Table III

COMPARISON OF DIFFERENT POX SCHEMES FOR PERMISSIONLESS BLOCKCHAINS

Puzzle Name	Origin of Hardness (One-way Function)	Designing Goal	Implementation Description	ZKP Properties	Simulation of Random Function	Features of Puzzle Design	Network Realization
Primitive proof of work [25], [82]	Partial preimage search via exhaustive queries to the random oracle	Sybil-proof	Repeated queries to cryptographic hash function	Yes	Yes	Single challenge	Bitcoin [1], Litecoin [88]
Proof of exercise [101]	Matrix product	Computation delegation	Probabilistic verification	N/A	No	Single challenge	N/A
Useful proof of work [80]	K-orthogonal vector, 3SUM, all-pairs shortest path, etc.	Computation delegation	Non-interactiveness via Fiat-Shamir transformation	Yes	Yes	Single challenge with sequential hash queries	N/A
Resource-efficient mining [96]	N/A	Computation delegation	Guaranteed by TEE	Yes	Yes	Trusted random oracle implemented by dedicated hardware	N/A
Proof of retrievability [106]	Merkle proofs of file fragments in the Merkle tree	Distributed storage	Non-interactiveness via Fiat-Shamir transformation and random Merkle proofs	Yes	Conditional	Two-stage challenge	Permacoin [105], KopperCoin [67]
Proof of space -time [38]	The repeated proof of retrievability over time	Decentralized storage market	Repeated PoR	Yes	Conditional	Two-stage challenge and repeated PoR over time	Filecoin [38]
Equihash [77]	The generalized birthday problem	ASIC resistance	Time-space complexity trade-off in proof generation [77]	Yes	Yes	Memory-hard	Zcash [42]
Ethash [110]	Random path searching a random DAG	ASIC resistance	Repeated queries to cryptographic hash function	Yes	Yes	Sequential, memory-hard puzzle	Ethereum [37]
Nnonoutsourceable scratch-off puzzle [78]	Generalization of proof of retrievability	Centralization resistance	Random Merkle proof	Yes	Yes	Two-stage challenge	N/A
Proof of space [112]	Merkle proofs of a vertex subset in a random DAG	Energy efficiency	Random Merkle proof	Yes	Yes	Two-stage challenge and measurement of proof quality	SpaceMint [112]
Proof of human work [98]	Radom CAPTCHA puzzle requiring human effort	Useful work and energy efficiency	CAPTCHA and PoW	Yes	Yes	Human in the loop	N/A