BLOCKCHAIN

- HIERARCHICAL: SOME CA WILL DECIDE ABOUT CERTIFICATION OR REVOCATION OF KEYS. THEY'RE LOG-BASED AND USE BLOCKCHAIN AS AN APPEND-ONLY PUBLIC BULLETIN. THIS PROPOSAL CAN BE SEEN AS A RELAXED CENTRALIZATION.
- WEB OF TRUST: THIS PROPOSAL REPLACE CA WITH MINERS. CERTIFICATE OWNERS PAY MINERS FOR THEY WORK.

- WANG USED BLOCKCHAIN AS A PUBLIC LOG TO MONITOR CA' SIGNING AND REVOCATION OPERATION. THE MINERS APPEND A TRANSACTIONS AFTER VERIFYING IT.

- KUBILAY INTRODUCED CERTLEDGER WHICH USES PUBLIC BLOCKCHAIN AS A PUBLIC LOG TO VALIDATE, STORE AND REVOKE CERTIFICATES.

- LEWISON USED ETHERIUM PLATFORM FOR PKI MANAGMENT AND MAINTENING KEYS. CENTRALIZED CA FOR ADDING AND REVOKING KEYS. THE CA IS CONSIDERED AS THE ROOT OF THE CHAIN. THE BLOCKCHAIN IS USED AS

A PUBLIC LOG.

○ MATSUMOTO AND REISCHUK PROPOSED IKP, (ETHERIUM BASED) IT USES SMART CONTRACTS TO OFFER AUTOMATIC RESPONSE TO CA MISBEHAVIOR AND INCENTIVATES FOR THOSE WHO HELP IN DETECTING MISBEHAVIORS. OF COURSE CA HAS A CENTRAL ROLE.

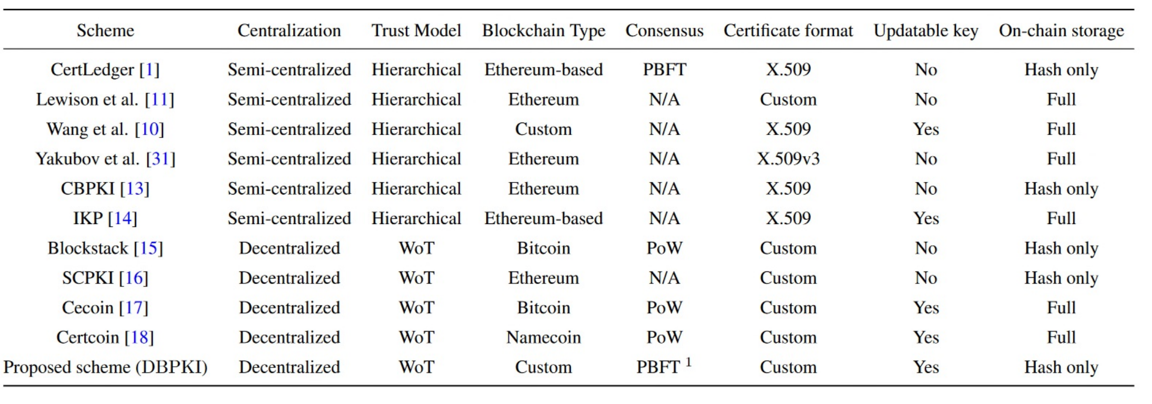
○ QIN PROPOSED CECOIN. CERTIFICATES ARE TREATED AS CURRENCIES AND STORED IN THE BLOCKCHAIN. MINERS GET PAID BY CERTIFICATE OWNER

○ ALBASSAM INTRODUCED SCPKI, EACH ENTITY USE SMART CONTRACTS TO PUBLISH A SET OF ATTRIBUTES, IT`S BASED ON ETHERIUM PLATFORM AND ALLOW ENTITY TO STORE E VERIFY IDENTITIES TROUGH A PGP-LIKE WEB OF TRUST. IT`S HAVE LIMITATIONS ABOUT ADAPTABILITY AND PRIVACY.

○ ALI INTRODUCED BLOCKSTACK, BASED ON BITCOIN BLOCKCHAIN, IT PROVIDE A NAME REGISTRATION SERVICE THAT ALLOW TO BIND PUBLIC KEYS TO THEIR NAMES.

- FROMKNECHT PROPOSED CERTCOIN, A BBPKI WHICH ENSURES IDENTITY RETENTION (TO PREVENT REGISTERING DIFFERENT PUBLIC KEYS FOR ONE IDENTITY).

- ANADA PROPOSED TO INCLUDE NOT ONLY THE SUBJECT ID INTO PUBLIC KEY BUT ALSO THE GUARANTORS' PUBLIC ID. THEY SUGGEST USING BLOCKCHAIN FOR MAINTAINING THE LIST OF KEYS IN A CONSISTENT WAY.



Scheme	Centralization	Trust Model	Blockchain Type	Consensus	Certificate format	Updatable key	On-chain storage
CertLedger [1]	Semi-centralized	Hierarchical	Ethereum-based	PBFT	X.509	No	Hash only
Lewison et al. [11]	Semi-centralized	Hierarchical	Ethereum	N/A	Custom	No	Full
Wang et al. [10]	Semi-centralized	Hierarchical	Custom	N/A	X.509	Yes	Full
Yakubov et al. [31]	Semi-centralized	Hierarchical	Ethereum	N/A	X.509v3	No	Full
CBPKI [13]	Semi-centralized	Hierarchical	Ethereum	N/A	X.509	No	Hash only
IKP [14]	Semi-centralized	Hierarchical	Ethereum-based	N/A	X.509	Yes	Full
Blockstack [15]	Decentralized	WoT	Bitcoin	PoW	Custom	No	Hash only
SCPKI [16]	Decentralized	WoT	Ethereum	N/A	Custom	No	Hash only
Cecoin [17]	Decentralized	WoT	Bitcoin	PoW	Custom	Yes	Full
Certcoin [18]	Decentralized	WoT	Namecoin	PoW	Custom	Yes	Full
Proposed scheme (DBPKI)	Decentralized	WoT	Custom	PBFT [1]	Custom	Yes	Hash only

References and examples taken from arxiv.org/pdf/2012.15351.pdf