



Flash Memory Summit

# Blockchain Technology in SSD Controllers



**Global Guide Consulting**

[xiaguigen@gmail.com](mailto:xiaguigen@gmail.com)

“Flash in IoT security”  
Hiroshi Watanabe

[hwhpnabe@gmail.com](mailto:hwhpnabe@gmail.com)



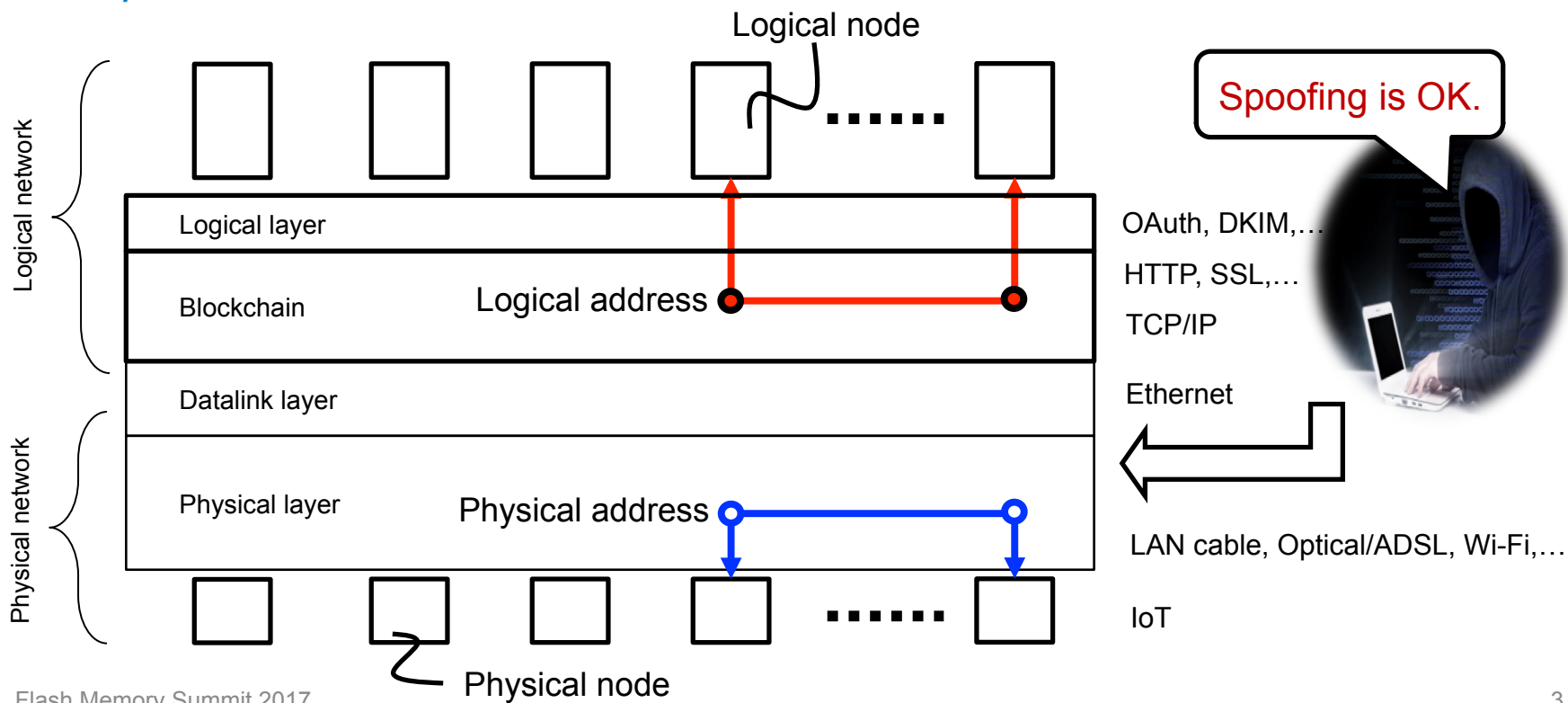
**IMSolution**

[www.imsolution.com.tw](http://www.imsolution.com.tw)





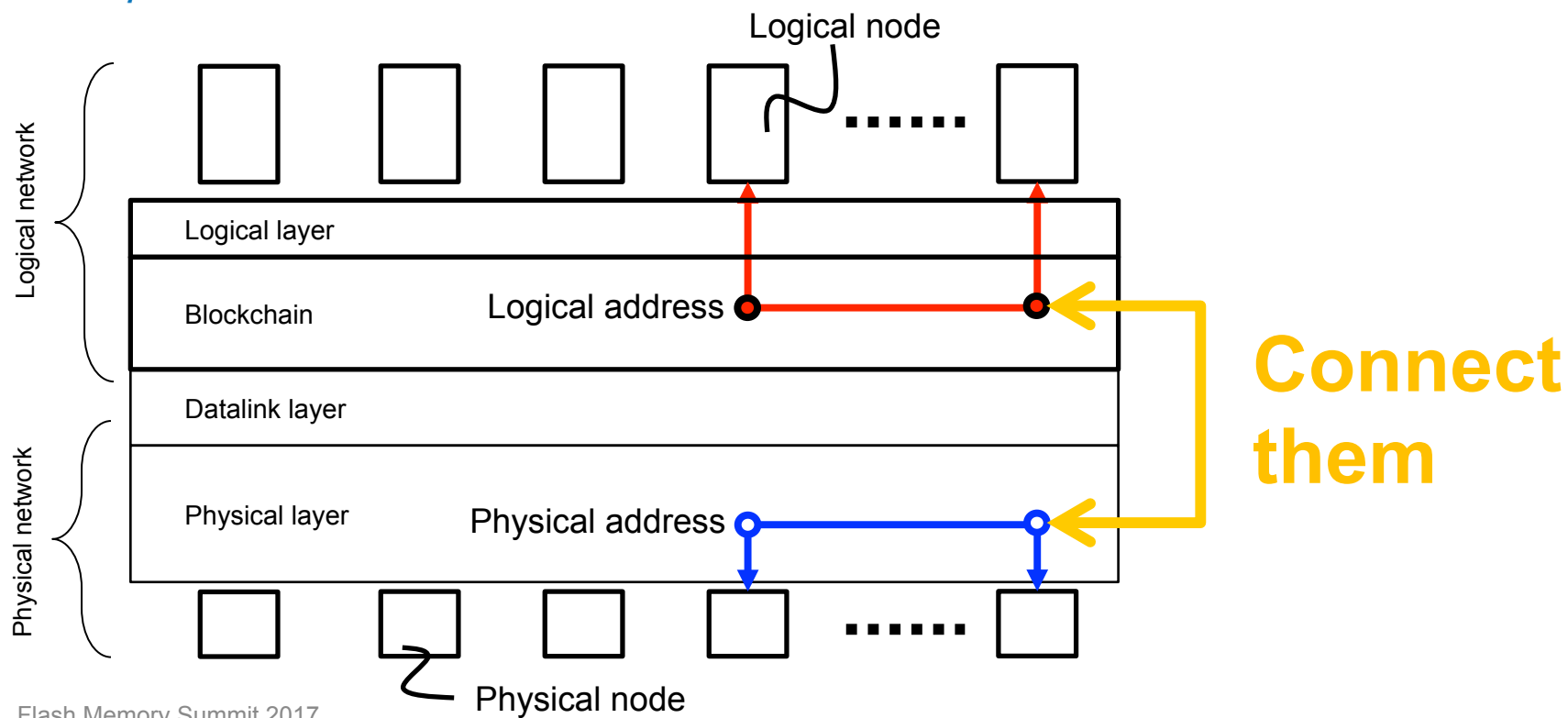
# Existing Blockchain cannot protect IoT.





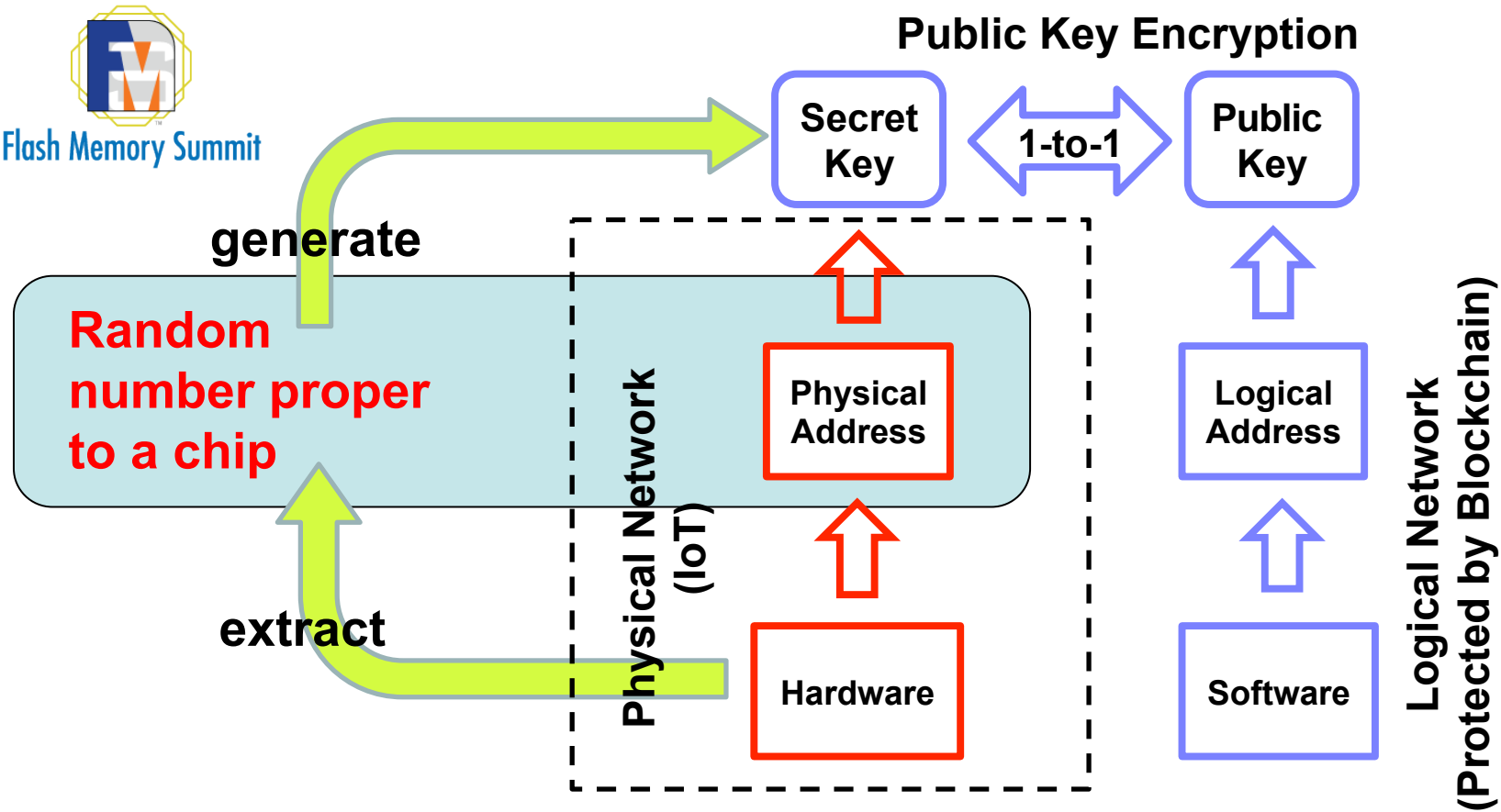
Flash Memory Summit

# Approve Blockchain to protect IoT.





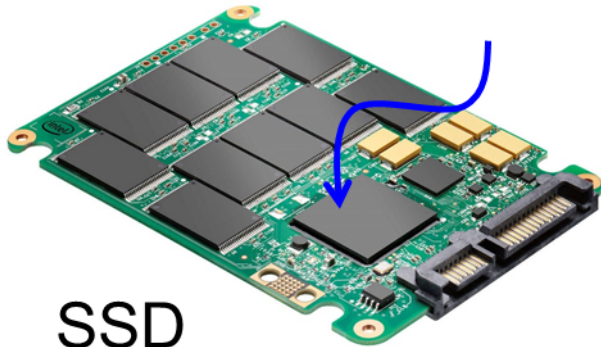
Flash Memory Summit



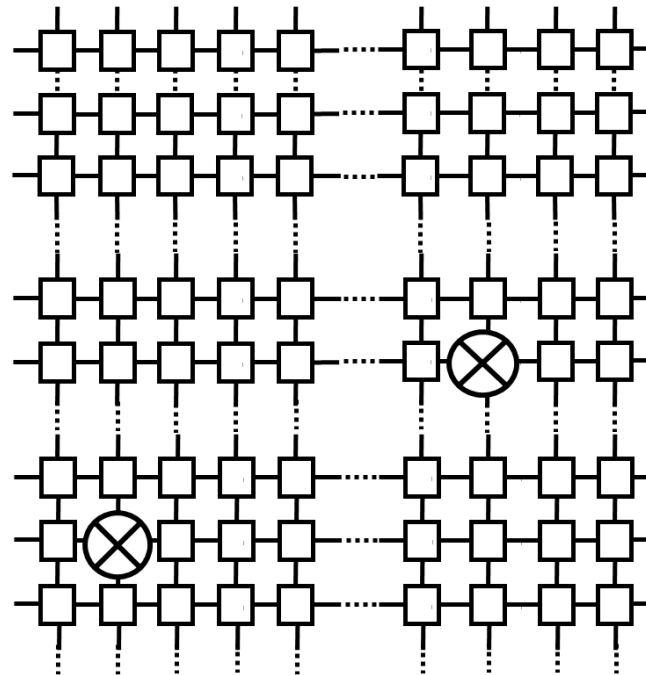


Flash Memory Summit

**Random  
number proper  
to a chip**



SSD

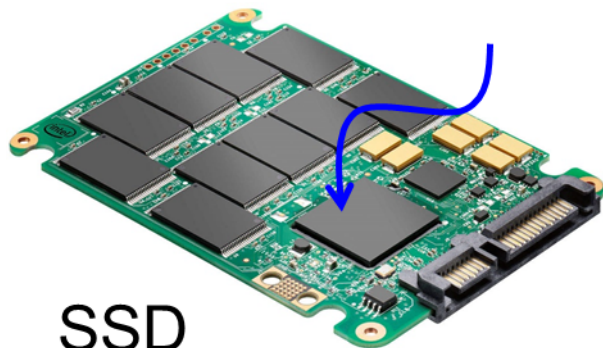


Fail bits  
distribution is  
physically  
random,  
which is  
specific to a  
chip.



Flash Memory Summit

Random number proper to a chip



SSD

## Physical address of a chip

```

00000000100000000010000000001000000011000000000100
0111011000000000001001001011100000000010101010011000
0000001010111100000000000011100111011000000000111101
11111000000000100011001110000000001101010101010000000
1011110011000000000010111110011110000000101111110000
000000011010011000110000000110100110101000000001101
011110100000000011011111001110000000110000000010000
0000111011111101011000000100100000
10010000000000100100111000000
1010011000000000000010110100101
1100000000001001100110100000011
0011100010001100000011010101001011
0000001101011001000000000000111101
00000011010000000010000000001000
000000100000001100000000100011101100000000010010
0101110000000010101001100000000101011110000000
00001110011101100000000011110111111000000001000110011
10000000001101010101010000000101111001100000000010
111110011110000000101111110000000000110100110001100
0000011010011010100000000110101111010000000001101111
100111000000011100000000100000000111010010001000000
010001111101011000000100100000100100000001001011010
001100000010010110100111000000101001100000100000001
01101000000000000010110100101110000000110010010010
0100000011001101001101000000110011100011010000001101
000000001100000011010101001011000000110101100100010
000001101100100000000000111101000000110000001111010
11011010.....

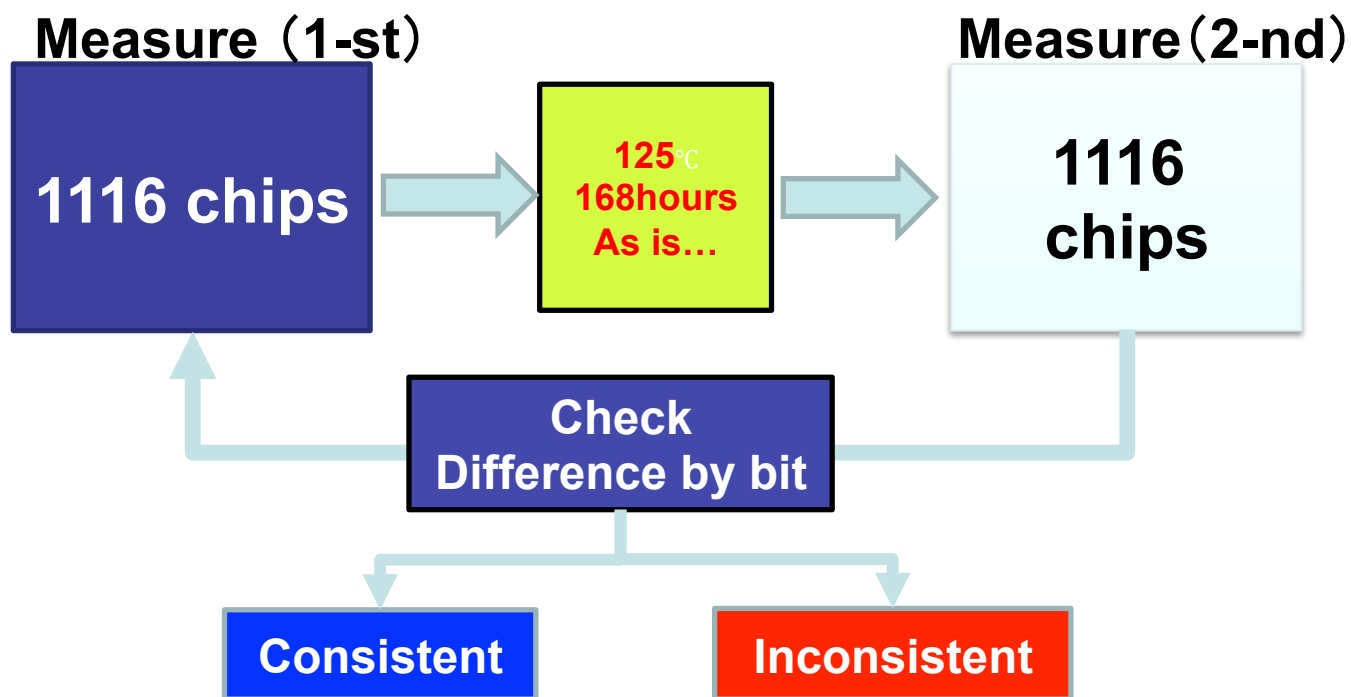
```

125°C  
168hours  
performed

Generated from fail bits distribution, which is specific to a chip and physically random with No FEP change



# Heating Acceleration Test







# Physical address of chip-No. 11/1116

## Before Bake

```

00000000100000000010000000010000000011000000001000111011000000
000010010010111000000000101010100110000000001010111000000000000
11100111011000000000111101111100000000100011001110000000001101010
101010000000101111001100000000001011111001111000000010111111100000
0000001101001100011000000011010011010100000000110101110100000000
01101111100111000000011100000000100000000111010010001000000010001
111101011000000100100000100100000010010110100011000000100101101
001110000001010011000001000000010110100000000000001011010010111
0000000110010010010010000001100110100110100000011001110001101000
0001101000000001100000011010101001011000000110101100100010000001
1011001000000000000111101000000110000001111010110110100000000100
000000010000000001000000001100000000010001110110000000001001001
011100000000010101010011000000000101011100000000000011001110110
000000001111011111000000001000110011100000000011010110101000000
0101111001100000000001011111001111000000010111111000000000011010
0110001100000000110100110101000000001101011101000000001101111100
1110000000111000000001000000001110100100010001000111110101100
00001001000001001000000010010110100010000010010010110100111000000
10100110000010000000101101000000000000101101001011100000001100
10010010010000001100110100110100000011001100110000110100000011010000
000011000000110101010010110000001010110010001000000110110010000
0000000011110100000011000000111101011011010

```

....

## After Bake

```

00000000100000000010000000010000000011000000001000111011000000
000010010010111000000000101010100110000000001010111000000000000
11100111011001000000111101111100000000100011001110000000001101010
1010100000010111100111100110000000001011111001111000000010111111100000
0000001101001100011000000011010011010100000000110101110100000000
0110111100111000000011100000000100000000111010010001000000010001
11101011000000100100000100100000010010110100011000000100101101
001110000001010011000001000000010110100000000000001011010010111
0000000110010010010010000001100110100110100000011001110001101000
0001101000000001100000011010101001011000000110101100100010000001
10110010000000000001111010000001100000011110101101101000000000100
0000000100000000010000000011000000000100011101100000000001001001
0111000000000101010100110000000001010111000000000000111001110110
0000000011110111110000000010001100111000000000110101010101000000
0101111001100000000001011111001111000000010111111000000000011010
0110001100000000110100110101000000001101011101000000001101111100
1110000000111000000001000000001110100100010001000111110101100
00001001000001001000000010010110100010000010010010110100111000000
10100110000010000000101101000000000000101101001011100000001100
10010010010000001100110100110100000011001100110000110100000011010000
000011000000110101010010110000001010110010001000000110110010000
0000000011110100000011000000111101011011010

```

....

All bits are consistent



# Physical address of chip-No. 606/1116

## Before Bake

```

00000000100011100000000010000000000000000101000001000000
000111001011010000000011111100111000000100010010101000000010010
0100100100000001001011011001000000010011000000100000001001101001
1000000000100110110000000000101001110111000000001100100011011000
000011001111100110000000111000010100100000001110101001001000000100
100111000000000010010101111011000000101010001101000000010101100
11110000000010101111001010000001010111100101100000010111000010000
0000001011100001110000000010111000011101000000101111101111000000
1101000000001000000011010000010010000000110101000000000000011011
111010101000000110111110111000000011100000010110000000111000111110
01000000111001000100000000001110100111010100000011101111000100000
00111011111001100000001111000000001000000111101001101000000000000
10000111000000000010000000000000000010100000010000000000111001
0110100000000111111001110000001000100101010000000101001001001
00000001001011011001000000100110000001000000010110100110000000
0010011011100000000001010011101110000000110011001100000001100
1111100110000000111000010100100000001110110110100000010010011100
000000000100101011110110000001010100011010000001010110011110000
00001010111100101000000101011110010100000101110000100000000001
0111000011100000001011100001110100001011111011111000000011010000
00001000000011010000010010000000111010100000000000001101111101010
1000000110111101110000000111000000101100000001110001111100100000
01110010001000000000011101001110101000000111011111000100000011101
1111001100000001111000000001000000111101001101000...

```

## After Bake

```

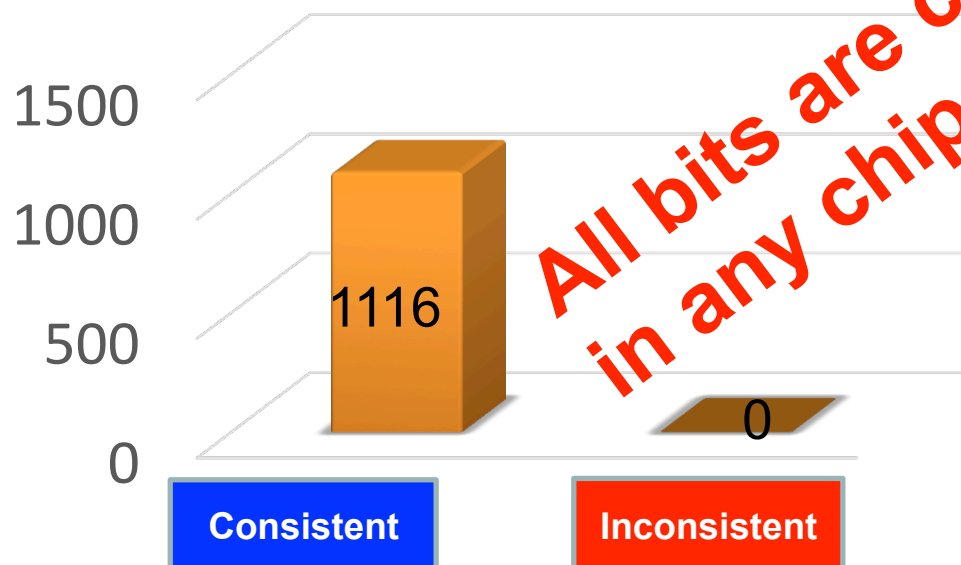
00000000100011100000000010000000000000000101000001000000
000011100101101000000011111100111000000100010010101000000010010
1001001001000001001011011001000000100110000001000000010011010
0110000001001101110000000000101001110111000000001100100011011
0000000100111110011000000011100001010010000000111010100100100000
01011001100000000001001010111101100000010101000110100000001010
000111000000001010111100101000000101011110010110000001011100001
0000000001011100001110000000010111000011101000000101111011111000
000011010000000100000011010000010010000001101010000000000000
110111110101010000011011111011100000001110000001011000000111000
111110010000001110010001000000000111010011010100000011011111000
10000000111011111001100000001111000000001000000111101001101000000
0000001000011100000000001000000000000000001010000001000000000
01110010110100000000111111001110000001000100101010000000100100
100100100000010010110110010000001001100000010000000010011010011
000000000100110111000000000010100111011100000001100100011011000
00001100111110011000000011100001010010000000111010100100100000010
01001110000000000010010101111011000000101010001101000000001010110
01111000000001010111100101000000101011110010110000001011100001000
0000000101110000111000000001011000011101000000101111011111000000
011010000000010000000110100000100100000001101010000000000001101
11110101010000001101111011100000001110000001011000000011100011111
00100000011100100010000000001110100111010100000011101111100010000
000111011111001100000001111000000001000000111101001101000...

```

All bits are consistent

## Measurement Result

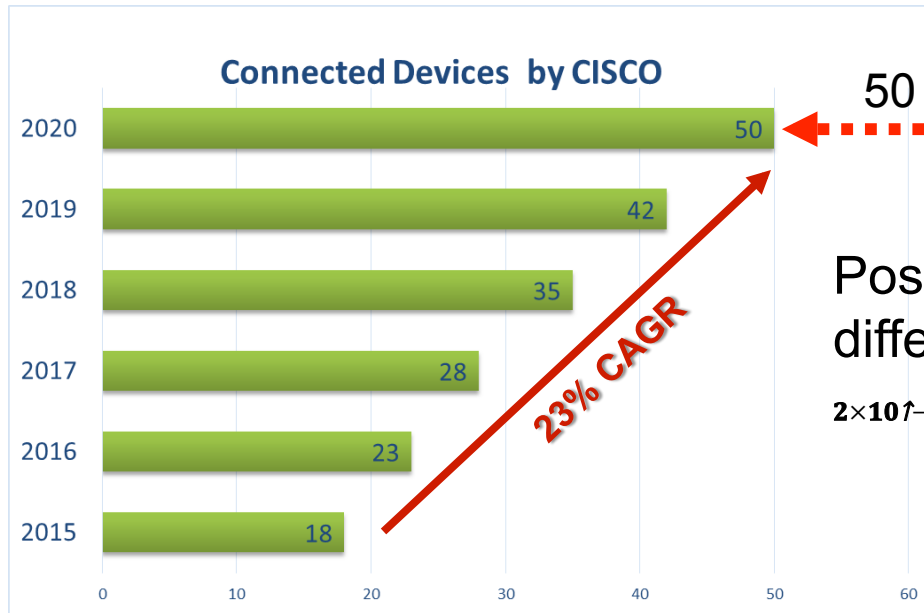
The number of Chips





# Mass-product feasibility

Suppose 1-Gb cash with 1-kb fail bits.  
(Less than 6-sigma.)



50 B chips will be necessary in 2020.

Possibility that physical addresses of two different chips are accidentally identical is

$$2 \times 10^{17} - 6,422 .$$



Flash Memory Summit

## Conclusion

- Physical address = Physical randomness of chip
- Cheapest, Reliable, Ease to stable shipment in large quantity
- Physical addresses are respectively connected to logical addresses, which are protected by blockchain, with the secure controller for SSDs.



Global Guide Consulting



IMSolution

[www.imsolution.com.tw](http://www.imsolution.com.tw)