Protocolos Intermediários

Carimbo de Tempo (timestamping)

- Necessidade de provar a existência de um documento em determinada data.

$A \rightarrow T : M$ (documento)

$T \rightarrow A : t_n$ (carimbo de tempo)

Problemas?
- Privacidade?
- Base de dados?
- Erros de transmisão?
- Confiança no arbitro?

Protocolos Intermediários

Timestamping com assinatura digital

$A : H_n$

$A \rightarrow T : t_n$

$T \rightarrow A : S_{KR_T} (H_n, t_n)$

Problemas?
- Produção de carimbo quando desejado

Protocolos Intermediários

Linking Protocol

$A \rightarrow T : H_n,\ A$

$T \rightarrow A : S_{KR_T}\ (\ n,\ A,\ H_n,\ t_n,\ I_{n-1},\ H_{n-1},\ t_{n-1},\ L_n\ )$

onde: $L_n = H\ (\ I_{n-1},\ H_{n-1},\ t_{n-1},\ L_{n-1}\ )$

após próximo carimbo

$T \rightarrow A : I_{n+1}$

Problemas?

- Documento fictício

Protocolos Intermediários

Protocolo distribuído

$A : V_1, V_2, V_3, \ldots V_k$

onde: V_i = produzidos por geradores pseudo-randômicos seguros

$A \rightarrow P_1 : H_n\ (\ V_1\ )$

$A \rightarrow P_2 : H_n\ (\ V_2\ )$

.....

$A \rightarrow P_k : H_n\ (\ V_k\ )$

$P_i \rightarrow A\ : S_{KR_P}\ (\ H_n,\ t_n\ )$

A : armazena

Protocolos Intermediários

Assinatura em grupo

(1) Somente membros do grupo podem assinar,

(2) Quem recebe pode verificar que a assinatura é válida e pertence ao grupo,

(3) Quem recebe não consegue identificar qual membro do grupo assinou,

(4) No caso de disputa, ou após um período estabelecido, a assinatura pode ser “aberta” para revelar a identidade de quem assinou,

Protocolos Intermediários

Assinatura em grupo

(1) Arbitro gera um conjunto de KUKR´s e entrega a cada membro do grupo uma lista de KUKR´s única.
Total de KUKR´s = n * m (n membros, m par de chaves cada membro)

(2) Arbitro publica a conjunto de KU´s em ordem aleatória.

(3) Quando um membro deseja assinar um documento, escolhe uma chave aleatoriamente de sua lista pessoal.

(4) Quando alguém deseja verificar a qual grupo pertence a assinatura, busca no conjunto a KU´s e verifica a assinatura.

(5) No caso de disputa, arbitro sabe a quem pertece a KU.