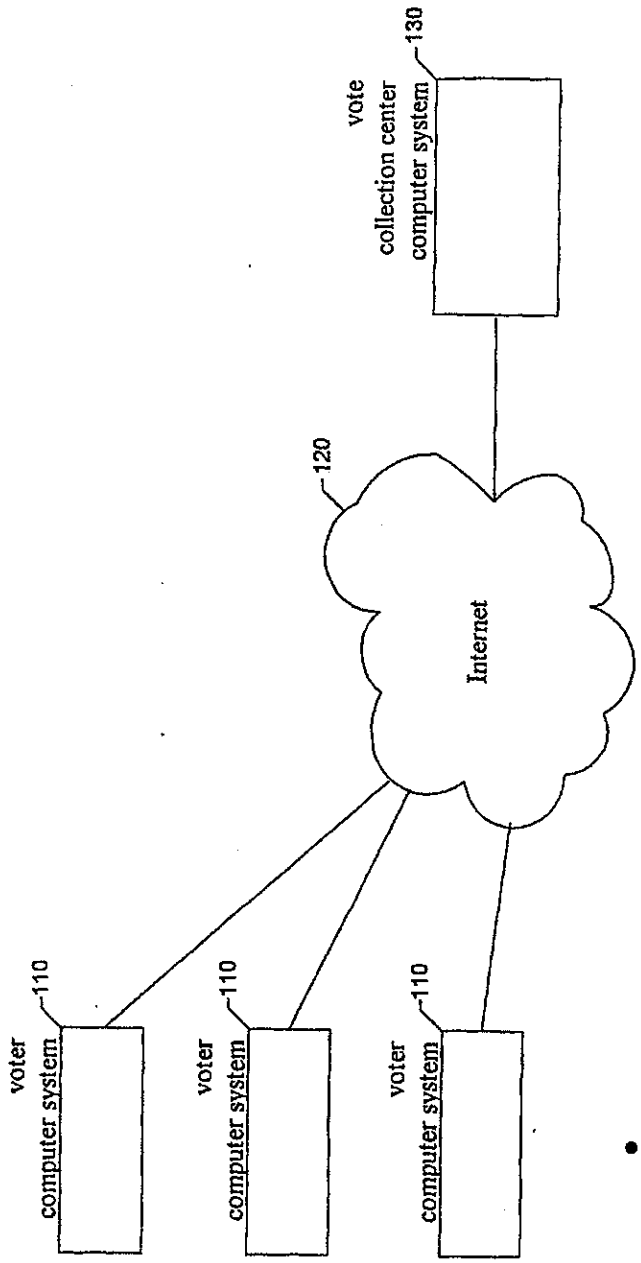

vote
collection center
computer system
130
120
Internet
voter
computer system
110
voter
computer system
110
voter
computer system
110

Fig. 1

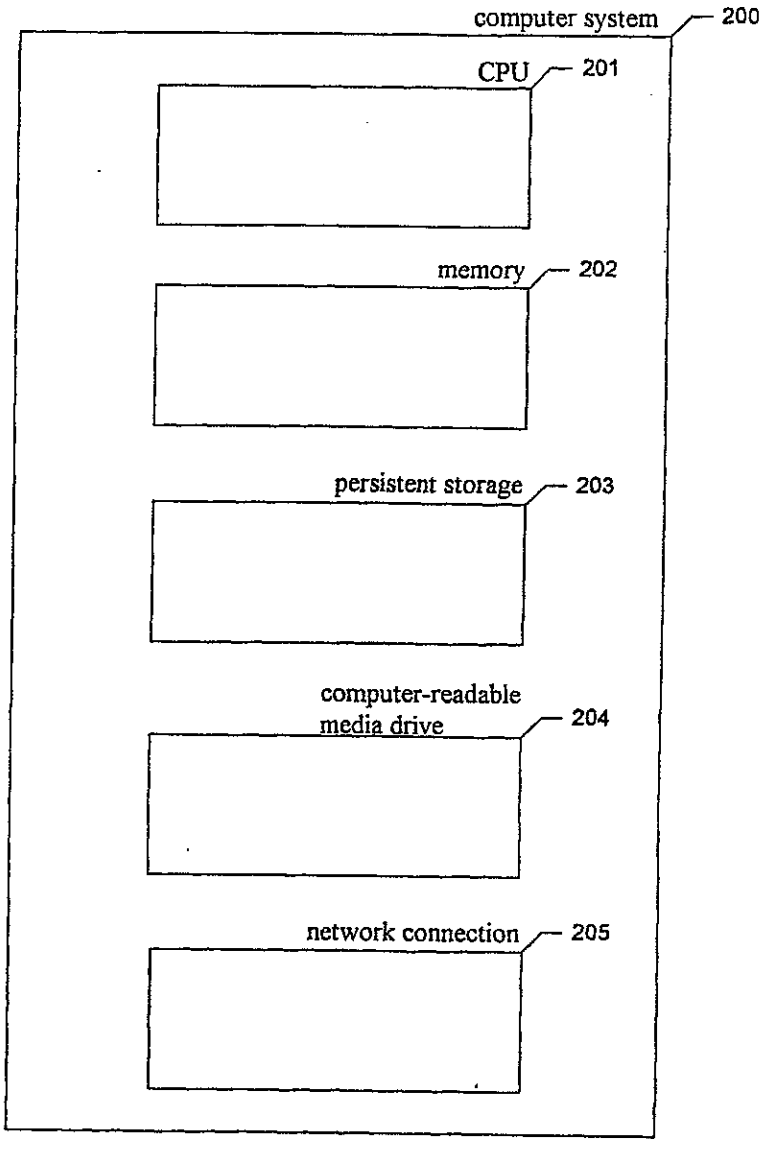

computer system
200
CPU
201
memory
202
persistent storage
203
computer-readable
media drive
204
network connection
205

Fig. 2

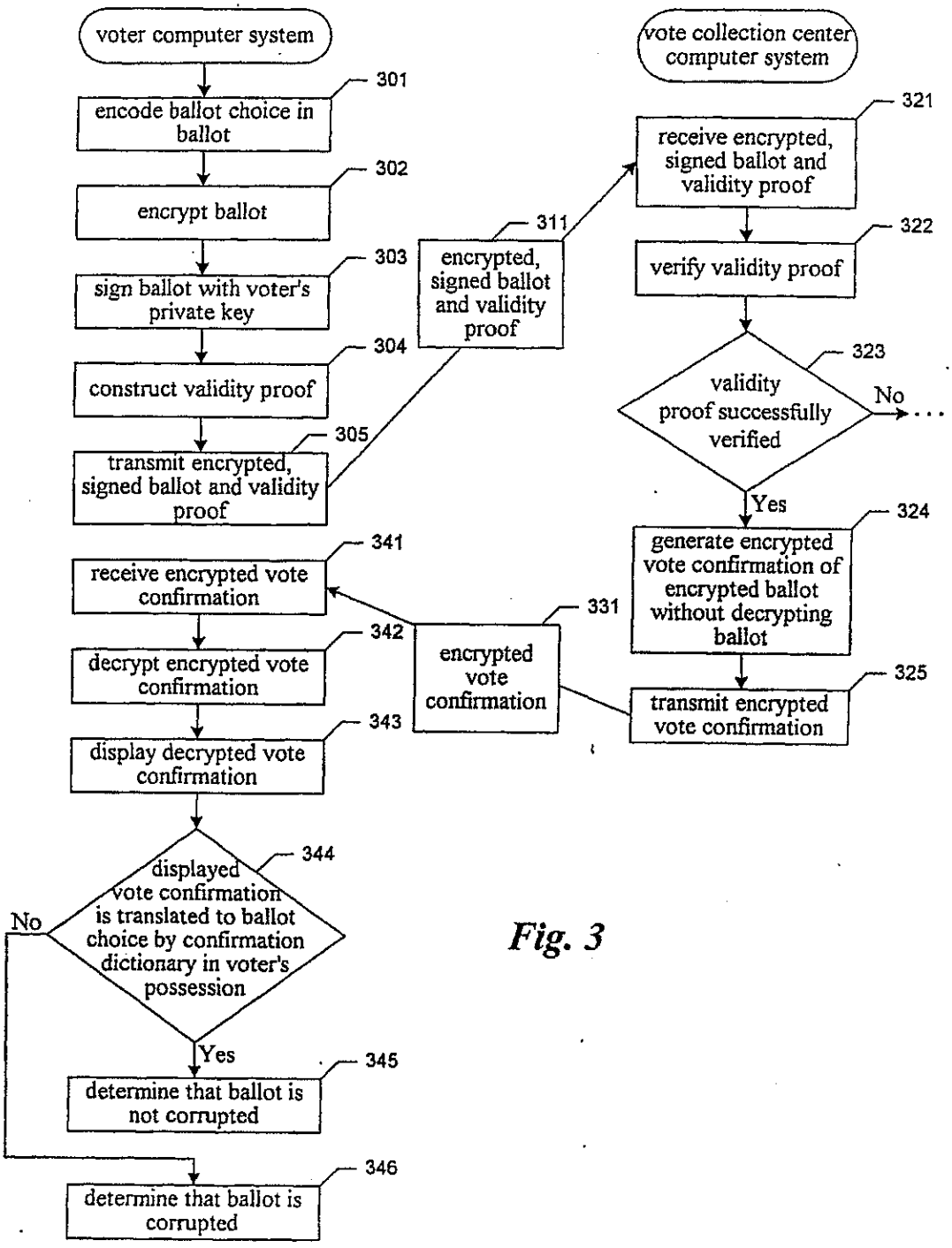

voter computer system
vote collection center computer system
301
encode ballot choice in ballot
302
encrypt ballot
303
sign ballot with voter's private key
304
construct validity proof
305
transmit encrypted, signed ballot and validity proof
311
encrypted, signed ballot and validity proof
321
receive encrypted, signed ballot and validity proof
322
verify validity proof
323
validity proof successfully verified
No
Yes
324
generate encrypted vote confirmation of encrypted ballot without decrypting ballot
325
transmit encrypted vote confirmation
331
encrypted vote confirmation
341
receive encrypted vote confirmation
342
decrypt encrypted vote confirmation
343
display decrypted vote confirmation
344
displayed vote confirmation is translated to ballot choice by confirmation dictionary in voter's possession
No
Yes
345
determine that ballot is not corrupted
346
determine that ballot is corrupted

Fig. 3