24. Counterfactual: Generalized State Channels, https://l4.ventures/papers/statechannels.pdf
25. DagCoin Draft, https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf
26. SPECTRE (BlockDAG), https://docs.wixstatic.com/ugd/242600_bc8db338d74a4cdcbf90a81ab78a7711.pdf
27. PHANTOM (BlockDAG), https://docs.wixstatic.com/ugd/242600_92372943016c47ecb2e94b2fc07876d6.pdf
28. PHANTOM, GHOSTDAG (BlockDAG), https://eprint.iacr.org/2018/104.pdf
29. IOTA, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvslqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
30. Hashgraph, https://swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf
31. Nano, https://nano.org/en/whitepaper
32. EOS, https://github.com/EOSIO/Documentation/blob/master/ko-KR/TechnicalWhitePaper.md

우리팀!!!

김호기



전정호

손현석

한겨레

이종복

안상화

Q&A

한겨레 (kr8534@gmail.com)