



COMPLEX
CYBER
INFRASTRUCTURE

smart contracts

principles and beyond

Blockchain and the Law. April 2021, seminar UCP

Giovanni Sileno, University of Amsterdam. g.sileno@uva.nl

smart contract

- term introduced by Nick szabo in the 1996

Smart Contracts: Building Blocks for Digital Markets

Copyright (c) 1996 by Nick Szabo
permission to redistribute without alteration hereby granted

Glossary

(This is a partial rewrite of the article which appeared in Extropy #16)

Introduction

The contract, a set of promises agreed to in a "meeting of the minds", is the traditional way to formalize a relationship. While contracts are primarily used in business relationships (the focus of this article), they can also involve personal relationships such as marriages. Contracts are also important in politics, not only because of "social contract" theories but also because contract enforcement has traditionally been considered a basic function of capitalist governments.

Whether enforced by a government, or otherwise, the contract is the basic building block of a free market economy. Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Algorithmic information theory suggests that such evolved structures are often prohibitively costly to recompute. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like property rights that make the modern free market work [Hayek].

smart contract

- term introduced by Nick szabo in the 1996
- ...well before the introduction of blockchain (2008)

Smart Contracts: Building Blocks for Digital Markets

Copyright (c) 1996 by Nick Szabo
permission to redistribute without alteration hereby granted

Glossary

(This is a partial rewrite of the article which appeared in Extropy #16)

Introduction

The contract, a set of promises agreed to in a "meeting of the minds", is the traditional way to formalize a relationship. While contracts are primarily used in business relationships (the focus of this article), they can also involve personal relationships such as marriages. Contracts are also important in politics, not only because of "social contract" theories but also because contract enforcement has traditionally been considered a basic function of capitalist governments.

Whether enforced by a government, or otherwise, the contract is the basic building block of a free market economy. Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Algorithmic information theory suggests that such evolved structures are often prohibitively costly to recompute. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like property rights that make the modern free market work [Hayek].

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

"smart contract"

A set of promises,

including protocols within which the parties perform on the other promises.

The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics,

thus these contracts are "smarter" than their paper-based ancestors.

No use of artificial intelligence is implied.

"smart contract"

a bilateral contract is a formal agreement in which both parties exchange promises to perform



A set of promises,

including protocols within which the parties perform on the other promises.

The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics,

thus these contracts are "smarter" than their paper-based ancestors.

No use of artificial intelligence is implied.

"smart contract"

A set of promises,

rules, procedures constraining the interaction

*including **protocols within which the parties perform** on the other promises.*

The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics,

thus these contracts are "smarter" than their paper-based ancestors.

No use of artificial intelligence is implied.

"smart contract"

A set of promises,

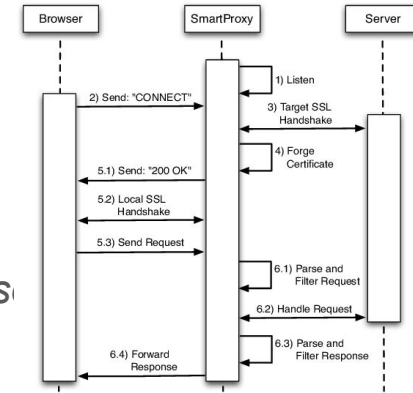
rules, procedures constraining the interaction

including protocols within which the parties perform on the other promises

The **protocols** are usually **implemented with programs** on a computer network, or in other forms of digital electronics,

thus these contracts are "smarter" than their paper-based ancestors.

No use of artificial intelligence is implied.



"smart contract"

A set of promises,

including protocols within which the parties perform on the other promises.

The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics,

*thus these contracts are "**smarter**" than their paper-based ancestors.*

???

No use of artificial intelligence is implied.

"smart contract"

A set of promises,

including protocols within which the parties perform on the other promises.

The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics,

thus these contracts are "smarter" than their paper-based ancestors.

No use of artificial intelligence is implied.

then, smart in what sense?

- According to the vulgata:
 - as the contract will perform exactly as designed
 - it eliminates the need for “trust” amongst the parties
 - ...and traditional third-parties (lawyers, notaries, courts) whose activity is meant to increase the confidence in the contract



then, smart in what sense?

- According to the vulgata:
 - as the contract will perform exactly as designed
 - it eliminates the need for “trust” amongst the parties
 - ...and traditional third-parties (lawyers, notaries, courts) whose activity is meant to increase the confidence in the contract
- smart perhaps is in the sense of *economically profitable*?

\$\$\$

then, smart in what sense?

crucial critical point to all this enterprise!!!

- According to the vulgata:
 - as **the contract will perform exactly as designed** 
 - it eliminates the need for “trust” amongst the parties
 - ...and traditional third-parties (lawyers, notaries, courts) whose activity is meant to increase the confidence in the contract
- smart perhaps is in the sense of *economically profitable?*

then, smart in what sense?

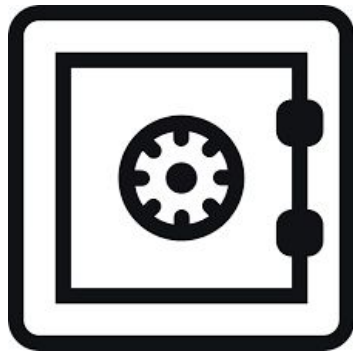
crucial critical point to all this enterprise!!!

- According to the vulgata:
 - as **the contract will perform exactly as designed**
 - it eliminates the need for “trust” amongst the parties
 - ...and traditional third-parties (lawyers, notaries, courts) whose activity is meant to increase the confidence in the contract
- smart perhaps is in the sense of *economically profitable?*

how? making breaches **prohibitively expensive**

\$\$\$

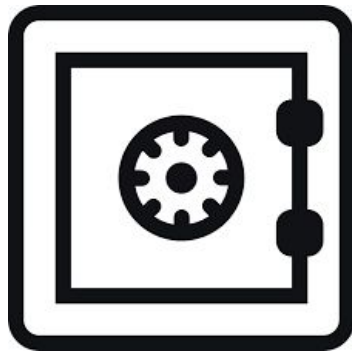
essential idea: technology as a vault



the *possibility* of breaching is
prohibitively expensive

ex-ante enforcement

essential idea: technology as a vault



the *possibility* of breaching is
prohibitively expensive

ex-ante enforcement

- What to protect?
 - (valuable?) digital assets
 - “contracts” (reified as assets)
 - automated performance

tokens!

in terms of medieval technology

- How to protect (the content of) a book from invasions, wars, and plagues?



in terms of medieval technology

- How to protect (the content of) a book from invasions, wars, and plagues?
- Copy it, and distribute the copies through a network of monasteries!



in terms of medieval technology

- How to protect (the content of) a book from invasions, wars, and plagues?
- Copy it, and distribute the copies through a network of monasteries!



If a node is destroyed, a copy is still maintained in all others!!!



in terms of medieval technology

- Typically copying bring errors, exemplars of the book are never identical



in terms of medieval technology

- Typically copying bring errors, exemplars of the book are never identical

technological improvement:

introduce **error checking** machinery, typically via additional content used to **check integrity**



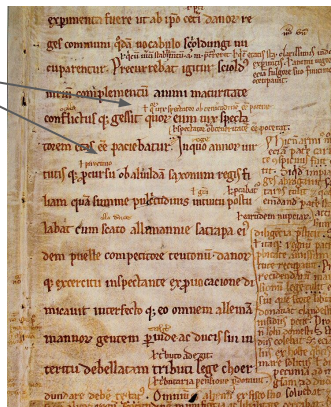
in terms of medieval technology

- Typically copying bring errors, exemplars of the book are never identical

technological improvement:

introduce **error checking** machinery, typically via additional content used to **check integrity**

e.g. glosses
rephrasing
the meaning
of some word



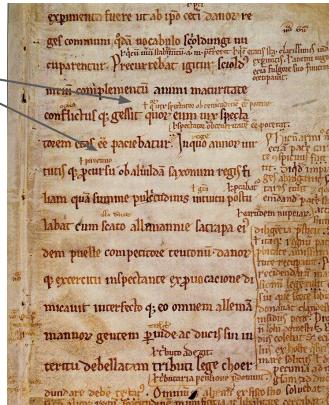
in terms of medieval technology

- Typically copying bring errors, exemplars of the book are never identical

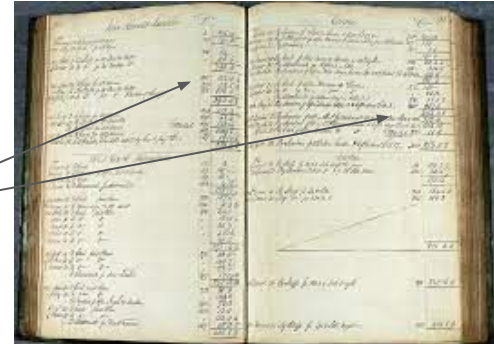
technological improvement:

introduce **error checking** machinery, typically via additional content used to **check integrity**

e.g. glosses
rephrasing
the meaning
of some word



double entry
bookkeeping
(Florence,
Venice ~1300)



in terms of medieval technology

- Typically copying bring errors, exemplars of the book are never identical



- Introduce **conflict resolution strategies**
 - philology provides several methods to “reconstruct” the original source, e.g. majority of sources, comparative analysis, provenance history



in terms of medieval technology

- Typically copying bring errors, exemplars of the book are never identical



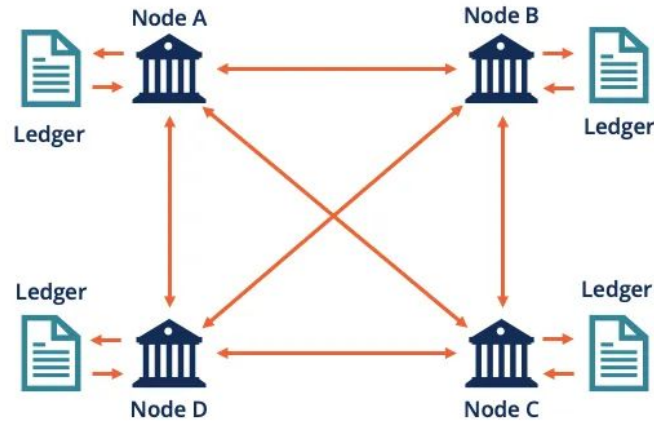
“consensus” protocol

- Introduce **conflict resolution strategies**
 - philology provides several methods to “reconstruct” the original source, e.g. *majority of sources*, comparative analysis, provenance history

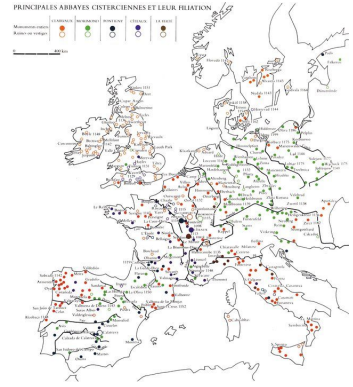


"blockchain" =

- **distributed** ledger + consensus protocol

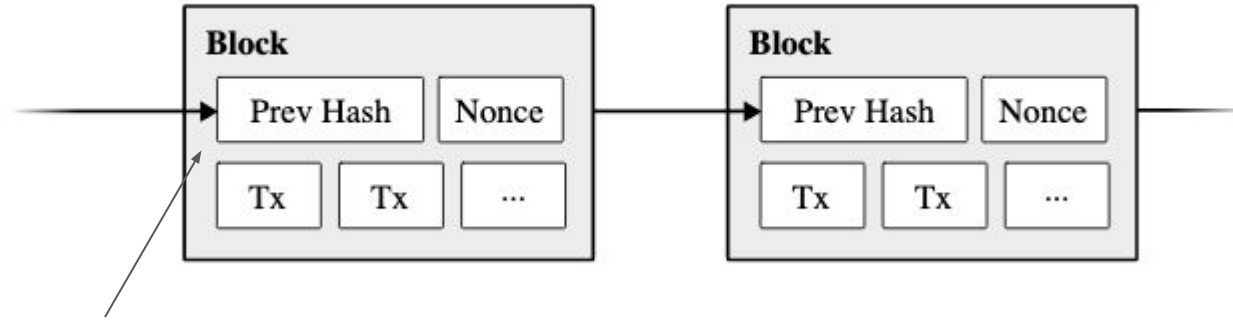
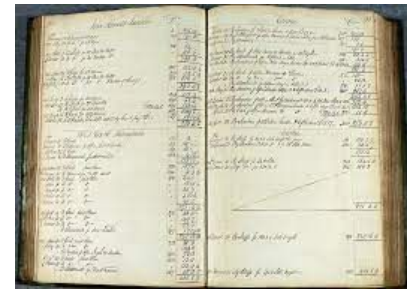


the same ledger is
copied across the
network



"blockchain" =

- distributed **ledger** + consensus protocol

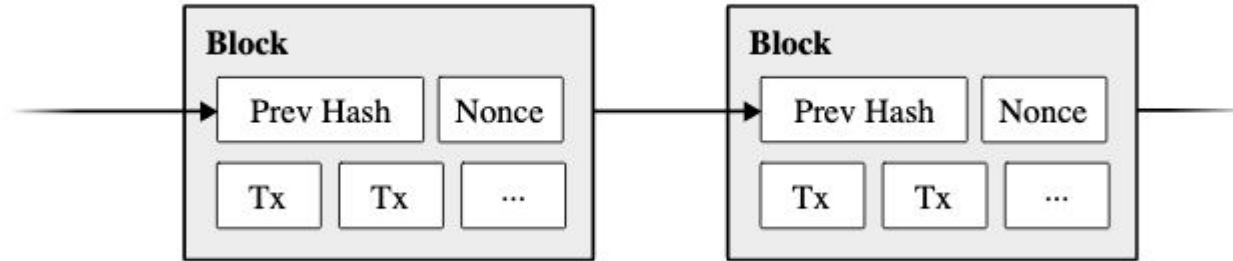


the ledger embeds
machinery to test its
integrity

compressed information (a sort of *fingerprint*) of the previous block,
if the previous block is modified its hash is not the same

"blockchain" =

- distributed ledger + consensus protocol



checks for integrity are performed across the network, no central authority

techniques: **Proof of Work (PoW)**, **Proof of Stake (PoS)**, etc.

`"smart contract"`

`= code running on blockchain`

`"smart contract"`

`= code running on blockchain`

which code?

in most cases Ethereum

“smart contract”

= code running on blockchain

which code?

in most cases Ethereum

source code

```
pragma solidity >=0.4.22 <0.6.0;

contract Ballot {
    struct Voter {
        uint weight;
        bool voted;
        address delegate;
        uint vote;
    }

    struct Proposal {
        bytes32 name;
        uint voteCount;
    }

    address public chairperson;

    [...]
```

“human-readable” instructions

[developer's view]

"smart contract"

= code running on blockchain

which code?

in most cases Ethereum

source code

```
pragma solidity >=0.4.22 <0.6.0;

contract Ballot {
    struct Voter {
        uint weight;
        bool voted;
        address delegate;
        uint vote;
    }

    struct Proposal {
        bytes32 name;
        uint voteCount;
    }

    address public chairperson;

    [...]
```

compilation



byte-code or machine code

```
1 60606040526004361061006d576000357
2 000000: PUSH1 0x60
3 000002: PUSH1 0x40
4 000004: MSTORE
5 000005: PUSH1 0x04
6 000007: CALLDATASIZE
7 000008: LT
8 000009: PUSH2 0x006d
9 000012: JUMPI
10 000013: PUSH1 0x00
11 000015: CALLDATALOAD
12 000016: PUSH29 0x0100000000000000
13 000046: SWAP1
14 000047: DIV
15 000048: PUSH4 0xffffffff
16 000053: AND
17 000054: DUP1
18 000055: PUSH4 0x362186ed
19 000060: EQ
20 000061: PUSH2 0x008d
21 000064: JUMPI
22 000065: DUP1
23 000066: PUSH4 0x30052624
```

"human-readable" instructions
[developer's view]

low-level instructions
[user's view]

"smart contract"

= code running on blockchain

which code?

in most cases Ethereum

libraries
in byte-code



source code

```
pragma solidity >=0.4.22 <0.6.0;  
  
contract Ballot {  
    struct Voter {  
        uint weight;  
        bool voted;  
        address delegate;  
        uint vote;  
    }  
  
    struct Proposal {  
        bytes32 name;  
        uint voteCount;  
    }  
  
    address public chairperson;  
  
    [...]
```

compilation



byte-code or machine code

```
1 60606040526004361061006d576000357  
2 000000: PUSH1 0x60  
3 000002: PUSH1 0x40  
4 000004: MSTORE  
5 000005: PUSH1 0x04  
6 000007: CALLDATASIZE  
7 000008: LT  
8 000009: PUSH2 0x006d  
9 000012: JUMPI  
10 000013: PUSH1 0x00  
11 000015: CALLDATALOAD  
12 000016: PUSH29 0x0100000000000000  
13 000046: SWAP1  
14 000047: DIV  
15 000048: PUSH4 0xffffffff  
16 000053: AND  
17 000054: DUP1  
18 000055: PUSH4 0x362186ed  
19 000060: EQ  
20 000061: PUSH2 0x008d  
21 000064: JUMPI  
22 000065: DUP1  
23 000066: PUSH4 0x362186ed  
24 000069: EQ  
25 000070: JUMPI  
26 000071: PUSH2 0x008d  
27 000074: JUMPI  
28 000075: PUSH1 0x00  
29 000077: JUMP  
30 000079: JUMPDEST  
31 000080: PUSH1 0x00  
32 000082: JUMP  
33 000084: JUMPDEST  
34 000085: PUSH1 0x00  
35 000087: JUMP  
36 000089: JUMPDEST  
37 000090: PUSH1 0x00  
38 000092: JUMP  
39 000094: JUMPDEST  
40 000095: PUSH1 0x00  
41 000097: JUMP  
42 000099: JUMPDEST  
43 000100: PUSH1 0x00  
44 000102: JUMP  
45 000104: JUMPDEST  
46 000105: PUSH1 0x00  
47 000107: JUMP  
48 000109: JUMPDEST  
49 000110: PUSH1 0x00  
50 000112: JUMP  
51 000114: JUMPDEST  
52 000115: PUSH1 0x00  
53 000117: JUMP  
54 000119: JUMPDEST  
55 000120: PUSH1 0x00  
56 000122: JUMP  
57 000124: JUMPDEST  
58 000125: PUSH1 0x00  
59 000127: JUMP  
60 000129: JUMPDEST  
61 000130: PUSH1 0x00  
62 000132: JUMP  
63 000134: JUMPDEST  
64 000135: PUSH1 0x00  
65 000137: JUMP  
66 000139: JUMPDEST  
67 000140: PUSH1 0x00  
68 000142: JUMP  
69 000144: JUMPDEST  
70 000145: PUSH1 0x00  
71 000147: JUMP  
72 000149: JUMPDEST  
73 000150: PUSH1 0x00  
74 000152: JUMP  
75 000154: JUMPDEST  
76 000155: PUSH1 0x00  
77 000157: JUMP  
78 000159: JUMPDEST  
79 000160: PUSH1 0x00  
80 000162: JUMP  
81 000164: JUMPDEST  
82 000165: PUSH1 0x00  
83 000167: JUMP  
84 000169: JUMPDEST  
85 000170: PUSH1 0x00  
86 000172: JUMP  
87 000174: JUMPDEST  
88 000175: PUSH1 0x00  
89 000177: JUMP  
90 000179: JUMPDEST  
91 000180: PUSH1 0x00  
92 000182: JUMP  
93 000184: JUMPDEST  
94 000185: PUSH1 0x00  
95 000187: JUMP  
96 000189: JUMPDEST  
97 000190: PUSH1 0x00  
98 000192: JUMP  
99 000194: JUMPDEST  
100 000195: PUSH1 0x00  
101 000197: JUMP  
102 000199: JUMPDEST  
103 000200: PUSH1 0x00  
104 000202: JUMP  
105 000204: JUMPDEST  
106 000205: PUSH1 0x00  
107 000207: JUMP  
108 000209: JUMPDEST  
109 000210: PUSH1 0x00  
110 000212: JUMP  
111 000214: JUMPDEST  
112 000215: PUSH1 0x00  
113 000217: JUMP  
114 000219: JUMPDEST  
115 000220: PUSH1 0x00  
116 000222: JUMP  
117 000224: JUMPDEST  
118 000225: PUSH1 0x00  
119 000227: JUMP  
120 000229: JUMPDEST  
121 000230: PUSH1 0x00  
122 000232: JUMP  
123 000234: JUMPDEST  
124 000235: PUSH1 0x00  
125 000237: JUMP  
126 000239: JUMPDEST  
127 000240: PUSH1 0x00  
128 000242: JUMP  
129 000244: JUMPDEST  
130 000245: PUSH1 0x00  
131 000247: JUMP  
132 000249: JUMPDEST  
133 000250: PUSH1 0x00  
134 000252: JUMP  
135 000254: JUMPDEST  
136 000255: PUSH1 0x00  
137 000257: JUMP  
138 000259: JUMPDEST  
139 000260: PUSH1 0x00  
140 000262: JUMP  
141 000264: JUMPDEST  
142 000265: PUSH1 0x00  
143 000267: JUMP  
144 000269: JUMPDEST  
145 000270: PUSH1 0x00  
146 000272: JUMP  
147 000274: JUMPDEST  
148 000275: PUSH1 0x00  
149 000277: JUMP  
150 000279: JUMPDEST  
151 000280: PUSH1 0x00  
152 000282: JUMP  
153 000284: JUMPDEST  
154 000285: PUSH1 0x00  
155 000287: JUMP  
156 000289: JUMPDEST  
157 000290: PUSH1 0x00  
158 000292: JUMP  
159 000294: JUMPDEST  
160 000295: PUSH1 0x00  
161 000297: JUMP  
162 000299: JUMPDEST  
163 000300: PUSH1 0x00  
164 000302: JUMP  
165 000304: JUMPDEST  
166 000305: PUSH1 0x00  
167 000307: JUMP  
168 000309: JUMPDEST  
169 000310: PUSH1 0x00  
170 000312: JUMP  
171 000314: JUMPDEST  
172 000315: PUSH1 0x00  
173 000317: JUMP  
174 000319: JUMPDEST  
175 000320: PUSH1 0x00  
176 000322: JUMP  
177 000324: JUMPDEST  
178 000325: PUSH1 0x00  
179 000327: JUMP  
180 000329: JUMPDEST  
181 000330: PUSH1 0x00  
182 000332: JUMP  
183 000334: JUMPDEST  
184 000335: PUSH1 0x00  
185 000337: JUMP  
186 000339: JUMPDEST  
187 000340: PUSH1 0x00  
188 000342: JUMP  
189 000344: JUMPDEST  
190 000345: PUSH1 0x00  
191 000347: JUMP  
192 000349: JUMPDEST  
193 000350: PUSH1 0x00  
194 000352: JUMP  
195 000354: JUMPDEST  
196 000355: PUSH1 0x00  
197 000357: JUMP  
198 000359: JUMPDEST  
199 000360: PUSH1 0x00  
200 000362: JUMP  
201 000364: JUMPDEST  
202 000365: PUSH1 0x00  
203 000367: JUMP  
204 000369: JUMPDEST  
205 000370: PUSH1 0x00  
206 000372: JUMP  
207 000374: JUMPDEST  
208 000375: PUSH1 0x00  
209 000377: JUMP  
210 000379: JUMPDEST  
211 000380: PUSH1 0x00  
212 000382: JUMP  
213 000384: JUMPDEST  
214 000385: PUSH1 0x00  
215 000387: JUMP  
216 000389: JUMPDEST  
217 000390: PUSH1 0x00  
218 000392: JUMP  
219 000394: JUMPDEST  
220 000395: PUSH1 0x00  
221 000397: JUMP  
222 000399: JUMPDEST  
223 000400: PUSH1 0x00  
224 000402: JUMP  
225 000404: JUMPDEST  
226 000405: PUSH1 0x00  
227 000407: JUMP  
228 000409: JUMPDEST  
229 000410: PUSH1 0x00  
230 000412: JUMP  
231 000414: JUMPDEST  
232 000415: PUSH1 0x00  
233 000417: JUMP  
234 000419: JUMPDEST  
235 000420: PUSH1 0x00  
236 000422: JUMP  
237 000424: JUMPDEST  
238 000425: PUSH1 0x00  
239 000427: JUMP  
240 000429: JUMPDEST  
241 000430: PUSH1 0x00  
242 000432: JUMP  
243 000434: JUMPDEST  
244 000435: PUSH1 0x00  
245 000437: JUMP  
246 000439: JUMPDEST  
247 000440: PUSH1 0x00  
248 000442: JUMP  
249 000444: JUMPDEST  
250 000445: PUSH1 0x00  
251 000447: JUMP  
252 000449: JUMPDEST  
253 000450: PUSH1 0x00  
254 000452: JUMP  
255 000454: JUMPDEST  
256 000455: PUSH1 0x00  
257 000457: JUMP  
258 000459: JUMPDEST  
259 000460: PUSH1 0x00  
260 000462: JUMP  
261 000464: JUMPDEST  
262 000465: PUSH1 0x00  
263 000467: JUMP  
264 000469: JUMPDEST  
265 000470: PUSH1 0x00  
266 000472: JUMP  
267 000474: JUMPDEST  
268 000475: PUSH1 0x00  
269 000477: JUMP  
270 000479: JUMPDEST  
271 000480: PUSH1 0x00  
272 000482: JUMP  
273 000484: JUMPDEST  
274 000485: PUSH1 0x00  
275 000487: JUMP  
276 000489: JUMPDEST  
277 000490: PUSH1 0x00  
278 000492: JUMP  
279 000494: JUMPDEST  
280 000495: PUSH1 0x00  
281 000497: JUMP  
282 000499: JUMPDEST  
283 000500: PUSH1 0x00  
284 000502: JUMP  
285 000504: JUMPDEST  
286 000505: PUSH1 0x00  
287 000507: JUMP  
288 000509: JUMPDEST  
289 000510: PUSH1 0x00  
290 000512: JUMP  
291 000514: JUMPDEST  
292 000515: PUSH1 0x00  
293 000517: JUMP  
294 000519: JUMPDEST  
295 000520: PUSH1 0x00  
296 000522: JUMP  
297 000524: JUMPDEST  
298 000525: PUSH1 0x00  
299 000527: JUMP  
300 000529: JUMPDEST  
301 000530: PUSH1 0x00  
302 000532: JUMP  
303 000534: JUMPDEST  
304 000535: PUSH1 0x00  
305 000537: JUMP  
306 000539: JUMPDEST  
307 000540: PUSH1 0x00  
308 000542: JUMP  
309 000544: JUMPDEST  
310 000545: PUSH1 0x00  
311 000547: JUMP  
312 000549: JUMPDEST  
313 000550: PUSH1 0x00  
314 000552: JUMP  
315 000554: JUMPDEST  
316 000555: PUSH1 0x00  
317 000557: JUMP  
318 000559: JUMPDEST  
319 000560: PUSH1 0x00  
320 000562: JUMP  
321 000564: JUMPDEST  
322 000565: PUSH1 0x00  
323 000567: JUMP  
324 000569: JUMPDEST  
325 000570: PUSH1 0x00  
326 000572: JUMP  
327 000574: JUMPDEST  
328 000575: PUSH1 0x00  
329 000577: JUMP  
330 000579: JUMPDEST  
331 000580: PUSH1 0x00  
332 000582: JUMP  
333 000584: JUMPDEST  
334 000585: PUSH1 0x00  
335 000587: JUMP  
336 000589: JUMPDEST  
337 000590: PUSH1 0x00  
338 000592: JUMP  
339 000594: JUMPDEST  
340 000595: PUSH1 0x00  
341 000597: JUMP  
342 000599: JUMPDEST  
343 000600: PUSH1 0x00  
344 000602: JUMP  
345 000604: JUMPDEST  
346 000605: PUSH1 0x00  
347 000607: JUMP  
348 000609: JUMPDEST  
349 000610: PUSH1 0x00  
350 000612: JUMP  
351 000614: JUMPDEST  
352 000615: PUSH1 0x00  
353 000617: JUMP  
354 000619: JUMPDEST  
355 000620: PUSH1 0x00  
356 000622: JUMP  
357 000624: JUMPDEST  
358 000625: PUSH1 0x00  
359 000627: JUMP  
360 000629: JUMPDEST  
361 000630: PUSH1 0x00  
362 000632: JUMP  
363 000634: JUMPDEST  
364 000635: PUSH1 0x00  
365 000637: JUMP  
366 000639: JUMPDEST  
367 000640: PUSH1 0x00  
368 000642: JUMP  
369 000644: JUMPDEST  
370 000645: PUSH1 0x00  
371 000647: JUMP  
372 000649: JUMPDEST  
373 000650: PUSH1 0x00  
374 000652: JUMP  
375 000654: JUMPDEST  
376 000655: PUSH1 0x00  
377 000657: JUMP  
378 000659: JUMPDEST  
379 000660: PUSH1 0x00  
380 000662: JUMP  
381 000664: JUMPDEST  
382 000665: PUSH1 0x00  
383 000667: JUMP  
384 000669: JUMPDEST  
385 000670: PUSH1 0x00  
386 000672: JUMP  
387 000674: JUMPDEST  
388 000675: PUSH1 0x00  
389 000677: JUMP  
390 000679: JUMPDEST  
391 000680: PUSH1 0x00  
392 000682: JUMP  
393 000684: JUMPDEST  
394 000685: PUSH1 0x00  
395 000687: JUMP  
396 000689: JUMPDEST  
397 000690: PUSH1 0x00  
398 000692: JUMP  
399 000694: JUMPDEST  
400 000695: PUSH1 0x00  
401 000697: JUMP  
402 000699: JUMPDEST  
403 000700: PUSH1 0x00  
404 000702: JUMP  
405 000704: JUMPDEST  
406 000705: PUSH1 0x00  
407 000707: JUMP  
408 000709: JUMPDEST  
409 000710: PUSH1 0x00  
410 000712: JUMP  
411 000714: JUMPDEST  
412 000715: PUSH1 0x00  
413 000717: JUMP  
414 000719: JUMPDEST  
415 000720: PUSH1 0x00  
416 000722: JUMP  
417 000724: JUMPDEST  
418 000725: PUSH1 0x00  
419 000727: JUMP  
420 000729: JUMPDEST  
421 000730: PUSH1 0x00  
422 000732: JUMP  
423 000734: JUMPDEST  
424 000735: PUSH1 0x00  
425 000737: JUMP  
426 000739: JUMPDEST  
427 000740: PUSH1 0x00  
428 000742: JUMP  
429 000744: JUMPDEST  
430 000745: PUSH1 0x00  
431 000747: JUMP  
432 000749: JUMPDEST  
433 000750: PUSH1 0x00  
434 000752: JUMP  
435 000754: JUMPDEST  
436 000755: PUSH1 0x00  
437 000757: JUMP  
438 000759: JUMPDEST  
439 000760: PUSH1 0x00  
440 000762: JUMP  
441 000764: JUMPDEST  
442 000765: PUSH1 0x00  
443 000767: JUMP  
444 000769: JUMPDEST  
445 000770: PUSH1 0x00  
446 000772: JUMP  
447 000774: JUMPDEST  
448 000775: PUSH1 0x00  
449 000777: JUMP  
450 000779: JUMPDEST  
451 000780: PUSH1 0x00  
452 000782: JUMP  
453 000784: JUMPDEST  
454 000785: PUSH1 0x00  
455 000787: JUMP  
456 000789: JUMPDEST  
457 000790: PUSH1 0x00  
458 000792: JUMP  
459 000794: JUMPDEST  
460 000795: PUSH1 0x00  
461 000797: JUMP  
462 000799: JUMPDEST  
463 000800: PUSH1 0x00  
464 000802: JUMP  
465 000804: JUMPDEST  
466 000805: PUSH1 0x00  
467 000807: JUMP  
468 000809: JUMPDEST  
469 000810: PUSH1 0x00  
470 000812: JUMP  
471 000814: JUMPDEST  
472 000815: PUSH1 0x00  
473 000817: JUMP  
474 000819: JUMPDEST  
475 000820: PUSH1 0x00  
476 000822: JUMP  
477 000824: JUMPDEST  
478 000825: PUSH1 0x00  
479 000827: JUMP  
480 000829: JUMPDEST  
481 000830: PUSH1 0x00  
482 000832: JUMP  
483 000834: JUMPDEST  
484 000835: PUSH1 0x00  
485 000837: JUMP  
486 000839: JUMPDEST  
487 000840: PUSH1 0x00  
488 000842: JUMP  
489 000844: JUMPDEST  
490 000845: PUSH1 0x00  
491 000847: JUMP  
492 000849: JUMPDEST  
493 000850: PUSH1 0x00  
494 000852: JUMP  
495 000854: JUMPDEST  
496 000855: PUSH1 0x00  
497 000857: JUMP  
498 000859: JUMPDEST  
499 000860: PUSH1 0x00  
500 000862: JUMP  
501 000864: JUMPDEST  
502 000865: PUSH1 0x00  
503 000867: JUMP  
504 000869: JUMPDEST  
505 000870: PUSH1 0x00  
506 000872: JUMP  
507 000874: JUMPDEST  
508 000875: PUSH1 0x00  
509 000877: JUMP  
510 000879: JUMPDEST  
511 000880: PUSH1 0x00  
512 000882: JUMP  
513 000884: JUMPDEST  
514 000885: PUSH1 0x00  
515 000887: JUMP  
516 000889: JUMPDEST  
517 000890: PUSH1 0x00  
518 000892: JUMP  
519 000894: JUMPDEST  
520 000895: PUSH1 0x00  
521 000897: JUMP  
522 000899: JUMPDEST  
523 000900: PUSH1 0x00  
524 000902: JUMP  
525 000904: JUMPDEST  
526 000905: PUSH1 0x00  
527 000907: JUMP  
528 000909: JUMPDEST  
529 000910: PUSH1 0x00  
530 000912: JUMP  
531 000914: JUMPDEST  
532 000915: PUSH1 0x00  
533 000917: JUMP  
534 000919: JUMPDEST  
535 000920: PUSH1 0x00  
536 000922: JUMP  
537 000924: JUMPDEST  
538 000925: PUSH1 0x00  
539 000927: JUMP  
540 000929: JUMPDEST  
541 000930: PUSH1 0x00  
542 000932: JUMP  
543 000934: JUMPDEST  
544 000935: PUSH1 0x00  
545 000937: JUMP  
546 000939: JUMPDEST  
547 000940: PUSH1 0x00  
548 000942: JUMP  
549 000944: JUMPDEST  
550 000945: PUSH1 0x00  
551 000947: JUMP  
552 000949: JUMPDEST  
553 000950: PUSH1 0x00  
554 000952: JUMP  
555 000954: JUMPDEST  
556 000955: PUSH1 0x00  
557 000957: JUMP  
558 000959: JUMPDEST  
559 000960: PUSH1 0x00  
560 000962: JUMP  
561 000964: JUMPDEST  
562 000965: PUSH1 0x00  
563 000967: JUMP  
564 000969: JUMPDEST  
565 000970: PUSH1 0x00  
566 000972: JUMP  
567 000974: JUMPDEST  
568 000975: PUSH1 0x00  
569 000977: JUMP  
570 000979: JUMPDEST  
571 000980: PUSH1 0x00  
572 000982: JUMP  
573 000984: JUMPDEST  
574 000985: PUSH1 0x00  
575 000987: JUMP  
576 000989: JUMPDEST  
577 000990: PUSH1 0x00  
578 000992: JUMP  
579 000994: JUMPDEST  
580 000995: PUSH1 0x00  
581 000997: JUMP  
582 000999: JUMPDEST  
583 001000: PUSH1 0x00  
584 001002: JUMP  
585 001004: JUMPDEST  
586 001005: PUSH1 0x00  
587 001007: JUMP  
588 001009: JUMPDEST  
589 001010: PUSH1 0x00  
590 001012: JUMP  
591 001014: JUMPDEST  
592 001015: PUSH1 0x00  
593 001017: JUMP  
594 001019: JUMPDEST  
595 001020: PUSH1 0x00  
596 001022: JUMP  
597 001024: JUMPDEST  
598 001025: PUSH1 0x00  
599 001027: JUMP  
600 001029: JUMPDEST  
601 001030: PUSH1 0x00  
602 001032: JUMP  
603 001034: JUMPDEST  
604 001035: PUSH1 0x00  
605 001037: JUMP  
606 001039: JUMPDEST  
607 001040: PUSH1 0x00  
608 001042: JUMP  
609 001044: JUMPDEST  
610 001045: PUSH1 0x00  
611 001047: JUMP  
612 001049: JUMPDEST  
613 001050: PUSH1 0x00  
614 001052: JUMP  
615 001054: JUMPDEST  
616 001055: PUSH1 0x00  
617 001057: JUMP  
618 001059: JUMPDEST  
619 001060: PUSH1 0x00  
620 001062: JUMP  
621 001064: JUMPDEST  
622 001065: PUSH1 0x00  
623 001067: JUMP  
624 001069: JUMPDEST  
625 001070: PUSH1 0x00  
626 001072: JUMP  
627 001074: JUMPDEST  
628 001075: PUSH1 0x00  
629 001077: JUMP  
630 001079: JUMPDEST  
631 001080: PUSH1 0x00  
632 001082: JUMP  
633 001084: JUMPDEST  
634 001085: PUSH1 0x00  
635 001087: JUMP  
636 001089: JUMPDEST  
637 001090: PUSH1 0x00  
638 001092: JUMP  
639 001094: JUMPDEST  
640 001095: PUSH1 0x00  
641 001097: JUMP  
642 001099: JUMPDEST  
643 001100: PUSH1 0x00  
644 001102: JUMP  
645 001104: JUMPDEST  
646 001105: PUSH1 0x00  
647 001107: JUMP  
648 001109: JUMPDEST  
649 001110: PUSH1 0x00  
650 001112: JUMP  
651 001114: JUMPDEST  
652 001115: PUSH1 0x00  
653 001117: JUMP  
654 001119: JUMPDEST  
655 001120: PUSH1 0x00  
656 001122: JUMP  
657 001124: JUMPDEST  
658 001125: PUSH1 0x00  
659 001127: JUMP  
660 001129: JUMPDEST  
661 001130: PUSH1 0x00  
662 001132: JUMP  
663 001134: JUMPDEST  
664 001135: PUSH1 0x00  
665 001137: JUMP  
666 001139: JUMPDEST  
667 001140: PUSH1 0x00  
668 001142: JUMP  
669 001144: JUMPDEST  
670 001145: PUSH1 0x00  
671 001147: JUMP  
672 001149: JUMPDEST  
673 001150: PUSH1 0x00  
674 001152: JUMP  
675 001154: JUMPDEST  
676 001155: PUSH1 0x00  
677 001157: JUMP  
678 001159: JUMPDEST  
679 001160: PUSH1 0x00  
680 001162: JUMP  
681 001164: JUMPDEST  
682 001165: PUSH1 0x00  
683 001167: JUMP  
684 001169: JUMPDEST  
685 001170: PUSH1 0x00  
686 001172: JUMP  
687 001174: JUMPDEST  
688 001175: PUSH1 0x00  
689 001177: JUMP  
690 001179: JUMPDEST  
691 001180: PUSH1 0x00  
692 001182: JUMP  
693 001184: JUMPDEST  
694 001185: PUSH1 0x00  
695 001187: JUMP  
696 001189: JUMPDEST  
697 001190: PUSH1 0x00  
698 001192: JUMP  
699 001194: JUMPDEST  
700 001195: PUSH1 0x00  
701 001197: JUMP  
702 001199: JUMPDEST  
70
```

"smart contract" most used meaning
= **immutable low-level instructions**
cloned on each node
running in a decentralized fashion

"smart contract" most used meaning
= immutable low-level instructions
cloned on each node
running in a decentralized fashion

- What are the **gaps** with usual contracts?

a bilateral contract is a formal agreement in which both parties exchange promises to perform



contracts vs "smart contracts"

- **Readability:** parties should understand what the agreement is about

contracts vs “smart contracts”

- **Readability:** parties should understand what the agreement is about
- **Control:** parties should maintain **autonomy** on performance. e.g. non-foreseeable conditions may cause justifiable release of duty, that can be assessed only *ex-post*

contracts vs “smart contracts”

- **Readability:** parties should understand what the agreement is about
- **Control:** parties should maintain autonomy on performance. e.g. non-foreseeable conditions may cause justifiable release of duty, that can be assessed only *ex-post*
- **Amendment, Delegation, Mandate,** etc. are all **common constructs applicable on contracts** (unless explicitly disabled), but not in smart contracts.

contracts vs “smart contracts”

- **Readability:** parties should understand what the agreement is about
- **Control:** parties should maintain autonomy on performance. e.g. non-foreseeable conditions may cause justifiable release of duty, that can be assessed only *ex-post*
- **Amendment, Delegation, Mandate,** etc. are all common constructs applicable on contracts (unless explicitly disabled), but not in smart contracts.
- **Regulation:** there is not an equivalent of **contract law** or **private law** regulations (a sort of meta-contracts) in smart contracts

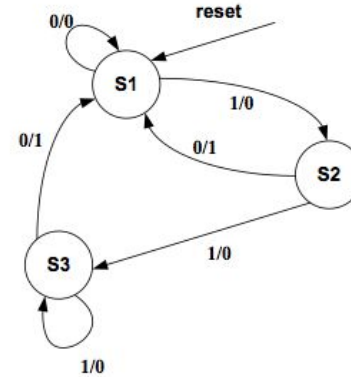
contracts vs “smart contracts”

- **Readability:** parties should understand what the agreement is about
- **Control:** parties should maintain autonomy on performance. e.g. non-foreseeable conditions may cause justifiable release of duty, that can be assessed only *ex-post*
- **Amendment, Delegation, Mandate,** etc. are all common constructs applicable on contracts (unless explicitly disabled), but not in smart contracts.
- **Regulation:** there is not an equivalent of contract law or private law regulations (a sort of meta-contracts) in smart contracts
- **Informational model (e.g. normative primitives):** contemporary smart contracts allow to specify *imperative instructions* driving performance mapping only to positive duties. What about **prohibitions**? What about **permissions, legal competences**?

cf. normative systems, computational theory of law

contracts vs “smart contracts”

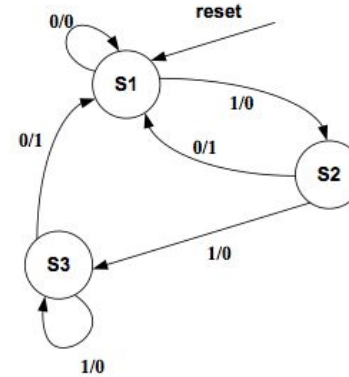
- Readability
- Control and *ex-post* enforcement
- Amendment, Delegation, Mandate
- Regulation
- Informational model



In most practical applications smart contracts depend on offline events, triggered by oracles. The environment “sets” the pace of execution.

contracts vs “smart contracts”

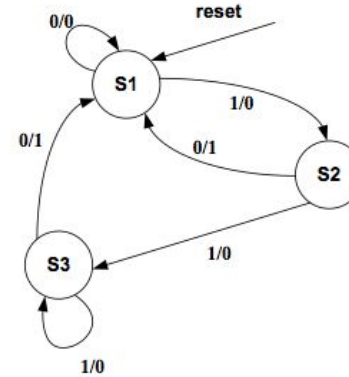
- Readability
- Control and *ex-post* enforcement
- Amendment, Delegation, Mandate
- Regulation
- Informational model



However, the **“dynamics” of contracts** depends not only on performance-related elements, but also on **contextual factors** (legal, social, physical) that *modify the contract semantics* itself.

contracts vs “smart contracts”

- Readability
- Control and *ex-post* enforcement
- Amendment, Delegation, Mandate
- Regulation
- Informational model

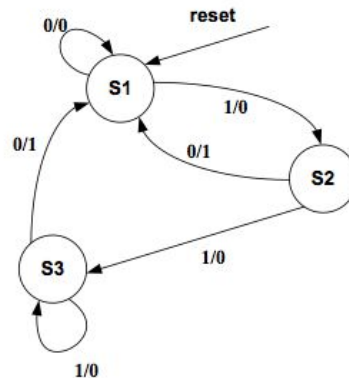


However, the **“dynamics” of contracts** depends not only on performance-related elements, but also on **contextual factors** (legal, social, physical) that *modify the contract semantics* itself.

The question is: **Can any socio-institutional systems (legal or not) be sustainable without these capacities?**

contracts vs “smart contracts” vs digital enforceable contracts?

- Readability
- Control and *ex-post* enforcement
- Amendment, Delegation, Mandate
- Regulation
- Informational model



However, the **“dynamics” of contracts** depends not only on performance-related elements, but also on **contextual factors** (legal, social, physical) that *modify the contract semantics* itself.

The question is: **Can any socio-institutional systems (legal or not) be sustainable without these capacities?**