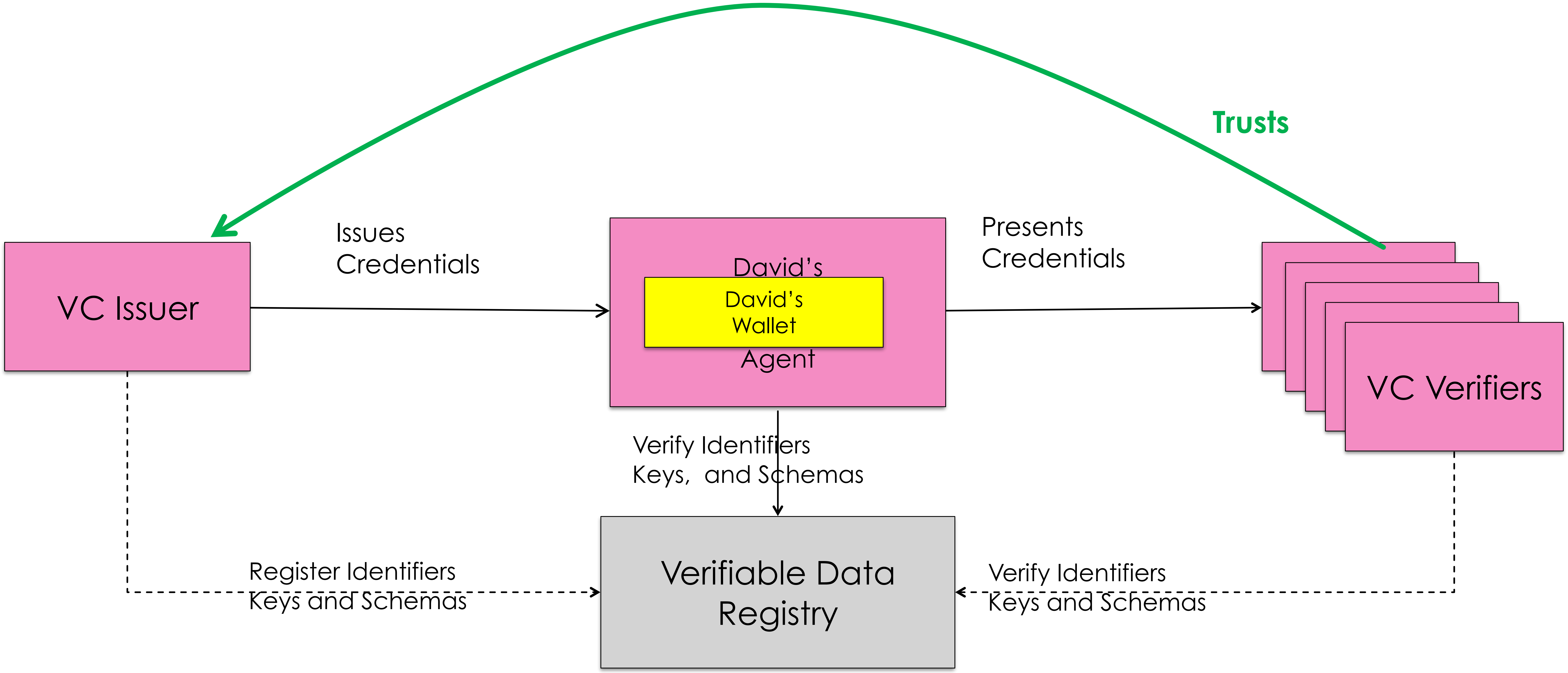
Why do we need DIDs

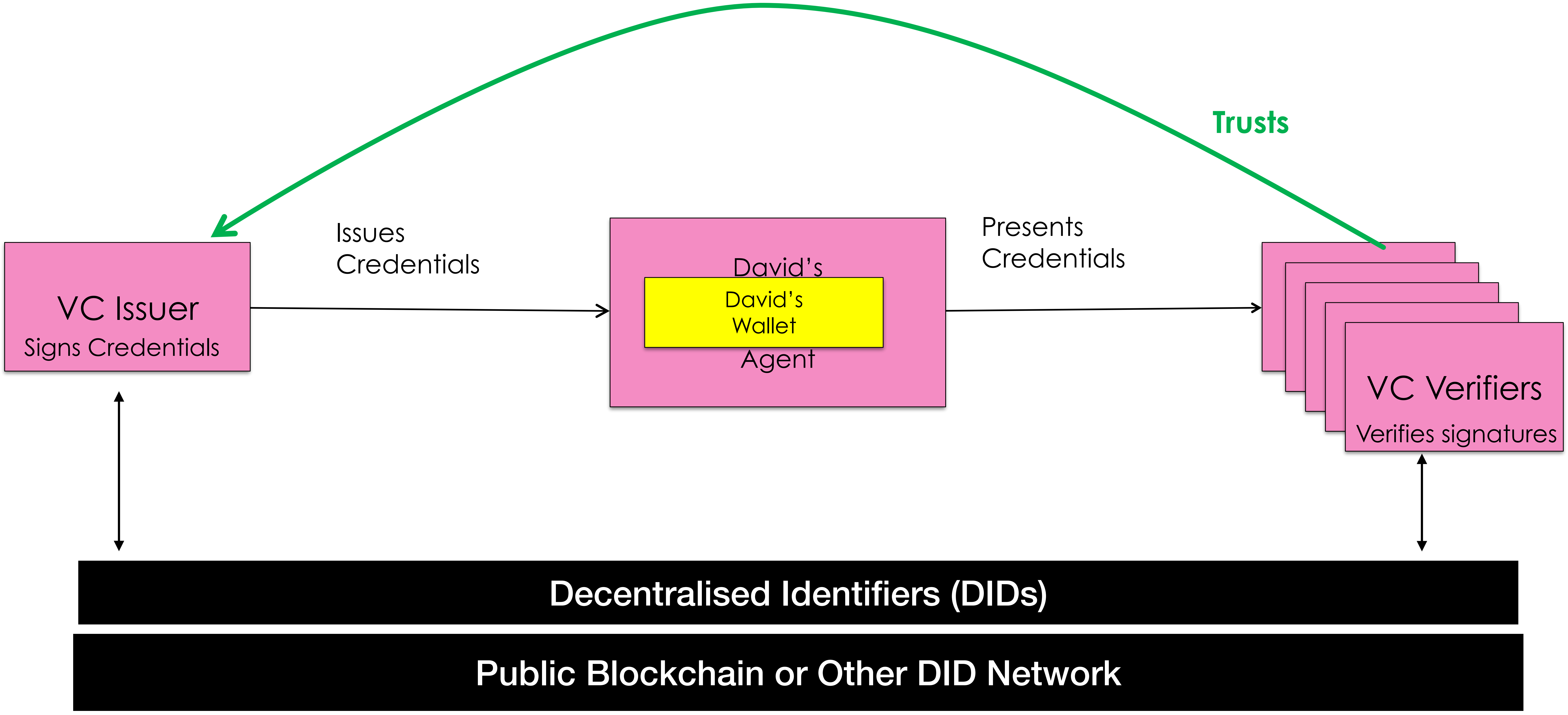
When they are not required for SSI

David Chadwick 9 June 2021

W3C VC Architecture



FAKE W3C VC Architecture



Taken from Self Sovereign Identity, Eds Drummond Reed and Alex Preukshat

Important Points about the VC Data Model

- Blockchains and DIDs are NOT part of the W3C VC Data Model

  DIDs are not necessary for verifiable credentials to be useful. Specifically, verifiable credentials do not depend on DIDs and DIDs do not depend on verifiable credentials.

  W3C Verifiable Credentials Data Model Recommendation, 2019

- This does not stop VC ecosystems from adding DIDs and Blockchains where they are seen to add value

- I believe they currently do not, and only serve to increase the TCO

Decentralised Identifiers (DIDs)

What is the problem?

- The “centralised identifier” problem
- which broadly states that the identifiers held by the Issuers are not yours, but theirs, so you are relying on their identifiers to identify you
- If you stop paying for the service, you lose the identifier
- Everyone should be able to create their own identifiers and be responsible for them
- People should not have to rely on any external authority in order to obtain an identifier

Decentralised Identifiers (DIDs)

The Solution

- DIDs are based on cryptographic keys, but rather than use the Key ID directly
- DIDs provide a level of indirection between a public key and an identifier
- Original idea was each DID would point to a DID document stored on a blockchain
- Everyone would have a DID, comprising
- did:<did method>:<did method specific string>
- Currently approx 100 DID methods are registered

Decentralised Identifiers (DIDs)

What is the problem?

- the “centralised identifier” problem
- which broadly states that the identifiers held by the Issuers are not yours, but theirs, so you are relying on their identifiers to identify you
- Everyone should be able to create their own identifiers and be responsible for them
- People should not have to rely on any external authority in order to obtain an identifier

What is wrong with DIDs?

The problem is wrongly stated

- People in general are not interested in IDENTIFIERS.
- Computers are
- People are interested in IDENTITIES.
- But it is IMPOSSIBLE for two strangers to reliably identify each other
- All IDENTITIES must be issued by trusted third parties using centralised systems
- So we have a solution for a non-existent problem

What is wrong with DIDs

The implementation is wrong

- Initial idea: Everyone should have a DID stored on a blockchain
- BAD IDEA.
- DIDs provide globally unique correlating handles, so destroy people's privacy
- So then implementors decided users' DIDs should not be stored on blockchains, only those of issuers and verifiers (but some still do :-)
- And DIDs no longer need to have associated stored DID documents
- Furthermore blockchains are notoriously resource hungry
- Finally, each DID implementation uses centralised registries anyway (DNS, IdP DBs. etc.)
- So what is the point of DIDs?
- We can simply use public key IDs

What is wrong with DIDs?

For the die hards

- We will allow people to have hundreds of DIDs, with none on the blockchain, so that everyone can have pairwise DIDs with each other, thereby protecting their privacies. Good idea?
- No, bad idea
- You still have no idea who a DID belongs to
- You need to know their identity and for this you need VCs
- If the issuer issues long lived VCs then the user must have hundreds of copies of the same VC, each with a different DID, to stop verifier correlation

Arguments against long lived VCs

- With long lived VCs, either the same DID will be given to multiple Verifiers allowing correlation, or the user must store hundreds of copies of the same VC, each with a different DID
- Implementing Selective Disclosure with long lived VCs requires complex non-standard cryptography (e.g. ZKPs) or hashing schemes
- Requires a privacy protecting revocation system to be implemented
- Why did highly successful SAML and OIDC opt for short-lived non-revocable claims?
- Conclusion. Use short lived non-revocable VCs issued on demand, selectively disclosed to the verifier's GDPR requirements, using standard cryptography

Take Aways

- Biometrics should be considered as part of the VC landscape
  - People should have control over the use of their biometrics
- Protocols for handling VCs should never assume DIDs
- Protocols for handling VCs should contain public keys (directly or indirectly)
- Infrastructure for handling VCs should consider notorisation and external audit