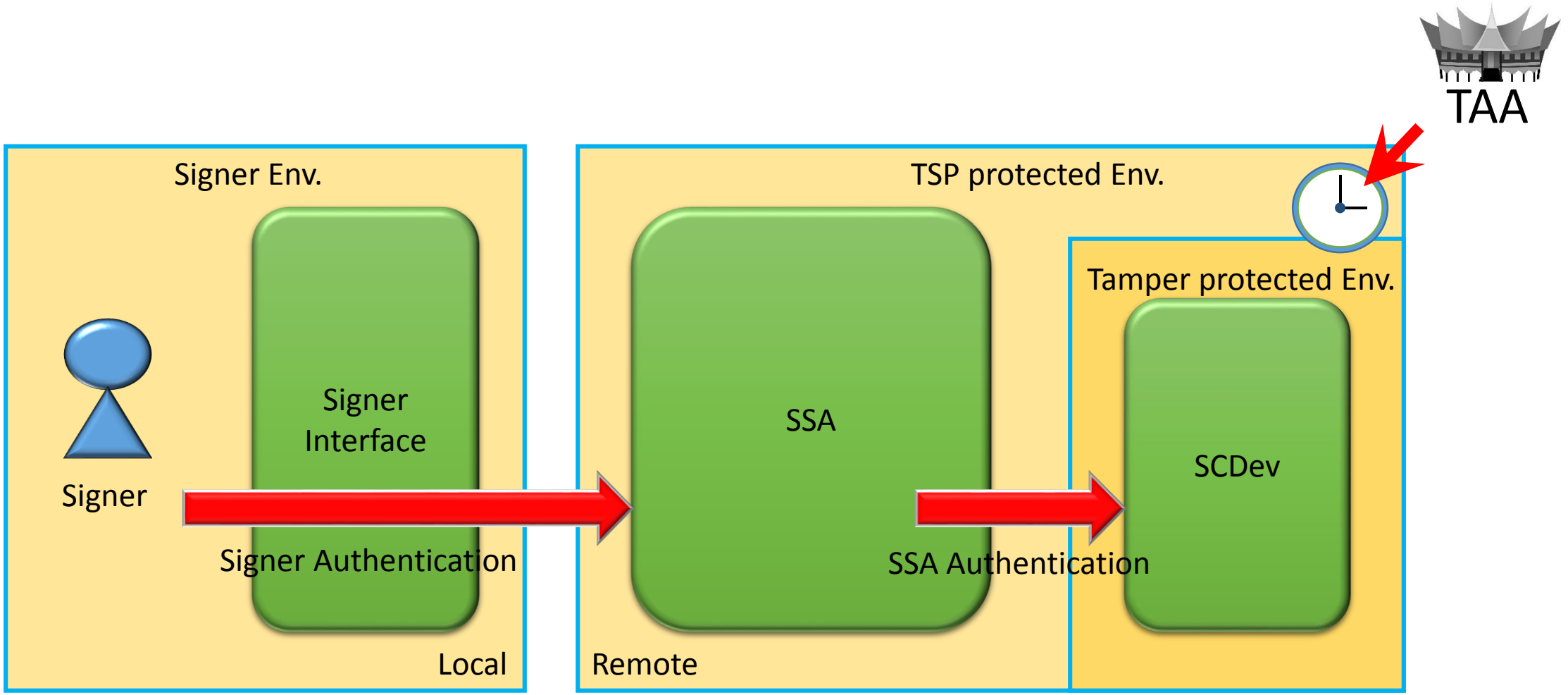
リモート署名とブロックチェーンはタイムスタンプの天敵となるか？

2016年5月22日

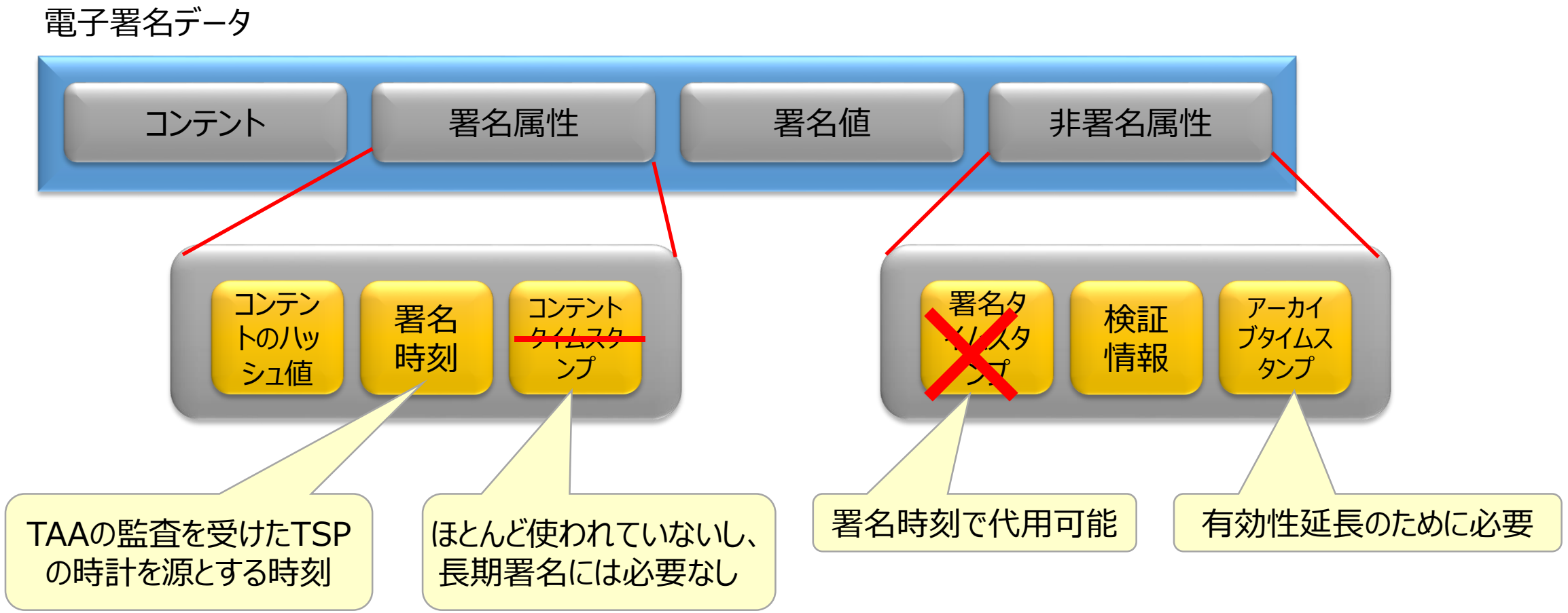
宮崎

第壱章 リモート署名はタイムスタンプを駆逐するか？

リモート署名の時刻のトレーサビリティを確保

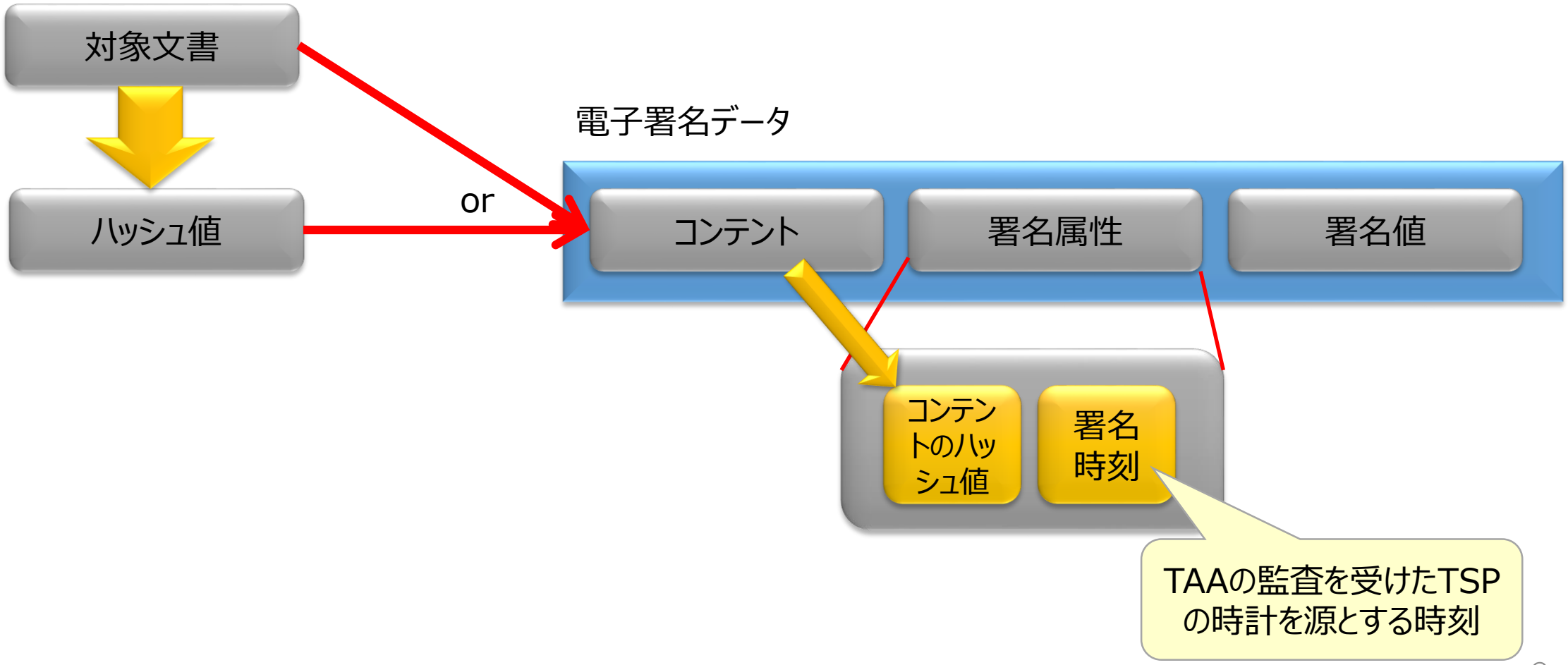


署名時刻(signing time)を信用できる！



署名時刻の証明にタイムスタンプは不要！

署名時刻(signing time)はコンテントの存在時刻も保証する！



リモート署名がタイムスタンプの代用となる！

しか～し

- 署名鍵がSCDev以外に存在しないことの保証をどうする？
  - 「認定」とどう結びつけるか？
- 有効期間は？
  - やはり5年まで
- リモート署名契約
  - そりゃそうだ。
- 署名として利用したときとタイムスタンプとして利用したときとの区別は？
  - 署名目的を明確に定義できないと誤解を招きかねない。

いろいろと制約がありそう。

第弐章 ブロックチェーンはタイムスタンプを駆逐するか？

既に存在！？

- リンキング方式のタイムスタンプ
  - SecureSeal
  - GuardTime
  - Surety.com A
- ブロックチェーンを利用したタイムスタンプ
  - Apostille
  - ほか

『非中央集権的』
じゃないとね

でもこれをブロックチェーンといっちゃうの？

単機能じゃないと

公証って、タイムスタンプとは違ってない？

ビットコインにハッシュ値を紛れ込ませる？

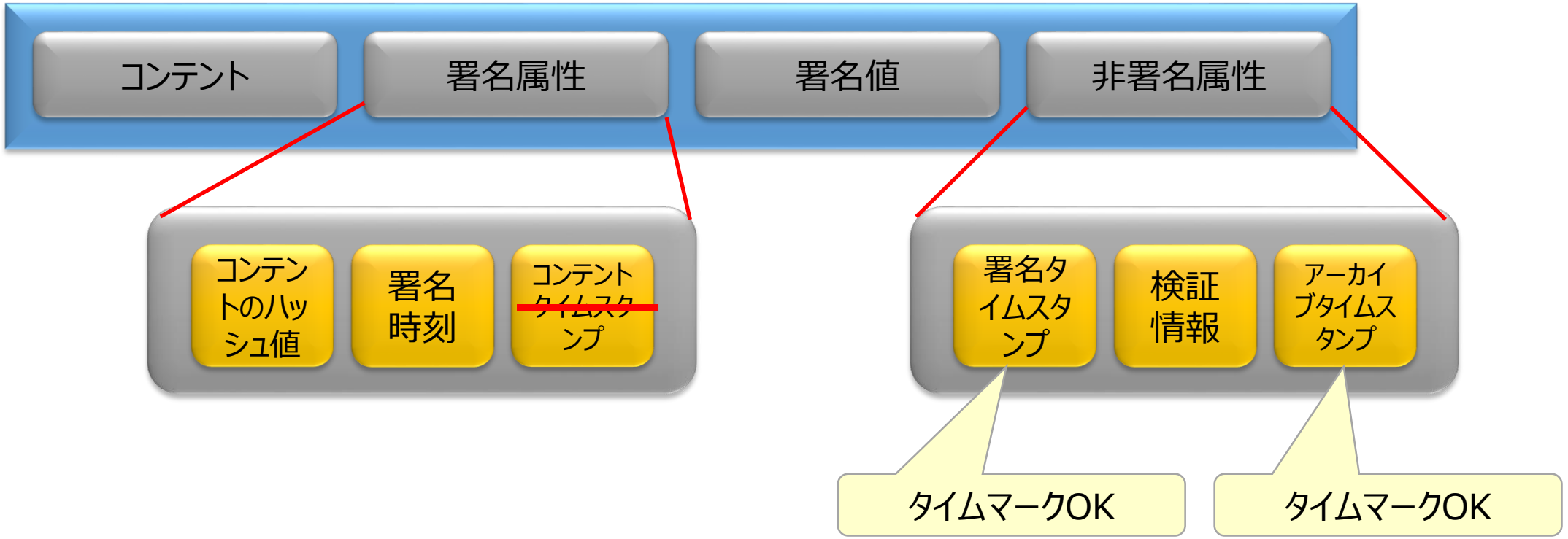
- そのためのサービスもいろいろあるらしい。
  - Proof of Existence
  - OriginStamp
  - Uproove
  - ほか

- 約10分ごとにブロックが追加され、時刻情報がブロックやトランザクションのいろんなところに書き込まれている。

  ⇒ブロック間の順序性は保証できるし、ブロックの時刻情報もある程度信頼できる。~~しかもタダ（安価）！？~~ **ウソ？！**
  ⇒タイムマークとして使える！

タイムマーク

- 長期署名でもタイムスタンプの代わりにタイムマークの利用が認められていた。



タイムマークの標準化

- スロバキアの誰かさんが標準化を進めている

  ISO/WD 14533-4
  Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 4: Part 4: Attributes pointing to external Proof of Existence objects used in Long term signature formats (PoEAttributes)

⇒ビットコインに紛れ込んだハッシュ値をタイムマークとしてポイントできれば長期署名では十分使えそう！

しか～し （PKI day 2107の繰返し）

- 第三者に対するトラストの[illegible]
  - 当事者が信用[illegible]して信頼を与えられるの？
  - 「認定」す[illegible]
- 長期にわたるトラスト[illegible]
  - 暗号アルゴリズムの脆弱化を乗り越えて、何十年もブロックチェーン全体をみんなで共有するの？

ダメかも？
でも用途によっては使えそう

検討は続く…