Scalable "Smart Contracts" via Proofs and Single-Use-Seals

Peter Todd

Jan 27th 2017

37EC 7D7B 0A21 7CDB 4B4E 007E 7FAB 1142 67E4 FA04
Chances are nothing in this talk is original, just forgotten in blockchain mania.
$n$ nodes with $k$ transactions $\implies O(n^2)$ total work
Let’s Buy a House With Blockchain!

Peter Todd

BPASE’17
The Goal - Accurate UI/UX
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

I hereby transfer ownership of the property 136 E Palm Cir, Placentia CA, to Alice, 17D7 54B6 CD63 B41D E511 D504 4E41 1E33 8CCE 1BF3.

Signed,
Bob

-----BEGIN PGP SIGNATURE-----
iQEeBAEBCAAGBQi3WLAAoJECSBQD2l8JH7o2kH/ix7jUm0Mtke5PgJviKtUA17fheRLRsRC8Xhk/QBgyYUhV23H/kLrJZMmQtqDL5rCFa+1SRtH79B7G0B3ox0ZmU=
=+Ptj
-----END PGP SIGNATURE-----
Title Transfer Protocol

\[ T_0 = \text{Genesis Title} \tag{1} \]
\[ T_i = (\text{Owner}, T_{i-1}) \tag{2} \]
\[ W_0 = \bot \tag{3} \]
\[ W_i = (\text{Sig}, W_{i-1}) \tag{4} \]
\[ \text{TitleVerify}(T_i, W_i) := T_i \in G \parallel (\text{CheckSig}_{T_{i-1}}(W_{i\text{Sig}}, T_i) \land \text{TitleVerify}(T_{i-1}, W_{i-1})) \tag{5, 6, 7} \]
I hereby transfer ownership of the property 136 E Palm Cir, Placentia CA, to Adam, C921 7238 4F38 7DBA ED4D 4201 65EB 9636 F02C 5704.

Signed,
Bob

-----BEGIN PGP SIGNATURE-----

iQEcBAEBCAAGBQJYi3d5AAoJECSBQD2l8JH7QTgH/1liqZK8J7B7LkMv5ih8qq3A+AWotEGqwRiblEVFhLb17z2A1qohtbEF9Wkb/s4FLQLOLjTdJ4p12H7TYEw05rk=
=CmlW

-----END PGP SIGNATURE-----
Physical Single-Use-Seals
Secure if $\not\exists (w_1, w_2)$ such that $\text{SealVerify}(s, w_1, m_1) = \text{True}$ and $\text{SealVerify}(s, w_2, m_2) = \text{True}$
Single-Use-Seal - Useful Definition

\[
\text{SeallInit}(\text{Conditions}) \rightarrow s \quad (11)
\]
\[
\text{SealClose}(\text{Auth}, s, m) \rightarrow w \quad (12)
\]
\[
\text{SealVerify}(s, w, m) \rightarrow \text{Bool} \quad (13)
\]
SealInit($m$) := $H(m) \rightarrow s$ \hfill (14)
SealVerify($s$, $w$, $m$) := $H(m) === s$ \hfill (15)
SealInit() := Random($\mathbb{Z}^{256}$) $\rightarrow$ $s$ \hspace{1cm} (16)

SealVerify($s$, $w$, $m$) := $H(w + m)$ $==$ $s$ \hspace{1cm} (17)
“Genie, I wish to know $w$ such that $H(w + m) == s$.”
SealInit() := Random($\mathbb{Z}^{256}$) $\rightarrow$ s \hspace{1cm} (18)

SealClose(s, m) := Sign$_P$(s + m) $\rightarrow$ w \hspace{1cm} (19)

SealVerify(s, w, m) := CheckSig$_P$(w, s + m) \hspace{1cm} (20)

Secure if SealClose() can only be called once.
SealInit() := Create transaction output $\rightarrow s$ \hspace{1cm} (21)
SealClose(s, m) := Spend output and commit to $m \rightarrow w$ \hspace{1cm} (22)
SealVerify(s, w, m) := Verify commit tx in blockchain \hspace{1cm} (23)
Teechan Press Release:
5. Consequently, Teechan lends itself to an efficient implementation. Our prototype achieves a throughput of 2,480 transactions per second per channel, with settlement latency overheads of 0.4 ms.

Teechan Paper:
We have built and deployed the Teechan framework using Intel SGX on the Bitcoin network. Our experiments show that Teechan can achieve 2,480 transactions per second on a single channel, with sub-millisecond latency.
Every one of these CPUs can be selling a different house:
Do Proofs and Single-Use-Seals Scale?

$O(n)$?
Thank you!