

Keychain

System Diagrams



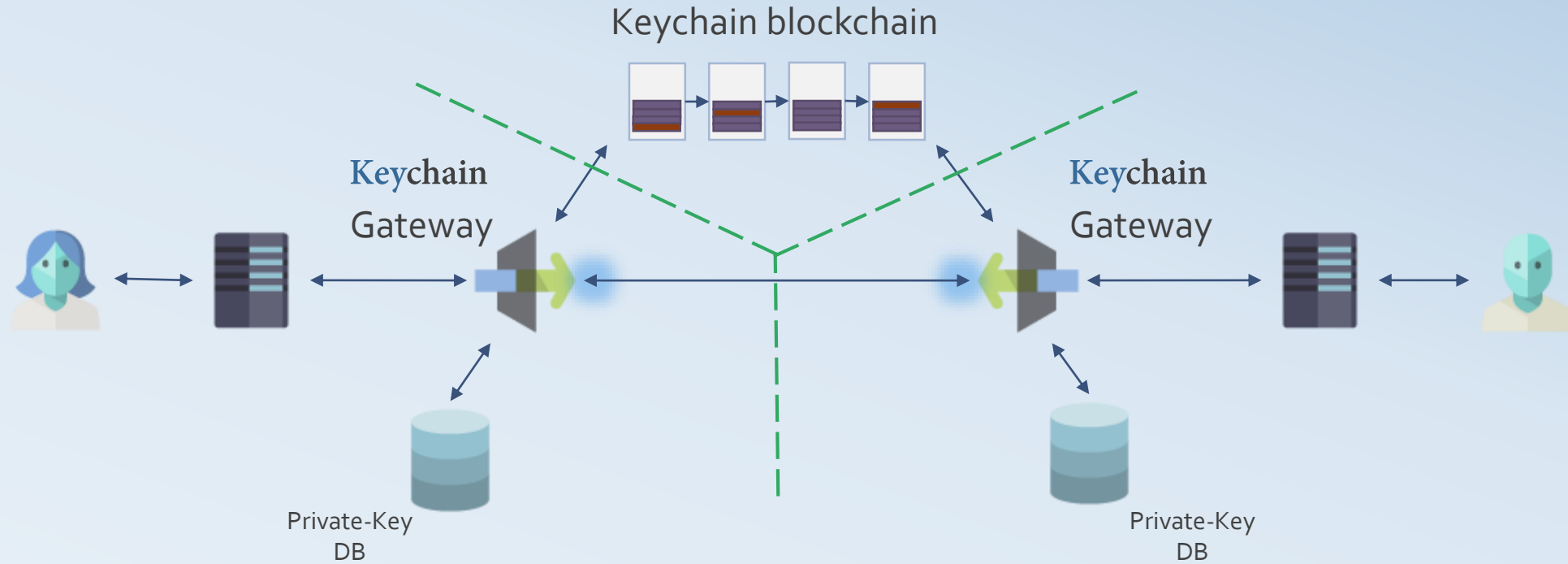
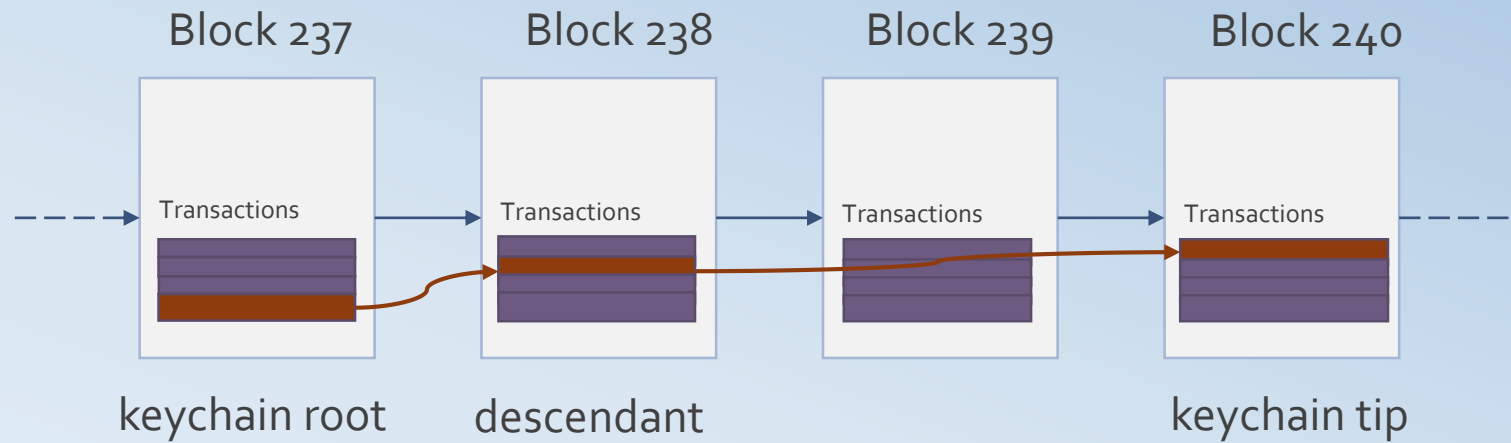


Fig. 1. Keychain Overview



Sample transaction payload

```
{  
  "type": "encryption",  
  "key": "0xA1B3FED...C76D5A",  
  "description": "RSA",  
  "version": "cryptopp-1.6.2"  
}
```

Fig. 2. Anatomy of a Keychain

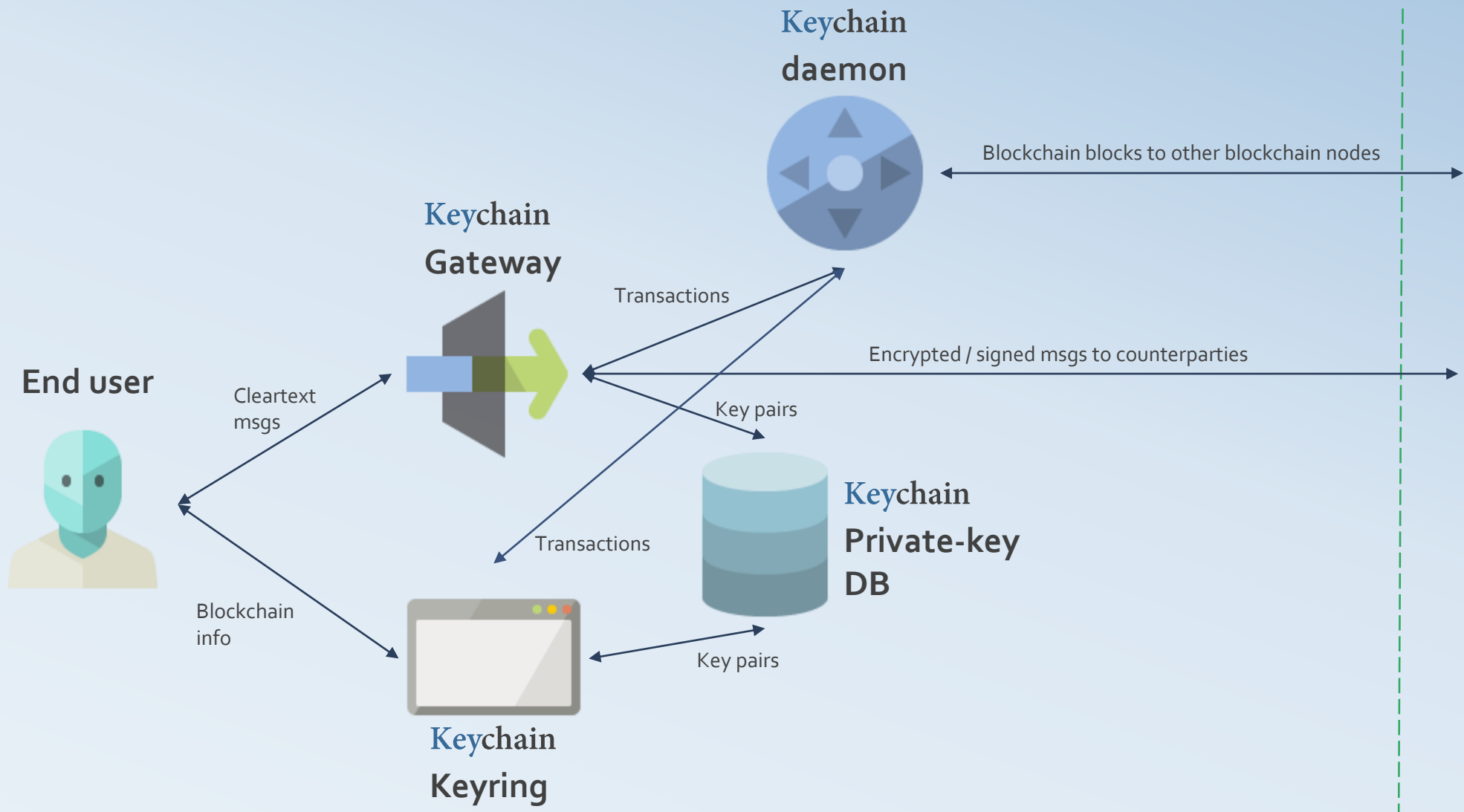


Fig. 3. Keychain System Components

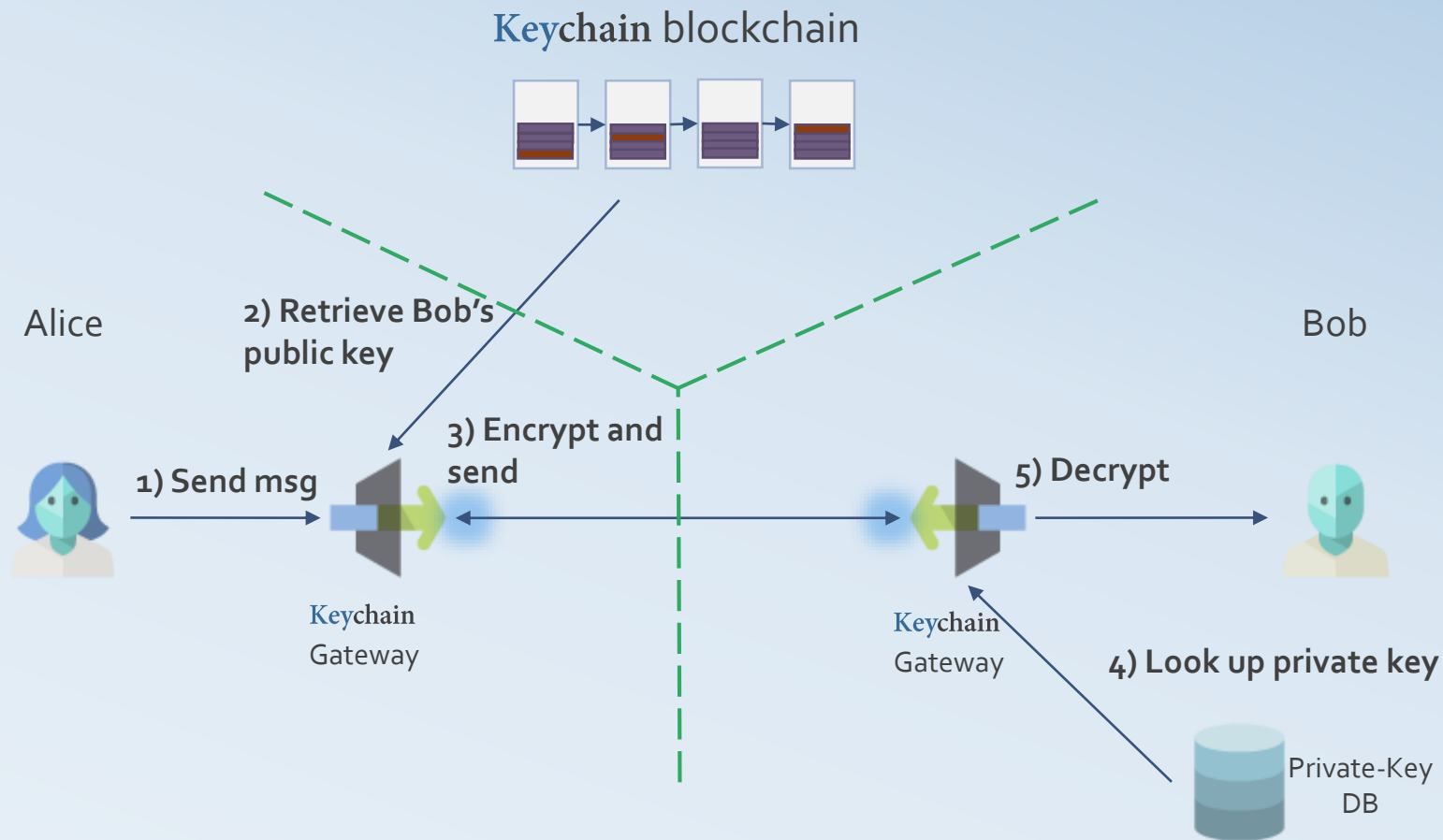


Fig. 4. Encryption and Decryption

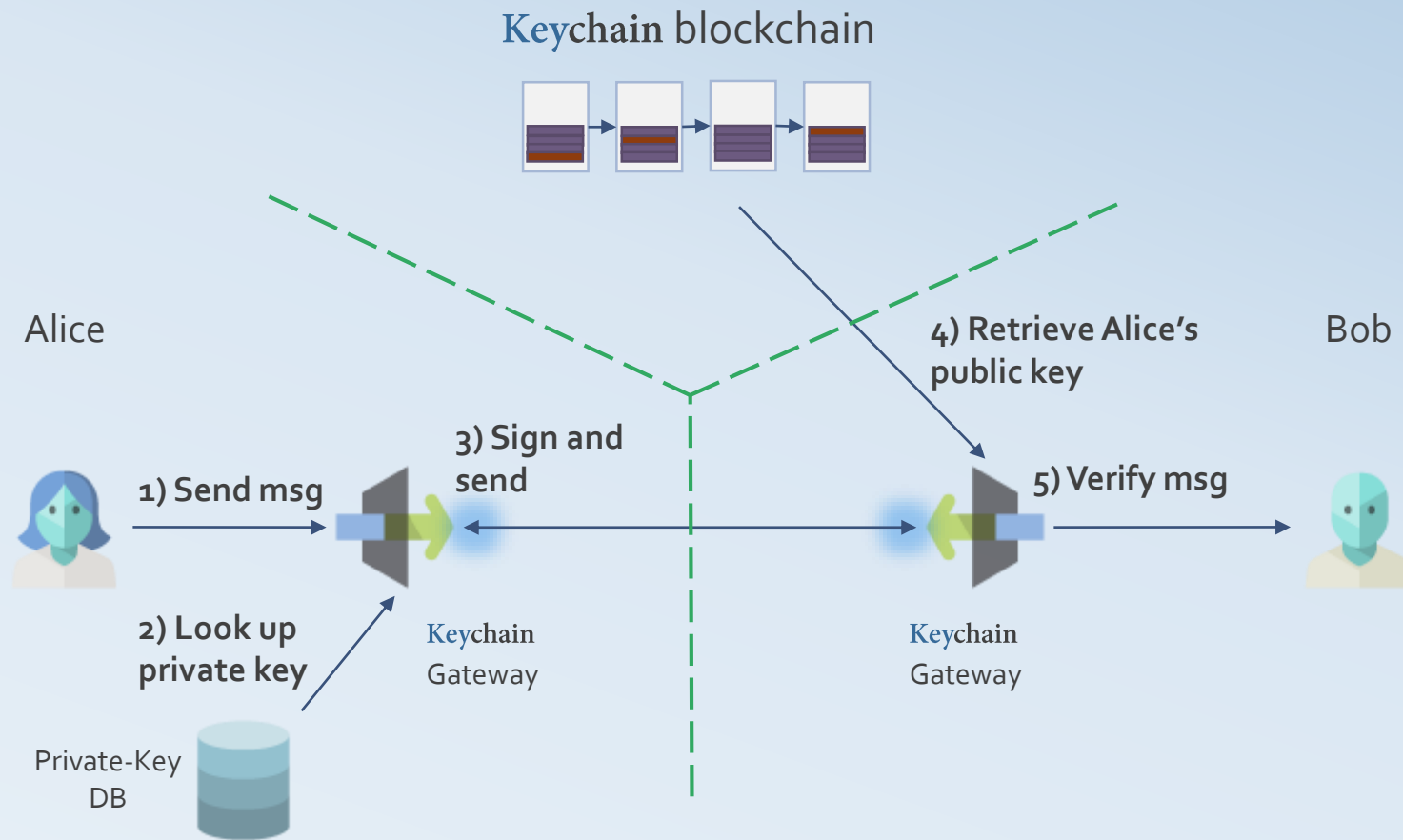


Fig. 5. Signing and Verification

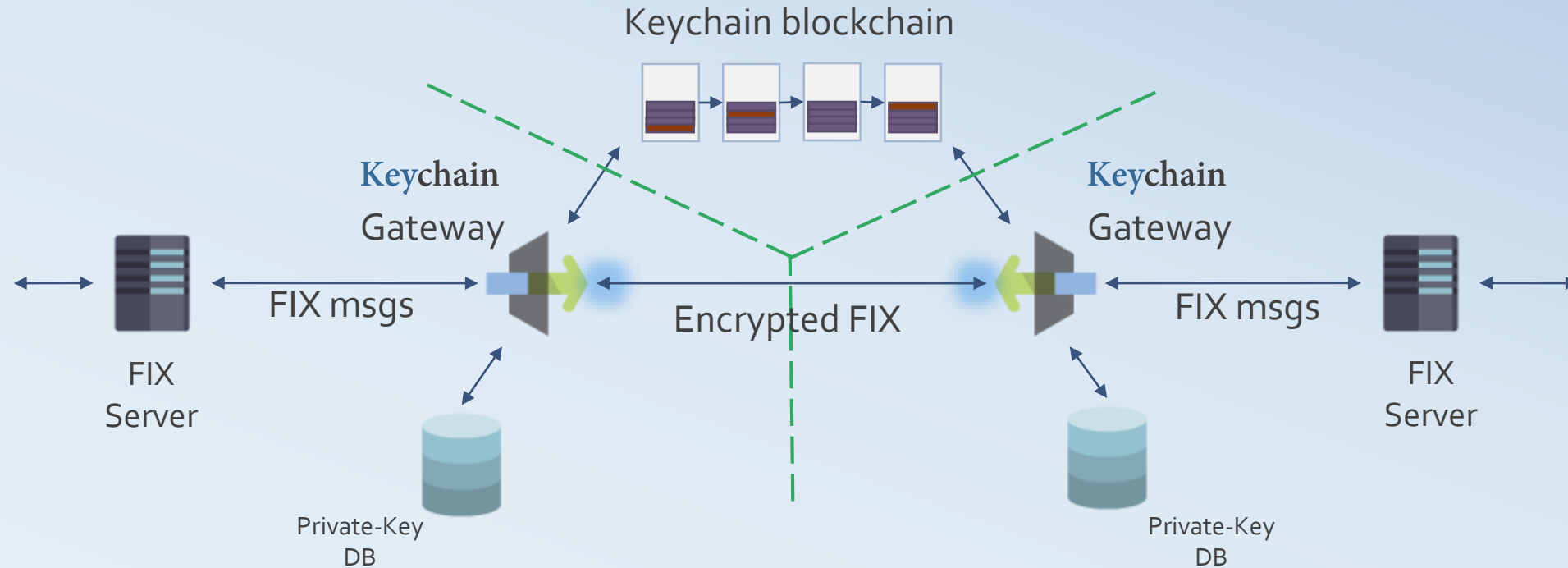


Fig. 6. Sample Process-driven Configuration

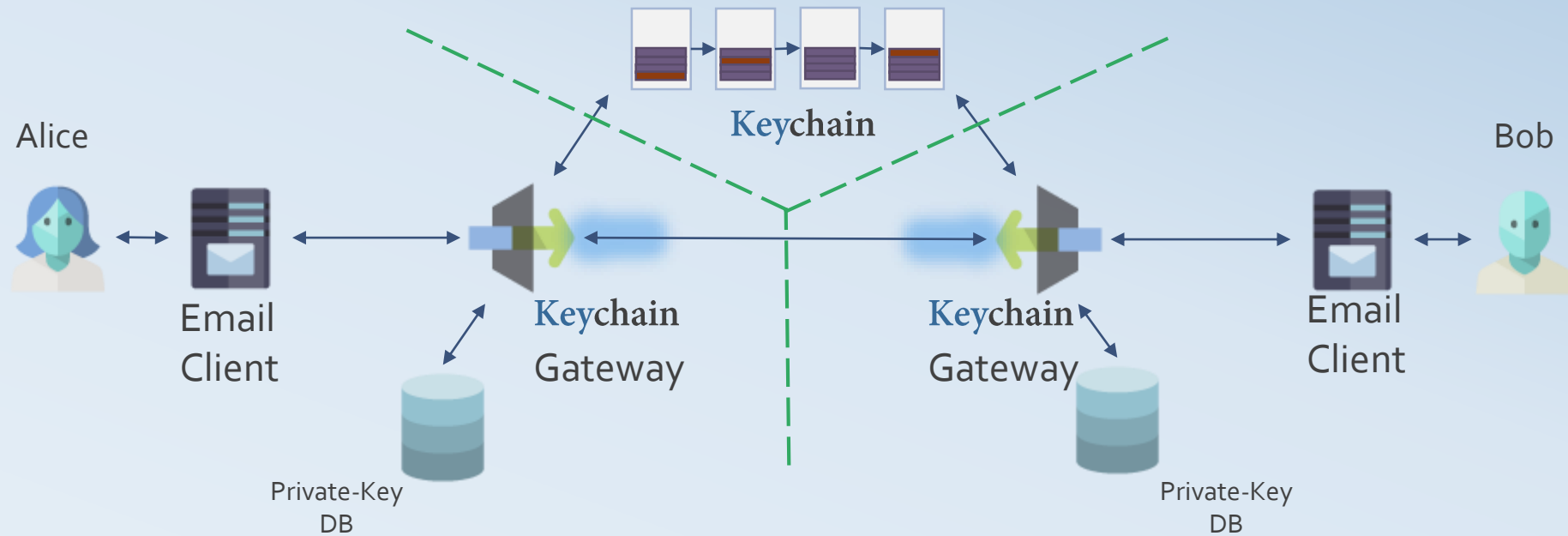


Fig. 7. Secure Email Communication Configuration



Fig. 8. QR Code of a Sample Root Key Transaction ID

```
Applications  Places  Sun May 8, 10:06 AM
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/kcgw

File Edit View Search Terminal Tabs Help

vagrant@vagrant-ubuntu-trusty-64: /vagrant/bin
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/keyring
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/kcgw

In [12]:
In [12]:
In [12]: e = g.encrypt('SMBC1', 'Got it!!!')
INFO:Main:encryption pubkey: ...f466abec

In [13]: print e
<SecureMessage Timestamp="2016-05-08 01:04:50.257350+00" Cipher="AES" PKI="ElGamal">
  <AssociatedData>
    <InitialValue>74F149C33635DD63146DB3A25DB339E0</InitialValue>
    <EncryptedSymmetricKeys>
      <EncryptedSymmetricKey>
        <CipherText>8D002FD0FF49BC257EB7E468C0747CB27A8DE3CA0090F51351D70825C3630677CF686B9A647167A632958B8C9524FD57979A622BF6788527E244E96D5ACE06F1C9DB5E015042B0D7654F7DBDB7C5431A9E
1B65EF147963F1739C2B9A4ABB296B30D3CAC5786D946FDA85434210B53AB5339D106B71F2A6073F888FB8C53451DFBEEBCAC0D5FA91D33A78B1371ACA73294B21240B4DFDC482F9C952E759986406506FE5D02228D2C24A0ED10CBA39245
D91B8849B0A6FCAB24F3CD4831459CD1140AE2958E93326944C6C9A4E1C748FBC06A376A8F3F7E1B98384044D406841FAE220981B0E27EE20045583AC09245F9F12E0804E122B040B2992804E50D108484945A4129D0BB3ED4A2AF9AA3308
4F7D3F601EDE331B0CC99A015272563636BD0D1F0F53B72B4781CC2D9F2FDD14BEBCB7FCB5C775D8CB84631FF82931BD3E27D7006C62E1E9CA5F23EC6FF527A45966E96AA90FE9C758960738B14972869D178E0225631BC9C48D2AB1CE6FB2
0DF1F3E75147A70AFD151B1A2E2868B20BBDABEB2A0402AC3D1B987ED36F963DA45C5B75D65AF8D1D7CC6B15342A7CC8A746F1C4DA56286E04DC17D87A149D8BAD7A4559A600037BEE175672F090212586EC39AC0D69C17721AB48B6CEA174
CA2C48ED9043DF184ACAF27AD0949FBD8EE55BB9FB6F3B990558323996605A680739B988005DC715E05C17A4781DD2572A7BC8</CipherText>
      <PublicKey>3082020C02820101009670B338BB41C8226DBE56318ABA75BC69176801BC2D5006D27D7BF05618CCBDCDFED591AAC8D4831884441B3A7C4B8E45C087B033E8AA2DB49B128495C88E49B3741696CA9F2B3841
A7E8F4D5E937A6C568FFE772356C38288011830F07257FC1D39DDA3BE2961F7EAF55118CF8AADB13CDD23296CB3391BB3EC0ACD5D025320AC2A39FB546D28A0D13C56CE8B8964A86D15B02153B01445217E7A90408991320E5E6F0A1DF757
9D0A18FE43168484A162352707F65A5ABC2F35B7E61A9358E0E9B7506E8DF12D3564A747FDC95860B3DDE85D161715B56207EF30896E1728B6F7DA325C4B293607A9CAEA9C394A9D6B669CA41E552FE5D65FCA6E07DC9CD4B0201030282010
068F6723C7A02DE23B2E508A3F58AD4FFD7D39A83B91D289DAD73AEFE3FD899F760F59708DA6D7A07E1B92B2D78CA77C6E9A21425FDC0EA59BD06400130716A2ABE792565FEC8B2AC11461CD7E01144794A887FF58BAFE638750A6ACC9613
075FD63BB971658A9086C89397A857B3516E12A859B6601FE78B9F646341839E4183AE7AD5A32F40E1E273C5E67F0F741DB095C08EA7930A4C3A5FE55B23D20B5089ED9E5A52AC0AFAD3AD079ECC95CAB93C6837EE1056B6F12351B50EF7C
BDAE9F9207145FBECAC4AD095878117001AE23D201F478CC93D21DB933D483B801080D7A3557613FD57D4EE0C2206A9C680B7ADF7303A5D4483F51B4193BF466ABEC</PublicKey>
    </EncryptedSymmetricKey>
  </EncryptedSymmetricKeys>
</AssociatedData>
<EncryptedMessage>CB211D0D72A5A91616406E3ACA6B87B87551099C7B7AE94FEA</EncryptedMessage>
</SecureMessage>

In [14]:
In [14]:
In [14]: d = g.decrypt('SMBC1', 'redman', e)
INFO:Main:decryption pubkey: ...f466abec

In [15]: print d
Got it!!!

In [16]:
In [16]:
```

Fig. 9. Encryption and Decryption of Sample Message

Copyright Three Key Solutions Pte. Ltd. 2016

10

```
Applications  Places  Sun May 8, 10:06 AM
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/kcgw

File Edit View Search Terminal Tabs Help

vagrant@vagrant-ubuntu-trusty-64: /vagrant/bin
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/keyring
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/kcgw

In [16]:
In [16]:
In [16]:
In [16]:
In [16]:
In [16]:
In [16]:
In [16]: s = g.sign('SMBC1', 'redman', 'Got it!!!')

In [17]: print s
<SignedMessage>
  <Signatures>
    <SignatureKeyPair>
      <PublicKey>308201B63082012B06072A8648CE3804013082011E028181008AB6C979B01A7353067FDD8ACEF0A3871C402353449AF467825A70C5DB61B41EE46ABA2727F78C1DB4C3727A7BA29C07779C547B8A7984F833775
734E67E29C1C6D868F854969ED7DC2594536ADCB1FE4D907C077399BA3CDEADDA2ED244F2A8279CD46A6839C977E920AA1203E524964BA6C597E3A999CCDF3EEFFAB72A553021500C2AB95ECFF307F7EC81E4C617491B34BDC8988502818
0566F80CF38CC3AA41C44210552F2E8D2060FCE246DA025C2A1CB0DEDD56C7A60555821CA683B221B6EB5D30F55E402D70DFC58193CD75D03B043E0883E158C2F4C74A25C371E50E4D6F275FF13E8FD41A58BE089199F60D2FA69563EC1CFF
1E08348FB9D7F89DAB6C15BB85C9749DB23F89C65F71D4EC90D05CF2406C917EAC3038184000281804897DAD073C8A24BC72D4F0FA0BF1C1FF1F69FD170475357B5D9F4C8627AA7852504A6935DB301F7DF023BA27DE2B8009E47AF7F12B3
DF941DC0C1FEAB5F58D263037749EF11E06F08FE086537A99B29E2D9067EA125944FEBA7435CDB920FA7B3CA2A50C045A3B060DE105E7B8B9ACB38432494493BBB641E3484E28D69C00</PublicKey>
    <Signature>A93A23170128FD1EDD790303882D3983E58430A6475F9854567871B23BE2192A88E03725024DBA1E</Signature>
    </SignatureKeyPair>
  </Signatures>
  <Message>Got it!!!</Message>
</SignedMessage>

In [18]: g.verify('SMBC1', s)
- 01:06:05.224 DEBUG: Verified signature on message

Out[18]: True

In [19]:
In [19]:
In [19]:
In [19]:
In [19]:
```

Fig. 10. Signing and Verification of Sample Message

```
Applications Places Sun May 8, 10:06 AM
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/kgw

File Edit View Search Terminal Tabs Help

vagrant@vagrant-ubuntu-trusty-64: /vagrant/bin
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/keyring
vagrant@vagrant-ubuntu-trusty-64: /vagrant/src/kgw

In [19]:
In [19]:
In [19]: s = g.sign('SMBC1', 'redman', g.encrypt('SMBC1', 'Got it!!!'))
INFO:Main:encryption pubkey: ...f466abec

In [20]: print s
<SignedMessage>
  <Signatures>
    <SignatureKeyPair>
      <PublicKey>308201B63082012B06072A8648CE3804013082011E028181008AB6C979B01A7353067FDD8ACEF0A3871C402353449AF467825A70C50B61B41EE46ABA2727F78C1DB4C3727A7BA29C07779C547B8A7984F833775
734E67E29C1C6D868F854969ED7DC2594536ADCB1FE4D907C077399BA3CDEADDA2ED244F2A8279CD46A6839C977E920AA1203E524964BA6C597E3A999CCDF33EEFFAB72A553021500C2AB95ECFF307F7EC81E4C617491B34BFD8C8988502818
0566F80CF38C3AA41C44210552F2E8D2060FCE246DA025C2A1CB0DEDD567A60555821CA683B22186EB5D30F55E402D70DFC58193CD7503B043E0883E158C2F4C74A25C371E50E4D6F275FF13E8FD41A58BE089199F60D2FA69563EC1CFF
1E0834BF89D7F89DAB6C158B85C9749DB23F89C65F71D4EC90D05CF2406C917EAC3038184000281804897AD073C8A248C72D4F0FA0BF1C1FF1F69FD1704753537B5D9F4C8627AA7852504A6935DB301F7DF023BA27DE2B8009E47AF7F12B3
DF941DC0C1FEAB5F58D263037749EF11E06F0BFE086537A99B29E2D9067EA125944FEBA7435CDB920FA7B3CA2A50C045A3B606DE105E78BB9ACB38432494493BBB641E3484E28D69C00</PublicKey>
    <Signature>18D3FC9F95E30E1B810F44EFB46A495BFD3922AB20756135A8F3C90CD3B069CF863ABCD98E99ED00</Signature>
  </SignatureKeyPair>
</Signatures>
<Message>&lt;SecureMessage Timestamp="2016-05-08 01:06:24.108518+00" Cipher="AES" PKI="ElGamal"&gt;
&lt;AssociatedData&gt;
&lt;InitialValue&gt;B572F483E341FF3F1D9F2AE04238CA14&lt;/InitialValue&gt;
&lt;EncryptedSymmetricKeys&gt;
&lt;EncryptedSymmetricKey&gt;
&lt;CipherText&gt;75D62E65ABAEC4F609B2611D503340884A453385A9B5F3B60C9B2331992298DA6890AB912E030B5364B274FBEE03D4439D7B53F82BDFBCDBB4395EC185E8971498159BDC15E15C99983583D6AD
F31B9F22D7DAC2F762564334F67ECBDABB18669B77149F0280A8621C9CBB4DA25FCC309A1D68CCC8F9E4703A6AE048E1B43B3E2B32ECAA082E3C7CC139B3359A33CCF0787906546391309E65B5A2E283519731DCBFB32FEC1EAE208CB7B925
C2BDECC203B2416D4E8FBC08D04BCA03F34C2F2359112EDEC04A5EE0FDF6BFEBA85F4E787F074C653E02B5D092803EB4729E3EDA22717259EE373B25B5CDB60C9884F151AF9670B6BF65DF4CEE54AD0087D662C976D9CE67E0A822832294E
71E3126EA123080C2FAA65837E53224F0975E87298A118C1889F06B3C3EBC4B2E8F7F300B7CB803CCFE1C84C09B09847F27A8A6611164F474013F782BBB593F3C33E819DEB9DEACA04FC158E767EC514CCEF581BA25DB0845EE1BAD89A505B
81DCFE65E1FF1139274801391R42C88D37CE3F1C036768792944884DCA04C2BA1C3299B4E933BAD879744BD3BAFF02DE1EDFD4B3DD395F0C4C6AF7B8F1F3739C7EB6BE567E00B3ABF5B1318E5AAC71AEE6A434062F9CA3AD3A6D50A4EBE149
163E953A6A0B93648EB3ED7133DD73219BF500D875AE058CA28B18B8A4C9AC5A13632EC6F0BB4DB0F6F938583356F396E8C9713CBD1&lt;/CipherText&gt;
&lt;PublicKey&gt;3082020C02820101009670B3388B41C8226D0BE56318ABA75BC69176801BC2D50D6D27D78F05618CCBDCFE591AAC8D4831884441B3A7C488E45C087B033E8AA2DB49B128495C88E49B3741696CA9F
2B3841A7E8F4D5E5937A6C568FFE772356C38288011830F07257FC1D39DDA3BE2961F7EAF55118CF8AADB13CDD23296CB3391BB3EC0ACD5D025320AC2A39FB546D28A0D13C56CE8B8964A86D15B02153B01445217E7A90408991320E5E6F0A
1DF7579D0A18FE43168484A162352707F65A5ABC2F35B7E61A9358E0E9B7506E8DF12D3564A747FDC9586BD30DE85D161715B56207EF30896E1728B6F7DA325C4B293607A9C4EA9C394A9D6B669CA41E552FE5D65FCA6E07DC9CD4B0201030
282010068F6723C7A02DE2382E508A3F58AD4FFDF7D39A83B91D289DAD73AEFE3FD899F760F59708D6A07A07E1B92B2D78CA77C6E9A21425FDC0EA59BDD6409130716A2ABE792565FEC8B2AC11461CD7E01144794A887F58BAFE638750A6A
CC9613075FD63BB971658A9086C89397A857B3516E12A859B6601FE78B9F646341839E4183AE7AD5A32F40E1E273C5E67F0F741DB095C08EA7930A4C3A5FE5D5B23D20B5089ED9E5A52AC0AFAD3AD079ECC95CAB93C6837EE1056B6F123518
50EF7CDBAE9F9207145FBECAC4AD095878117001AE23D201F478CC93D21D893304B38801080D7A3557613FD57D4EE0C2206A9C680B7ADFA7303A5D4483F51B4193BF466ABEC&lt;/PublicKey&gt;
&lt;/EncryptedSymmetricKey&gt;
&lt;/EncryptedSymmetricKeys&gt;
&lt;/AssociatedData&gt;
&lt;/EncryptedMessage&gt;8B365DD435DCE722CD77C0EDC32CD8E2DE8E6A108500A3E6BD&lt;/EncryptedMessage&gt;
&lt;/SecureMessage&gt;
</Message>
</SignedMessage>

In [21]:
```

Fig. 11. Signing and Encryption Composition of Sample Message