Contribution of Singapore National Body to SC17 WG11

Use of blockchain in cards and biometrics

* *for WG11 study period work* *

(2020-12-15)

by Mr. LIN Yih

Chairman, Identification Technology Technical Committee

iTSC

Information Technology Standards Committee

Background

- WG11 has a study period on the use of blockchain technology in the area of biometrics as applied to cards (the scope of WG11)
- Our interest in this area also aligns with the broader interest of applying blockchain to IoT devices in Singapore
- Given SG national body is also planning a PlugFest event for BSoC (biometric system on card), we decided to develop a proof-of-concept (PoC) software to combine the two works
- The software that we developed will process biometric matching scores into a blockchain – to illustrate ideas

iTSC
Information Technology
Standards Committee

Our sample blockchain . . overview

- Each record in our sample blockchain comprises 5 fields:
  counter | previous_hash | data | nonce | current_hash
  A sample section is given below:

BC_20201203_120102_046.log - Notepad

File Edit Format View Help

counter | previous_hash | data | nonce | current_hash

```
000000000|F120BB5698D520C5691B6D603A00BFD662D13BF177A04571F9D10C0745DFA2A5|BEGIN=20201215_093310_351|0002CB06|8E709296C0702F2C74ADE3E01739AF46A2BADF5C5DF2EB35449ABBADC5C00000
000000001|8E709296C0702F2C74ADE3E01739AF46A2BADF5C5DF2EB35449ABBADC5C00000|20201203_120102_265,Finger001v01_Finger001v01.txt,98|00165FE1|3AFBBE28DFF4F999407D880FE625F8BF74BDF11E5AABC10701923E60CAE00000
000000002|3AFBBE28DFF4F999407D880FE625F8BF74BDF11E5AABC10701923E60CAE00000|20201203_120102_375,Finger001v01_Finger001v02.txt,98|00183804|1D0713C9DDC13CB03A9B8030AE36E08D29657C6E25F2F1782CA2FBFC1AB00000
000000003|1D0713C9DDC13CB03A9B8030AE36E08D29657C6E25F2F1782CA2FBFC1AB00000|20201203_120102_500,Finger001v01_Finger001v03.txt,98|0011AC75|81FB3A7B70515B8F7F065F49ADF1B53E6F9572132142C2D78CDE537321800000
000000004|81FB3A7B70515B8F7F065F49ADF1B53E6F9572132142C2D78CDE537321800000|20201203_120102_593,Finger001v01_Finger001v04.txt,98|0006809B|4BBA30AA87550D766CD06E95932D86E08E30D8CE5A64A9EFBF81AF7A8A100000
000000005|4BBA30AA87550D766CD06E95932D86E08E30D8CE5A64A9EFBF81AF7A8A100000|20201203_120102_687,Finger001v01_Finger001v05.txt,98|00015291|16C0D773A8809F8FCA79E8B78D32C2AC557897FD08B60C93F516DE1040000000
000000006|16C0D773A8809F8FCA79E8B78D32C2AC557897FD08B60C93F516DE1040000000|20201203_120102_812,Finger001v01_Finger001v06.txt,98|0011F866|D0095D851B1D77300B181C6E331D243B236C6060329CDEEE9ED771E1B8700000
000000007|D0095D851B1D77300B181C6E331D243B236C6060329CDEEE9ED771E1B8700000|20201203_120102_921,Finger001v01_Finger001v07.txt,98|000C9896|9EEBF3032176476C7926910595EAE101246C6572C4C4971A47D661D09BE00000
000000008|9EEBF3032176476C7926910595EAE101246C6572C4C4971A47D661D09BE00000|20201203_120103_062,Finger001v01_Finger001v08.txt,98|0007C626|866B52BD95194DCF71635C29EB0D18F57A7B1B3C7135FFDB52FC4B8BF5900000
000000009|866B52BD95194DCF71635C29EB0D18F57A7B1B3C7135FFDB52FC4B8BF5900000|20201203_120103_140,Finger001v01_Finger001v09.txt,98|0024CA44|4D0971CD56B433A966F1F1196E054A7EC226DEA2C97A435C0BFE2C031AA00000
000000010|4D0971CD56B433A966F1F1196E054A7EC226DEA2C97A435C0BFE2C031AA00000|20201203_120103_218,Finger001v01_Finger001v10.txt,98|00160430|A8B1067DED9843E321D82A221FC656D245119353B960045F7B0B4B3C0FF00000
000000011|A8B1067DED9843E321D82A221FC656D245119353B960045F7B0B4B3C0FF00000|20201203_120103_328,Finger001v01_Finger002v01.txt,28|0003B836|5F7AFE1EBAFC191029A12E10385E62153AC415878A4510A1BEB9779708D00000
000000012|5F7AFE1EBAFC191029A12E10385E62153AC415878A4510A1BEB9779708D00000|20201203_120103_453,Finger001v01_Finger002v02.txt,0|0016E542|512845784479E18F813857A5FE447A12EAAF9FAC1B1CB8BA0BDBCAA510200000
000000013|512845784479E18F813857A5FE447A12EAAF9FAC1B1CB8BA0BDBCAA510200000|20201203_120103_593,Finger001v01_Finger002v03.txt,42|000D6940|C833B9C915A9EFC27A548F006384AFB805B385864FC0793A09A82652F2100000
000000014|C833B9C915A9EFC27A548F006384AFB805B385864FC0793A09A82652F2100000|20201203_120103_718,Finger001v01_Finger002v04.txt,14|001BF785|B93CDAF449FDA2E8448714EBD34C4579C6E594CF9541341C008DFBEC55100000
000000015|B93CDAF449FDA2E8448714EBD34C4579C6E594CF9541341C008DFBEC55100000|20201203_120103_843,Finger001v01_Finger002v05.txt,14|000E9536|89E36E11446C5A8CF062E5D67838A5EA51A123DCE9169FC5EF0FD22C98400000
000000016|89E36E11446C5A8CF062E5D67838A5EA51A123DCE9169FC5EF0FD22C98400000|20201203_120103_953,Finger001v01_Finger002v06.txt,14|0019F665|CAEBE6359819600F22581B048F190F3BC5B537B49E55FC6B8AD5FB15E3400000
000000017|CAEBE6359819600F22581B048F190F3BC5B537B49E55FC6B8AD5FB15E3400000|20201203_120104_078,Finger001v01_Finger002v07.txt,0|001820F4|9F37EAD40C382CA9BFE9EA530C1A3BB82F091489D122DE99DE5D3D3756600000
000000018|9F37EAD40C382CA9BFE9EA530C1A3BB82F091489D122DE99DE5D3D3756600000|20201203_120104_203,Finger001v01_Finger002v08.txt,0|0015D417|E53BEDF285B1990CBAE1200687935B3B390F80C901D7AFEA6F4CB37D8DE00000
000000019|E53BEDF285B1990CBAE1200687935B3B390F80C901D7AFEA6F4CB37D8DE00000|20201203_120104_328,Finger001v01_Finger002v09.txt,14|001A4599|7FFAF592373D31DCFBEF5E86F80A41C55EF7B4D868F88F632F0B65502A800000
000000020|7FFAF592373D31DCFBEF5E86F80A41C55EF7B4D868F88F632F0B65502A800000|20201203_120104_453,Finger001v01_Finger002v10.txt,14|0005D68F|386F959C5F0AE6BEEC6CB62F8C9341FC6B5AE2C907062617C361D8A9B8E00000
000000021|386F959C5F0AE6BEEC6CB62F8C9341FC6B5AE2C907062617C361D8A9B8E00000|20201203_120104_578,Finger001v01_Finger003v01.txt,0|000FFAFC|3365D2151E1D39C5887ADBFA149B475769BDF952276747728BA2A8628D000000
000000022|3365D2151E1D39C5887ADBFA149B475769BDF952276747728BA2A8628D000000|20201203_120104_703,Finger001v01_Finger003v02.txt,0|00288BA7|6F7BD630E1152A66442236E2340EC81E1149731E0343151080539FE0ABB00000
000000023|6F7BD630E1152A66442236E2340EC81E1149731E0343151080539FE0ABB00000|20201203_120104_828,Finger001v01_Finger003v03.txt,0|000410E6|21DD38A6C30F5D2EFCBFD88B492019AC70533D9784441B0E9B20303E7E800000
000000024|21DD38A6C30F5D2EFCBFD88B492019AC70533D9784441B0E9B20303E7E800000|20201203_120104_937,Finger001v01_Finger003v04.txt,0|002C0EFC|69CEA311EC3782A1234FFA411EC8760FD45F95DBD5E0054334C346F56BC00000
000000025|69CEA311EC3782A1234FFA411EC8760FD45F95DBD5E0054334C346F56BC00000|20201203_120105_078,Finger001v01_Finger003v05.txt,0|00189EBB|9D67F5A5D95AEA9C7C8041EDD06A80D124E8D07B93C6D9F1585FADF340300000
000000026|9D67F5A5D95AEA9C7C8041EDD06A80D124E8D07B93C6D9F1585FADF340300000|20201203_120105_203,Finger001v01_Finger003v06.txt,0|000726F6|4DC41D86C54DCD1FA8C078EADFAA931192644B67F1DC45DD4FCBDDEE5DF00000
000000027|4DC41D86C54DCD1FA8C078EADFAA931192644B67F1DC45DD4FCBDDEE5DF00000|20201203_120105_328,Finger001v01_Finger003v07.txt,0|0011EAEA|C12F09AB2C817CCDEDB07273B57742664AC2CF0D116A884DE6D2FA5693400000
000000028|C12F09AB2C817CCDEDB07273B57742664AC2CF0D116A884DE6D2FA5693400000|20201203_120105_453,Finger001v01_Finger003v08.txt,0|00096074|A1F1C5FE98BE35720061228E23E07EFAE5DA1758F83C56F72015BC1A7DC00000
000000029|A1F1C5FE98BE35720061228E23E07EFAE5DA1758F83C56F72015BC1A7DC00000|20201203_120105_578,Finger001v01_Finger003v09.txt,14|00486EBE|EAF7C11FB07E6C06A7D2186DC67B706A8DB7455467460CE34573ACA577600000
000000030|EAF7C11FB07E6C06A7D2186DC67B706A8DB7455467460CE34573ACA577600000|20201203_120105_718,Finger001v01_Finger003v10.txt,0|000A0F83|4D9C84A8E9F854E8AB254A8C4DA77527DE1FFFB6FAF95F2AAB364C4086200000
000000031|4D9C84A8E9F854E8AB254A8C4DA77527DE1FFFB6FAF95F2AAB364C4086200000|20201203_120105_828,Finger001v01_Finger004v01.txt,0|001364C1|F7C93A4FD9BFB39455578EBBE03857EA204967A6067C78577691E172D8E00000
000000032|F7C93A4FD9BFB39455578EBBE03857EA204967A6067C78577691E172D8E00000|20201203_120105_953,Finger001v01_Finger004v02.txt,0|000130D3|39E94E32B95A696596F25F8C7EA360D43C65F01D7C8153E4A4F3400A9FE00000
000000033|39E94E32B95A696596F25F8C7EA360D43C65F01D7C8153E4A4F3400A9FE00000|20201203_120106_093,Finger001v01_Finger004v03.txt,0|002DB1DC|14E23C148ACB171EFE721529F06B2AE03848034B1625BFF984C1F6CBF4900000
000000034|14E23C148ACB171EFE721529F06B2AE03848034B1625BFF984C1F6CBF4900000|20201203_120106_203,Finger001v01_Finger004v04.txt,0|0005AD2F|B0E5D254EAA13FFFAEC6A8B2583FBC6908DEB869271E8F864999C8C0E8F00000
000000035|B0E5D254EAA13FFFAEC6A8B2583FBC6908DEB869271E8F864999C8C0E8F00000|20201203_120106_328,Finger001v01_Finger004v05.txt,0|00059F85|F92E0DFA96CC16E1B789C3BFEA047F1093F7EBE558927736FF0868C4F9400000
000000036|F92E0DFA96CC16E1B789C3BFEA047F1093F7EBE558927736FF0868C4F9400000|20201203_120106_453,Finger001v01_Finger004v06.txt,0|00039F87|46F453FF5A773768701 4D3A359CF4CFBD77642F7B8D67729FF5FBD8A6B100000
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Our sample blockchain . . counter

- The counter is displayed in decimal, range 0..999,999,999
- It is incremented for each data line, and the first data line has the number 1, while number 0 is reserved for the first record of the blockchain
- We call the first record (or block) the "BEGIN" record (instead of "genesis" block that is used in other literature)
- For our sample application, we added a "END" record after all the data lines – this is something other literature does not introduce

Our sample blockchain . . hash

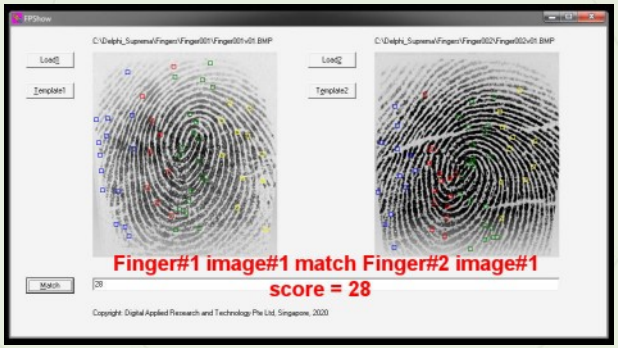
- Our hash value is the 32-byte result of SHA-256, expressed in hexadecimal
- In the "classical" or "standard" (?) manner, previous_hash is the current_hash value of the previous record
- Note that the previous_hash of record number 1 is the current_hash of record number 0 "BEGIN"
- The current_hash is the value of computing SHA-256 on **counter | previous_hash | data | nonce**
- For our example, all values are printable characters (decimal, hexadecimal, alphanumeric) and the separator '|' is not included in the SHA-256 calculation

iTSC
Information Technology
Standards Committee

Our sample blockchain . . data

- Each line of our data is the resultant score of matching one fingerprint data with another – same or different finger
- The source of these cross-matching scores is taken from a .LOG file that is produced by a cross-matching software intended for BSoC PlugFest
- In our example, the length of our data line is variable, because the matching score can be 1 to 3 digits (e.g. 0, 28, 98 or 100)
- Some examples:

  20201203_120103_218,Finger001v01_Finger001v10.txt,98
  20201203_120103_328,Finger001v01_Finger002v01.txt,28
  20201203_120103_453,Finger001v01_Finger002v02.txt,0



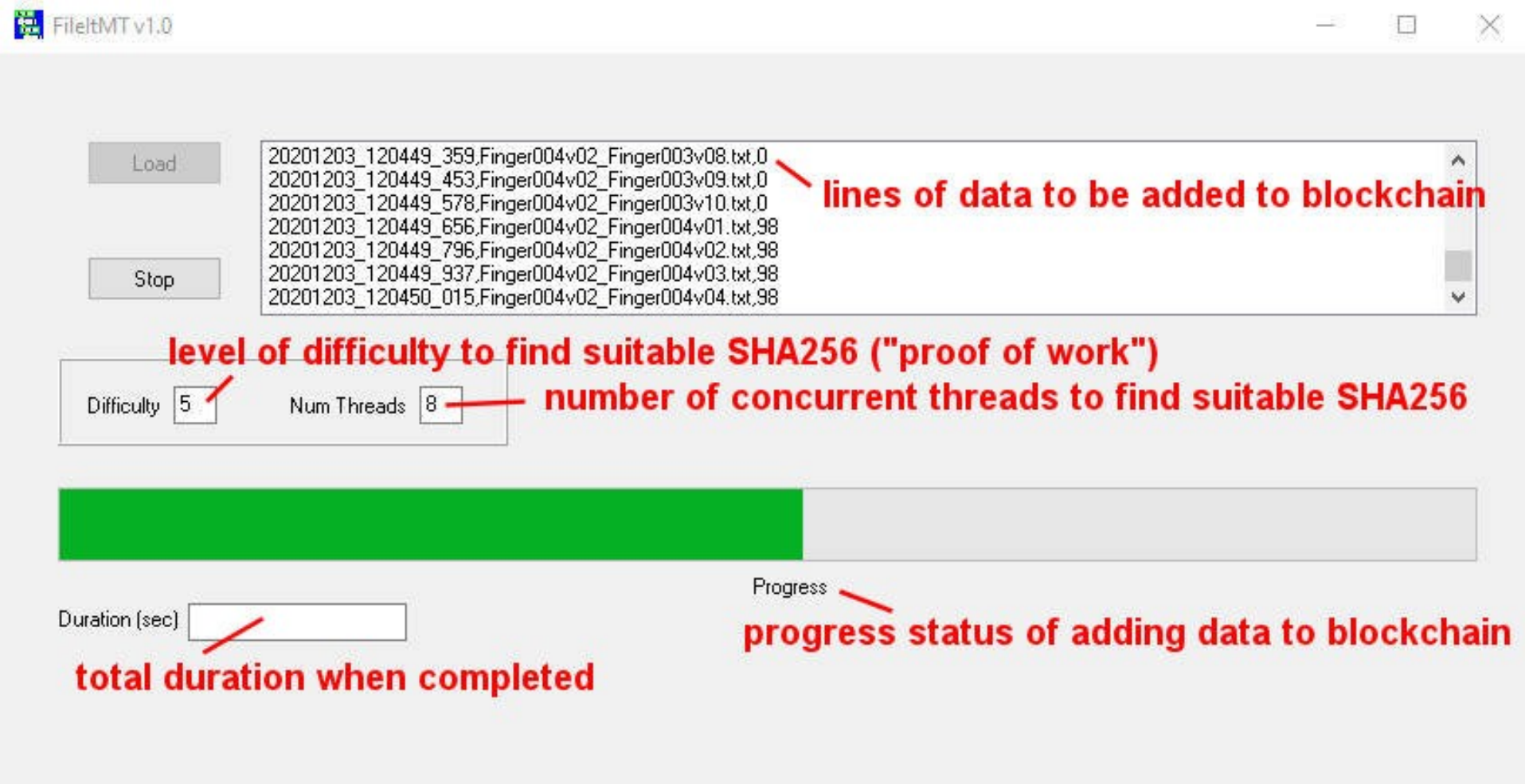
iTSC
Information Technology
Standards Committee

Our sample blockchain . . nonce

- Our nonce is a 4-byte hexadecimal value that is added so that the SHA-256 result can satisfy a "difficulty" requirement
- In our example, "difficulty" specifies the number of trailing zeros in the SHA-256 result
- For example, "difficulty=5" means 5 trailing hexadecimal zeros

Our sample blockchain . . FileITMT

- A screen snapshot of our blockchain software is attached



Our sample blockchain . . FileITMT

- The software starts by "loading" a .LOG file from a BSoC PlugFest session
- For each data line it reads in, it will package it into a format suitable for blockchain – adding a counter, previous_hash, nonce, current_hash
- The resultant output data line is inserted into another .LOG file
- There is an option to set the "difficulty" level and the number of processing threads to search for the suitable nonce that satisfies the "difficulty" requirement

iTSC
Information Technology
Standards Committee

Blockchain technology

Discussion

&

Analysis

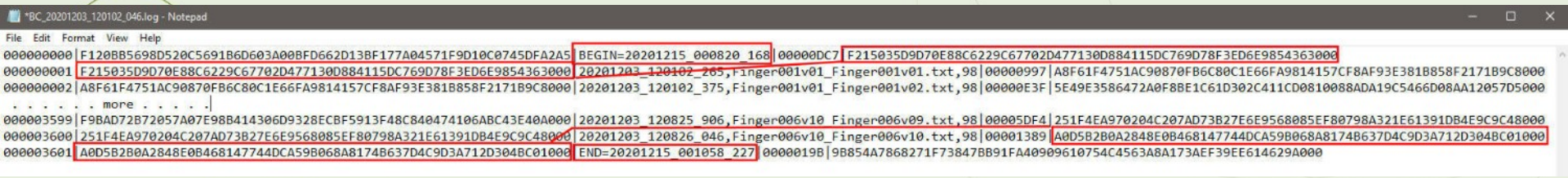
iTSC
Information Technology
Standards Committee

Blockchain technology

- Q: what is the idea behind blockchain?
- A: the main idea or the smallest data record (block) is the following:

  previous_hash | data | current_hash

- What this structure ensures, is that a change to any of the data entails a propagation of change to all the hash values that follows
- We intentionally introduced a "END" record to protect the last data record



Blockchain technology

- Q: what is the big deal with propagating hash calculation?
- A: nothing, calculating hash is very fast nowadays, unless you add a "difficulty", "nonce" requirement

- Q: so is there any use for single, simple blockchain?
- A: No (disappointment !!!) but distributing multiple copies of the same blockchain can be used for "verification using majority voting"

- Note: a large collection of blocks is also known as a "ledger" in other literature

iTSC
Information Technology
Standards Committee

Blockchain technology

- Q: how is introducing "difficulty", "slowness", "proof of work" useful?
- A: It adds time and computing cost to anyone who wants to alter the data. Any data that is received substantially late is suspected of having been altered

- Example: each record requires 5 minutes. If I prepare a set of blockchain and broadcast to N recipients, they should receive the set within "reasonably fast network speed" and anything after 5 minutes should be suspicious and subjected to further checks (e.g. by majority voting)

iTSC
Information Technology
Standards Committee

Blockchain technology

- Q: how does "majority voting" work?
- A: there are various understanding or implementation of the idea, however the main idea to ask a few other servers, or agents to verify some data that you have and reach your own conclusion by consensus or majority principle

- Note: other than "majority" voting, you can also have "trustable" servers or agents that you rely upon. A combination of "majority" and "trustable" is always possible

iTSC
Information Technology
Standards Committee

Blockchain technology

- Q: Any other usefulness of "BEGIN" and "END" blocks?
- A: If you have a blockchain and you wish to ask N servers or agents whether that blockchain is intact, the "BEGIN" and "END" blocks are sufficient for identification. This requires that the servers or agents kept complete copies of the blockchain ("BEGIN".. data .. "END"). This idea can be refined further for each project implementation

iTSC
Information Technology
Standards Committee

Blockchain technology

- Q: Does blockchain replace PKI or encryption?
- A: absolutely not! Blockchain, PKI, encryption, digital signature can be combined and used together, depending on what is the requirement and problem to solve
- Note: a strict, "text book" implementation of PKI requires constant "CRL" (certificate revocation list) checks. This ***maybe*** costly for some implementations and blockchain ***maybe*** a better option

iTSC
Information Technology
Standards Committee

Blockchain technology

- Q: Must data in blockchain be printable characters?
- A: absolutely not! The entire block can be binary or even BER-TLV !!!

iTSC
Information Technology
Standards Committee

Blockchain technology – what's next?

- Q: Can blockchain be used in reader terminals and networks?
- Q: Any other possible application areas within SC17 and SC17 WG11?
- Q: In our implementation, nonce is not propagated forward (i.e. there is previous_hash, but no prev_nonce). Is this correct?

iTSC
Information Technology Standards Committee

THE END

Thank you

Q&A

Further suggestions

iTSC
Information Technology
Standards Committee